УТВЕРЖДАЮ

{Руководитель} {Название Организации}

{ФИО}

XX _____ 20__ года

МОДЕЛЬ УГРОЗ

БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

«НАЗВАНИЕ ИС»

ПРИНАДЛЕЖАЩЕЙ

{НАЗВАНИЕ ОРГАНИЗАЦИИ}

Владивосток, 2017 г.

ОГЛАВЛЕНИЕ {не забывать обновлять после редактирования}

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищенном исполнении
ГИС	- государственная информационная система
ИСПДн	- информационная система персональных данных
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 информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её 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 – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических 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 информации.

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.

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 становится невозможным без использования дополнительной информации 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 – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, 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, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

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 раскрытие персональных данных неопределенному кругу лиц.

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 подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной 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 – технические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

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

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 в области защиты информации и персональных данных:

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

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

{ПДн} [3] - Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

{ГИС} [4] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года);

{ПДн} [5] - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года);

[6] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[7] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[8] - Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru);

{СКЗИ} [9] – Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432);

{СКЗИ} [10] – Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утверждены приказом ФСБ России от 10 июля 2014 года № 378).

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([4]-[7]), регламентирующих порядок обеспечения безопасности ПДн. {Если это ГИС без ПДн, то заменить на ЗИ или КИ, также убрать из определений все что связано с ПДн}

Настоящая «Модель угроз» содержит систематизированный перечень угроз безопасности персональных данных и иной защищаемой информации при их обработке в государственной информационной системе «Название ИС» (ГИС «Название ИС»). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных и иной защищаемой информации, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз определяет актуальные угрозы для ГИС «Название ИС».

Модель угроз содержит данные по угрозам безопасности персональных данных и иной защищаемой информации, обрабатываемых в ГИС «Название ИС», связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ГИС «Название ИС» с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ГИС «Название ИС» 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 ГИС «Название ИС», разработчиков ГИС «Название ИС» и их подсистем.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ГИС «Название ИС» 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 ГИС «Название ИС»;
- 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 ГИС «Название ИС», в результате которого может быть нарушено их функционирование;
- контроль за обеспечением третьего уровня защищенности персональных данных и третьего класса защищенности ГИС «Название ИС».

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

Угрозы безопасности ПДн, обрабатываемых в ГИС «Название ИС», содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ГИС «Название ИС». Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [7] и [8]. Кроме того, Модель угроз может быть пересмотрена по решению оператора ({Название организации}) на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ГИС «Название ИС», а также по результатам

мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

ОПИСАНИЕ ГИС «НАЗВАНИЕ ИС»

Общие сведения об информационной системе

Назначение ГИС «Название ИС» – автоматизация деятельности учреждений образования.

Оператор ГИС «Название ИС» – {Название организации}.

В ГИС «Название ИС» необходимо обеспечить конфиденциальность, целостность и доступность персональных данных.

В ГИС «Название ИС» обрабатываются специальные категории персональных данных более 100 000 субъектов.

Охрана помещений

{Описать}

Используемые в ГИС «Название ИС» информационные технологии создания и использования ПДн

{Описать}

Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных {убрать этот раздел, если нет СКЗИ}

В ГИС «Название ИС» существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ. К таким угрозам относятся угрозы, связанные с передачей персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

Дополнительные объекты защиты

Согласно [9] для ГИС «Название ИС» к объектам защиты дополнительно относятся:

1) применяемые в ГИС «Название ИС» СКЗИ;
2) среда функционирования криптосредства (СФК);
3) информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
4) документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФК;
5) носители защищаемой информации, используемые в ГИС «Название ИС» в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
6) используемые каналы (линии) связи;
7) помещения, в которых находятся ресурсы ГИС «Название ИС», имеющие отношение к криптографической защите персональных данных.

Характеристики безопасности объектов угроз

В ГИС «Название ИС» необходимо обеспечить целостность, доступность и конфиденциальность защищаемой информации.

