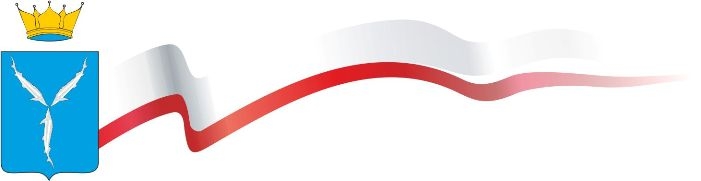
КОМИТЕТ ПО ИНФОРМАТИЗАЦИИ САРАТОВСКОЙ ОБЛАСТИ



г. Саратов

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
по защите информации, не составляющей государственную тайну и  
организации защиты информации, при автоматизированной обработке  
персональных данных в структурных подразделениях Правительства  
области, исполнительных органах государственной власти области,  
органах местного самоуправления области и подведомственных им  
организациях Саратовской области

УТВЕРЖДАЮ

Министр области –

председатель комитета

по информатизации области

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л.Ю. Кузнецова

СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#Содержание)

[ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 6](#Обозначения)

[СПИСОК ТЕРМИНОВ 7](#Термины)

[I.ЗАЩИТА ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ  
ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ  
ИНФОРМАЦИОННЫХ СИСТЕМАХ 11](#Глава1)

[ВВЕДЕНИЕ 11](#Введение)

[Организация защиты информации, содержащейся в информационной системе 12](#п1_1)

[Формирование требований к защите информации, содержащейся в  
информационной системе……………………………………………………………………14](#п1_2)

[Разработка системы защиты информации информационной системы 16](#п1_3)

[Внедрение системы защиты информации информационной системы…………………...18](#п1_4)

[Аттестация информационной системы и ввод ее в действие 20](#п1_5)

[Обеспечение защиты информации в ходе эксплуатации аттестованной  
информационной системы 22](#п1_6)

[Обеспечение защиты информации при выводе из эксплуатации  
аттестованной информационной системы или после принятия решения об  
окончании обработки информации ………………………………………………………...24](#п1_7)

[Определение класса защищенности информационной системы ………………………...25](#п1_8)

[Требования к мерам защиты информации, содержащейся в информационной ………..27](#п1_9)

[II. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИ  
АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В  
СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ ПРАВИТЕЛЬСТВА ОБЛАСТИ,  
ИСПОЛНИТЕЛЬНЫХ ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ  
ОБЛАСТИ, ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ ОБЛАСТИ И  
ПОДВЕДОМСТВЕННЫХ ИМ ОРГАНИЗАЦИЯХ САРАТОВСКОЙ ОБЛАСТИ](#Глава2) [44](#bookmark19)

[ВВЕДЕНИЕ 44](#Введение2)

[Понятие и состав персональных данных 44](#п2_1)

[Основные мероприятия по приведению информационных систем  
персональных данных в соответствие требованиям законодательства 48](#п2_2)

[Правовое основание обработки персональных данных 50](#п2_3)

[Перечень персональных данных, обрабатываемых в государственном или  
муниципальном органе в связи с реализацией трудовых отношений, а также в  
связи с оказанием государственных или муниципальных услуг и  
осуществлением государственных или муниципальных функций 50](#п2_4)

[Определение типа угроз и установление уровня защищенности персональных  
данных при их обработке в информационных системах персональных данных, в  
зависимости от угроз безопасности этих данных 51](#п2_5)

[Состав и содержание организационных и технических мер по обеспечению  
безопасности персональных данных при их обработке в информационных  
системах персональных данных……………… 56](#п2_6)

[Регистрация в качестве оператора персональных данных 71](#п2_7)

[Условия обеспечения конфиденциальности информации и Ответственность  
за нарушения требований Федерального закона № 152-ФЗ………………………………72](#п2_8)

[Получение согласия субъекта персональных данных на обработку его  
персональных данных 73](#п2_9)

[Правила обработки персональных данных…………… 74](#п2_10)

[Правила работы с обезличенными персональными данными 78](#п2_11)

[Правила рассмотрения операторами запросов субъектов персональных  
данных или их представителей……………………………………………………………...79](#п2_12)

[Разработка модели угроз безопасности персональных данных при их  
обработке в информационной системе персональных данных 82](#п2_13)

[Правила осуществления внутреннего контроля соответствия обработки  
персональных данных требованиям к защите персональных данных……………………87](#п2_14)

[Перечень нормативных правовых актов и документов, используемых при  
организации и проведении мероприятий по обеспечению безопасности  
персональных данных при их обработке в информационных системах  
персональных данных 88](#п2_15)

[Приложение 1. ПРОЕКТ Приказ о назначении ответственного за защиту](#Приложение1)

[информации 90](#Приложение1)

[Приложение 2. ПРОЕКТ Приказ о создании комиссии по классификации  
информационной системы 91](#Приложение2)