ПРИНЦИПЫ МОДЕЛИ УГРОЗ

{вариант с СКЗИ} В основе Модели угроз лежат следующие общие принципы:

1) Безопасность персональных данных и иной защищаемой информации при их обработке в информационных системах обеспечивается с помощью системы защиты информации в ГИС «Название ИС».

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных и иной защищаемой информации (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 информации ГИС «Название ИС» (в том числе и СКЗИ) не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (система защиты информации не предназначена для защиты 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) Криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ.

8) СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

9) Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

10) СКЗИ являются как средством защиты информации, так и объектом защиты.

{вариант без СКЗИ} В основе Модели угроз лежат следующие общие принципы:

1) Безопасность (обеспечение конфиденциальности, доступности и целостности) защищаемой информации при ее обработке в ГИС обеспечивается с помощью системы (подсистемы) защиты информации.

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

3) Защищаемая информация обрабатывается и хранится в государственной 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) Система защиты информации не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий.

5) Нарушитель может действовать на различных этапах жизненного цикла ГИС.

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.

По признаку принадлежности к ГИС «Название ИС» все нарушители делятся на две группы:

Внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ГИС «Название ИС»;

Внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ГИС «Название ИС».

Внешний нарушитель

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 ГИС «Название ИС», является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

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 ГИС «Название ИС» обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ГИС «Название ИС» в соответствии с принятой политикой информационной безопасности.

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 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, не 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).

К **внутренним нарушителям** могут относиться:

- администратор безопасности ГИС «Название ИС» (категория I);
- администраторы конкретных подсистем или баз данных ГИС «Название ИС» (категория II);
- пользователи ГИС «Название ИС» (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ГИС «Название ИС», но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал (водитель, уборщик помещений и т.п.) (категория VII);
- уполномоченный персонал разработчиков ГИС «Название ИС», который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ГИС «Название ИС» (категория VIII).

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

На лиц категорий I-II возложены задачи по администрированию программно-аппаратных средств и баз данных ГИС «Название ИС» для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ГИС «Название ИС». Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ГИС «Название ИС», а также к техническим и программным средствам ГИС «Название ИС», 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 ГИС «Название ИС» 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).

К лицам категорий I-II ввиду их исключительной роли в ГИС «Название ИС» 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-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.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

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

- общая информация – информации о назначении и общих характеристиках ГИС «Название ИС»;
- эксплуатационная информация – информация, полученная из эксплуатационной документации;
- чувствительная информация – информация, дополняющая эксплуатационную информацию об ГИС «Название ИС» (например, сведения из проектной документации ГИС «Название ИС»).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ГИС «Название ИС»;
- сведения об информационных ресурсах ГИС «Название ИС»: 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 ГИС «Название ИС»;
- данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
- исходные тексты программного обеспечения ГИС «Название ИС»;
- 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 автоматизированной информационной системе (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 о ГИС «Название ИС» и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ГИС «Название ИС». Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ГИС «Название ИС» в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными о ГИС «Название ИС» 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.

Предположения об имеющихся у нарушителя средствах реализации угроз:

- аппаратные компоненты средства защиты ПДн (СЗПДн);
- доступные в свободной продаже технические средства и программное обеспечение;

- специально разработанные технические средства и программное обеспечение.

Нарушители согласно банку данных угроз ФСТЭК России

Дополнительно в банке данных угроз ФСТЭК России определены три типа внешних и внутренних нарушителей – с низким потенциалом, со средним потенциалом и с высоким потенциалом.

Нарушители с низким потенциалом имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушители со средним потенциалом обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

Для ГИС «Название ИС» определен нарушитель со **средним** потенциалом.

{Удалить этот раздел, если нет СКЗИ} Обобщенные возможности источников атак

В соответствии с [9] выдвигаются предположения о наличии обобщенных возможностей у источников атак:

№ п/п	Описание возможности	Наличие возможности
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и СФК	Да
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и СФК	Да
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

Реализация угроз безопасности информации, определяемых по возможностям источников атак {удалить раздел, если нет СКЗИ}

Настоящий раздел сформирован в соответствии с [9], а также на основе данных нижеследующей таблицы делается вывод о необходимом классе СКЗИ для ГИС «Название ИС» в соответствии с [10].

В [9] и [10] в качестве мотивации в основном рассматриваются целенаправленные действия нарушителей, направленные на нарушение безопасности, защищаемой с помощью СКЗИ, информации или создание условий для этого (атаки). В то же время, в настоящей Модели угроз под нарушителем согласно разделу «Термины и определения» может пониматься как субъект атаки, так и физическое лицо, **случайно** совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных. В любом случае, внешний нарушитель является субъектом атаки, случайно совершить действия по нарушению свойств безопасности информации в ГИС «Название ИС» он не может, так как не имеет легальных прав доступа к элементам системы. В настоящей Модели угроз установлены возможности для сговора внутренних и внешних нарушителей. Сговоры, являющиеся комплексным нарушителем, объединяют в себе мотивации и возможности сговаривающихся потенциальных нарушителей. Комплексные нарушители являются субъектами атаки. Соответственно, наиболее опасным для ГИС «Название ИС» является комплексный нарушитель, совмещающий в себе целенаправленность атак на характеристики безопасности информации и возможности доступа к элементам ГИС «Название ИС» в пределах контролируемой зоны. Актуальность использования возможностей нарушителей для реализации атак определена в таблице.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФК; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФК	Актуально	
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в	Актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФК		
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФК	Актуально	
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с контрольно-пропускным режимом. Помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			санкционированного прохода. Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей. На АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты. Дополнительно неактуальность возможности обоснована в разделе «Угрозы, связанные с недекларированными возможностями системного и прикладного программного обеспечения» настоящей Модели угроз
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
4.1	Создание способов,	Не актуально	Не осуществляется обработка сведений,

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО		составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФК, обеспечивается в соответствии с контрольно-пропускным режимом. Помещения, в которых располагаются СКЗИ и СФК, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФК, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации. Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам. Осуществляется регистрация и учет действий пользователей. На АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты. Дополнительно неактуальность возможности обоснована в разделе «Угрозы, связанные с недекларированными возможностями системного и прикладного программного обеспечения» настоящей Модели угроз
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			возможности

В соответствии с изложенными выше предположениями о наличии возможностей у нарушителей на проведение атак и в соответствии с [10] (п. 12) в ГИС «Название ИС» должны применяться СКЗИ класса не ниже КС3.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий раздел составлен в соответствии с [6], [7] и [8]. В разделе определяются актуальные угрозы безопасности персональных данных и иной защищаемой информации, не затрагивающие вопросы, связанные с применением в ГИС «Название ИС» криптосредств.

Показатель исходной защищенности ГИС «Название ИС» {актуализировать показатели и % в соответствии с реалиями конкретной ГИС}

ГИС «Название ИС» имеет следующие технические и эксплуатационные характеристики:

а) Территориальное размещение ГИС «Название ИС» - локальная ГИС «Название ИС», развернутая в пределах одного здания. Уровень защищенности - высокий.

б) Наличие соединения с сетями связи общего пользования - ГИС «Название ИС», имеющая одноточечный выход в сеть общего пользования. Уровень защищенности - средний.

в) встроенные (легальные) операции с записями баз персональных данных – модификация, передача. Уровень защищенности - низкий.

г) разграничение доступа к персональным данным - ГИС «Название ИС», к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ГИС «Название ИС», либо субъект ПДн. Уровень защищенности - средний.

д) наличие соединений с другими базами персональных данных иных ГИС «Название ИС» - ГИС «Название ИС», в которой используется одна база ПДн, принадлежащая организации – владельцу данной ГИС «Название ИС». Уровень защищенности - высокий.