[Приложение 3. ПРОЕКТ Акт классификации информационной системы 92](#Приложение3)

[Приложение 4. ПРОЕКТ Типовая форма модели угроз безопасности](#Приложение4)

[информации и модели нарушителя 93](#Приложение4)

[Приложение 5. ПРОЕКТ Приказ о назначении ответственных за обеспечение  
безопасности персональных данных 110](#Приложение5)

[Приложение 6. ПРОЕКТ Приказ о назначении ответственного за обеспечение  
 безопасности персональных данных 111](#Приложение6)

[Приложение 7. ПРОЕКТ Перечень информационных систем персональных  
данных 112](#Приложение7)

[Приложение 8. ПРОЕКТ Перечень персональных данных, обрабатываемых в  
информационных системах персональных данных 113](#Приложение8)

[Приложение 9. ПРОЕКТ Образец уведомления об обработке (о намерении  
осуществлять обработку) персональных данных, рекомендации по заполнению  
образца форму уведомления об обработке (о намерении осуществлять  
обработку) персональных данных ….114](#Приложение9)

[Приложение 10. ПРОЕКТ Перечень должностей служащих государственного  
или муниципального органа, замещение которых предусматривает  
осуществление обработки персональных данных либо осуществление доступа к  
персональным данным ….118](#Приложение10)

[Приложение 11. ПРОЕКТ Перечень должностей, ответственных за проведение  
мероприятий по обезличиванию обрабатываемых персональных данных](#Приложение11)

[119](#Приложение11)

[Приложение 12. ПРОЕКТ Приказ о создании комиссии по определению уровня  
защищенности ИСПДн 120](#Приложение12)

[Приложение 13. ПРОЕКТ Акт определения уровня защищенности в  
ИСПДн 121](#Приложение13)

[Приложение 14. ПРОЕКТ Должностная инструкция ответственного за  
организацию обработки персональных данных в государственном или  
муниципальном органе 122](#Приложение14)

[Приложение 15. ПРОЕКТ Должностная инструкция администратора  
безопасности информационных систем персональных данных 124](#Приложение15)

[Приложение 16. ПРОЕКТ Типовое обязательство служащего государственного](#Приложение16)

[или муниципального органа, непосредственно осуществляющего обработку](#Приложение16)

[персональных данных, в случае расторжения с ним государственного или](#Приложение16)

[муниципального контракта прекратить обработку персональных данных,](#Приложение16)

[ставших известными ему в связи с исполнением должностных обязанностей………….127](#Приложение16)

[Приложение 17. ПРОЕКТ Форма согласия субъекта персональных данных на](#Приложение17)

[обработку персональных данных 128](#Приложение17)

[Приложение 18. ПРОЕКТ Форма согласия субъекта персональных данных на](#Приложение18)

[обработку персональных данных (для участников конкурса на формирования](#Приложение18)

[кадрового резерва, лиц состоящих в кадровом резерве) 129](#Приложение18)

[Приложение 19. ПРОЕКТ Форма согласия на обработку персональных данных](#Приложение19)

[государственных гражданских служащих, иных субъектов персональных](#Приложение19)

[данных 130](#Приложение19)

[Приложение 20. ПРОЕКТ Разрешительная система доступа к информационным](#Приложение20)

[ресурсам, программным и техническим средствам информационных систем](#Приложение20)

[персональных данных 131](#Приложение20)

[Приложение 21. ПРОЕКТ Порядок доступа служащих государственного или](#Приложение21)

[муниципального органа в помещения, в которых ведется обработка](#Приложение21)

[персональных данных 132](#Приложение21)

[Приложение 22. ПРОЕКТ Форма отзыва согласия субъекта на обработку](#Приложение22)

[персональных данных 133](#Приложение22)

[Приложение 23. ПРОЕКТ Форма запроса на получение информации,](#Приложение23)

[составляющей персональные данные у субъекта персональных данных………………. 134](#Приложение23)

[Приложение 24. ПРОЕКТ Форма уведомления об уничтожении персональных](#Приложение24)

[данных субъекта персональных данных 135](#Приложение24)

[Приложение 25. ПРОЕКТ Форма уведомления о блокировании персональных](#Приложение25)

[данных субъекта персональных данных 136](#Приложение25)

[Приложение 26. ПРОЕКТ Форма уведомления об уточнении персональных](#Приложение26)

[данных субъекта персональных данных 137](#Приложение26)

[Приложение 27. ПРОЕКТ Форма уведомления об обработке персональных](#Приложение27)

[данных субъекта персональных данных 138](#Приложение27)

[Приложение 28. ПРОЕКТ Форма журнала регистрации и учета обращений](#Приложение28)

[субъектов персональных данных………………………………………………………….. 140](#Приложение28)

[Приложение 29. ПРОЕКТ Модель угроз безопасности персональных данных](#Приложение29)