е) уровень обобщения (обезличивания) персональных данных - ГИС «Название ИС», в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности - низкий.

ж) объем персональных данных, которые предоставляются сторонним пользователям ГИС «Название ИС» без предварительной обработки - ГИС «Название ИС», не предоставляющие никакой информации. Уровень защищенности - высокий.

Определение исходной степени защищенности:

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	3	42%
2	Средний	2	71%
3	Низкий	2	-

В соответствии полученными данными устанавливается **средний показатель исходной защищенности**. Устанавливается значение коэффициента $\mathbf{Y_1=5}$.

Определение последствий от нарушения свойств безопасности информации (опасность угроз)

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ГИС «Название ИС» является информационной системой, для которой

нарушение конфиденциальности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ГИС «Название ИС» является информационной системой, для которой нарушение целостности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

С учетом обрабатываемых категорий персональных данных и прочих характеристик, ГИС «Название ИС» является информационной системой, для которой нарушение доступности информации, обрабатываемой в ней, может привести к негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет низкую опасность, если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Согласно методике определения актуальных угроз, угроза имеет высокую опасность, если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Согласно данным положениям для угроз частной модели, приводящих к нарушению конфиденциальности информации принимается **средняя опасность**.

Согласно данным положениям для угроз частной модели, приводящих к нарушению целостности информации принимается **средняя опасность**.

Согласно данным положениям для угроз частной модели, приводящих к нарушению доступности информации принимается **средняя опасность**.

Угрозы по банку данных угроз безопасности информации ФСТЭК России

В таблице приведены неприменимые к рассматриваемой ГИС «Название ИС» угрозы безопасности информации, приведено их условное обозначение в банке данных угроз ФСТЭК России, а также причины исключения данных угроз из списка рассматриваемых угроз.

№ п/п	Условные обозначения угроз, исключаемых из списка рассматриваемых угроз	Характеристика исключаемых угроз и причина исключения
1	УБИ.001, УБИ.002, УБИ.029, УБИ.038, УБИ.047, УБИ.050, УБИ.057, УБИ.060, УБИ.081, УБИ.082, УБИ.097, УБИ.105, УБИ.106, УБИ.110, УБИ.136, УБИ.146, УБИ.147, УБИ.148, УБИ.161	Из списка рассматриваемых угроз исключаются угрозы, связанные с системами распределенных вычислений (грид-системами), суперкомпьютерами и большими данными, поскольку такие технологии не применяются в рассматриваемой ГИС «Название ИС»
2		Из списка рассматриваемых угроз исключаются угрозы, связанные с системами виртуализации, поскольку такие технологии не применяются в рассматриваемой ГИС «Название ИС»
3		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием беспроводных сетей связи, поскольку такие технологии не применяются в рассматриваемой ГИС «Название ИС»
4		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием облачных сервисов и/или ресурсов, поскольку такие технологии не применяются в

№ п/п	Условные обозначения угроз, исключаемых из списка рассматриваемых угроз	Характеристика исключаемых угроз и причина исключения
		рассматриваемой ГИС «Название ИС»
5		Из списка угроз исключаются угрозы, связанные с уязвимостями Web-ресурсов, поскольку ГИС «Название ИС» не содержит веб-серверов, веб-сервисов и веб-ресурсов
6		Из списка рассматриваемых угроз исключаются угрозы, связанные с автоматическими системами управления технологическими процессами (АСУ ТП), поскольку ГИС «Название ИС» не является системой управления промышленными или иными технологическими мощностями
7		Из списка рассматриваемых угроз исключаются угрозы, связанные с использованием мобильных устройств, поскольку такие устройства не применяются в рассматриваемой ГИС «Название ИС»
8		Из списка рассматриваемых угроз исключаются оставшиеся угрозы, реализация которых возможна только нарушителем с высоким потенциалом

В следующей таблице приведены описания, условные обозначения, характеристики остальных угроз безопасности согласно банку данных угроз ФСТЭК России. В столбцах «Потенциал внутреннего нарушителя» и «Потенциал внешнего нарушителя» стоит «1», если потенциал высокий; «2», если потенциал средний; «3», если потенциал низкий; «-», если потенциал нарушителя не определен в банке данных угроз ФСТЭК России.

В столбце «Нарушаемые свойства безопасности информации» приняты следующие сокращения для свойств безопасности информации:

К – конфиденциальность;

Ц – целостность;

Д – доступность.

В столбце «Применимость» стоит знак «+», если данная угроза существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данная угроза не существует и не может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации.

№ п/п	Идентификатор	Описание угрозы	Способ реализации угрозы	Потенциал внутреннего нарушителя	Потенциал внешнего нарушителя	Объекты воздействия	Нарушаемые свойства безопасности информации	Предпосылки	Обоснование отсутствия предпосылок
Угрозы, связанные с криптографическими средствами защиты информации									
1.	УБИ.003	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки	Реализация угрозы возможна в случае наличия у нарушителя сведений о применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	-	2	Метаданные, системное программное обеспечение	К, Ц		
Угрозы, связанные с уязвимостями BIOS/UEFI									
2.	УБИ.004	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	3	-	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Ц		

№ п/п	Идентификатор	Описание угрозы	Способ реализации угрозы	Потенциал внутреннего нарушителя	Потенциал внешнего нарушителя	Объекты воздействия	Нарушаемые свойства безопасности информации	Предпосылки	Обоснование отсутствия предпосылок
		системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI							
3.									
4.									

Списки актуальных угроз

Угрозы из банка данных угроз безопасности информации ФСТЭК России являются совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации.

Из итогового списка исключаются угрозы, для которых в предыдущем разделе обоснована неприменимость.

Меры для нейтрализации угрозы считаются принятыми и достаточными, если они позволяют нейтрализовать все компоненты угрозы. Меры считаются принятыми, но недостаточными, если нейтрализуются не все компоненты угрозы. Меры считаются не принятыми, если они не позволяют нейтрализовать ни один компонент угрозы. Решение о наличии мер для нейтрализации каждой угрозы принимается на основе аудита ГИС «Название ИС». В списке актуальных угроз указывается «+», если меры приняты; «+-», если меры приняты, но недостаточны; «-», если меры не приняты.

Существование предпосылок для угроз определяется экспертом с учетом особенностей архитектуры и функционирования ГИС «Название ИС».

Вероятность угрозы определяется по таблице:

	Меры не приняты	**Меры недостаточны**	**Меры достаточны**
Есть предпосылки	Высокая вероятность (Y_2=10)	Средняя вероятность (Y_2=5)	Низкая вероятность (Y_2=2)

Коэффициент Y_1 – одинаков для всех угроз и определен в разделе «Показатель исходной защищенности.

Далее, для каждой угрозы в зависимости от вероятности и исходного уровня защищенности определяется возможность ее реализации – коэффициент $Y = (Y_1+Y_2)/20$.

В зависимости от значения Y, возможность реализации угроз может быть следующей:

0≤Y≤0,3 – возможность реализации угрозы **низкая**;
0,3<Y≤0,6 – возможность реализации угрозы **средняя**;
0,6<Y≤0,8 – возможность реализации угрозы **высокая**;
Y>0,8 – возможность реализации угрозы **очень высокая**.

Опасность каждой угрозы зависит от нарушаемых свойств безопасности информации и установлена в разделе «Определение последствий от нарушения свойств безопасности информации (опасность угроз)».

Актуальность угроз определяется по возможности реализации и опасности угрозы исходя из таблицы:

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

№ п/п	Угроза	Меры приняты	Коэффициент вероятности	Коэффициент реализуемости угрозы	Возможность реализации	Опасность	Актуальность
1	УБИ.003	+	5	0,50	Средняя	Средняя	Да
2							
3							
4							
5							
6							
7							