[при их обработке в информационной системе персональных данных 141](#Приложение29)

[Приложение 30. ПРОЕКТ Регламент учета средств защиты информации,](#Приложение30)

[эксплуатационной и технической документации к ним, электронных носителей](#Приложение30)

[персональных данных 165](#Приложение30)

[Приложение 31. ПРОЕКТ Положение по обеспечению безопасности](#Приложение31)

[персональных данных при их обработке в информационных системах](#Приложение31)

[персональных данных 168](#Приложение31)

[Приложение 32. ПРОЕКТ Протокол проведения внутренней проверки условий](#Приложение32)

[обработки персональных данных 176](#Приложение32)

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИТС - автоматизированная информационно-телекоммуникационная

система

АРМ - автоматизированное рабочее место

АУ - актуальные угрозы

ИС - автоматизированная система

ВТСС - вспомогательные технические средства и системы

ИБ - информационная безопасность

ИКХ - информация конфиденциального характера

ИСПДн - информационная система персональных данных

ИТ - информационные технологии

КЗ - контролируемая зона

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НДВ ПО - недекларируемые возможности программного обеспечения

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПЭМИН - побочные электромагнитные излучения и наводки

СВТ - средства вычислительной техники

СЗИ- средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СКЗИ - средство криптографической защиты информации

СФ - среда функционирования

ТКУИ - технические каналы утечки информации

УБПДн - угрозы безопасности персональных данных

СПИСОК ТЕРМИНОВ

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

Администратор безопасности информационной системы  
персональных данных – лицо, уполномоченное на проведение работ по  
поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах  
промышленной эксплуатации и модернизации.

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.

Биометрические персональные данные – сведения, которые  
характеризуют физиологические особенности человека, и на основе которых  
можно установить его личность, включая фотографии, отпечатки пальцев,  
образ сетчатки глаза, особенности строения тела и другую подобную  
информацию.

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

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.

Государственные информационные системы – федеральные  
информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

**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.

**Идентификация ИСПДн** – выделение в информационно -телекоммуникационной инфраструктуре учреждения областей (отдельных рабочих станций, узлов и сегментов сети), в которых осуществляется обработка персональных данных, определение границ контролируемых зон для выделенных областей, присвоение наименований отдельным информационным системам персональных данных в составе информационно- телекоммуникационной инфраструктуры учреждения.

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

**Информативный сигнал** – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных** – 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 таких средств.

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

**Иные категории персональных данных** – персональные данные не относящиеся к категории специальных, биометрических и общедоступных персональных данных.

**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.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

**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.

**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** – документ, содержащий перечень возможных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и характеризующий наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации угроз безопасности персональных данных.

**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.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**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 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.

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

**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.

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

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

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**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.

**Система защиты персональных данных** – совокупность организационных мер и технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технические мероприятия, обеспечивающие безопасность персональных данных.

**Специальные информационные системы** – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от и конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

**Специальные категории персональных данных** – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**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.

**Субъект персональных данных** – физическое лицо, к которому относятся определенные персональные данные либо которое может быть определено на основании определенных персональных данных.

**Технические средства информационной системы персональных данных** –средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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, применяемые в информационных системах.

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

**Типовые информационные системы** – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

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

**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.

**Уровень защищенности персональных данных** – это комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности информационных систем персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – слабость в средствах защиты, которая может быть использована для проникновения в систему.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

**I. 3АЩИТА ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ**

**ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В**

**ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ**

**ВВЕДЕНИЕ**

Настоящие рекомендации разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и на основании Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Настоящие Рекомендация могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

В документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Настоящие Рекомендации предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы (далее - заказчики) и операторов государственных информационных систем (далее - операторы).

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее - уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна

быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

При обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Рекомендации применяются наряду с Рекомендациями по организации защиты информации, при автоматизированной обработке персональных данных в структурных подразделениях правительства области, исполнительных органах государственной власти области, органах местного самоуправления области и подведомственных им организациях Саратовской области ([Глава II](#Глава2)).

Защита информации, содержащейся в государственной информационной системе (далее - информационная система), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

1. **Организация защиты информации, содержащейся в информационной**

**системе**

1. В информационной системе ***объектами защиты*** являются  
   информация, содержащаяся в информационной системе, технические средства  
   (в том числе средства вычислительной техники, машинные носители  
   информации, средства и системы связи и передачи данных, технические  
   средства обработки буквенно-цифровой, графической, видео- и речевой  
   информации), общесистемное, прикладное, специальное программное  
   обеспечение, информационные технологии, а также средства защиты  
   информации.
2. Для обеспечения защиты информации, содержащейся в  
   информационной системе, оператором назначается структурное подразделение  
   или должностное лицо (работник), ответственные за защиту информации  
   ([Приложение 1](#Приложение1)).
3. Для проведения работ по защите информации в ходе создания и  
   эксплуатации информационной системы обладателем информации (заказчиком)  
   и оператором в соответствии с законодательством Российской Федерации при  
   необходимости привлекаются организации, имеющие лицензию на  
   деятельность по технической защите конфиденциальной информации в  
   соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О  
   лицензировании отдельных видов деятельности». Список организаций,  
   имеющих лицензии на деятельность по технической защите конфиденциальной  
   информации доступен в Реестре лицензий на деятельность по технической  
   защите конфиденциальной информации на [сайте ФСТЭК России.](http://fstec.ru/tekhnicheskaya-zashchita-informatsii-ld/72-deyatelnost/tekushchaya/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/dokumenty-po-litsenzirovaniyu-deyatelnosti-organizatsij/reestry/216-reestr01)
4. Для обеспечения защиты информации, содержащейся в  
   информационной системе, применяются средства защиты информации,  
   прошедшие оценку соответствия в форме обязательной сертификации на  
   соответствие требованиям по безопасности информации в соответствии со  
   статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом  
   регулировании». Список СЗИ доступен в Государственном реестре  
   сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 на  
   [сайте ФСТЭК России.](http://fstec.ru/sistema-sertifikatsii-tzi/153-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00)
5. Защита информации, содержащейся в информационной системе,  
   является составной частью работ по созданию и эксплуатации информационной  
   системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе  
   эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз  
   безопасности информации в информационной системе, в рамках системы  
   (подсистемы) защиты информации информационной системы.

Организационные и технические меры защиты информации, реализуемые  
в рамках системы защиты информации информационной системы, в  
зависимости от информации, содержащейся в информационной системе, целей  
создания информационной системы и задач, решаемых этой информационной  
системой, должны быть направлены на исключение:

− неправомерных доступа, копирования, предоставления или  
распространения информации (обеспечение конфиденциальности  
информации);

− неправомерных уничтожения или модифицирования информации  
(обеспечение целостности информации);

− неправомерного блокирования информации (обеспечение  
доступности информации).

1. Для обеспечения защиты информации, содержащейся в  
   информационной системе, проводятся следующие мероприятия:

* формирование требований к защите информации, содержащейся в  
  информационной системе ([Глава I. Раздел 2](#п1_2));
* разработка системы защиты информации информационной системы  
  ([Глава I. Раздел 3](#п1_3));
* внедрение системы защиты информации информационной системы  
  ([Глава I. Раздел 4](#п1_4));
* аттестация информационной системы по требованиям защиты  
  информации (далее - аттестация информационной системы) и ввод ее в  
  действие ([Глава I. Раздел 5](#п1_5));
* обеспечение защиты информации в ходе эксплуатации  
  аттестованной информационной системы ([Глава I. Раздел 6](#п1_6));
* обеспечение защиты информации при выводе из эксплуатации  
  аттестованной информационной системы или после принятия решения об  
  окончании обработки информации ([Глава I. Раздел 7](#п1_7));.

1. **Формирование требований к защите информации, содержащейся в информационной системе**
   1. Формирование требований к защите информации, содержащейся в  
      информационной системе, осуществляется обладателем информации  
      (заказчиком).

Формирование требований к защите информации, содержащейся в  
информационной системе, осуществляется с учетом ГОСТ Р 51583 «Защита  
информации. Порядок создания автоматизированных систем в защищенном  
исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624  
«Защита информации. Автоматизированные системы в защищенном  
исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе  
включает:

* принятие решения о необходимости защиты информации,  
  содержащейся в информационной системе;
* классификацию информационной системы по требованиям защиты  
  информации;
* определение угроз безопасности информации, реализация которых  
  может привести к нарушению безопасности информации в информационной  
  системе, и разработку на их основе модели угроз безопасности информации;
* определение требований к системе защиты информации  
  информационной системы.
  1. При принятии решения о необходимости защиты информации,  
     содержащейся в информационной системе, осуществляется:
* анализ целей создания информационной системы и задач,  
  решаемых этой информационной системой;
* определение информации, подлежащей обработке в  
  информационной системе;
* анализ нормативных правовых актов, методических документов и  
  национальных стандартов, которым должна соответствовать информационная  
  система;
* принятие решения о необходимости создания системы защиты  
  информации информационной системы, а также определение целей и задач  
  защиты информации в информационной системе, основных этапов создания  
  системы защиты информации информационной системы и функций по  
  обеспечению защиты информации, содержащейся в информационной системе,  
  обладателя информации (заказчика), оператора и уполномоченных лиц.

После принятия решения обладателем информации (заказчиком)  
утверждается распорядительный документ о необходимости защиты  
информации, содержащейся в информационной системе.

* 1. ***Классификация информационной системы*** проводится в  
     зависимости от значимости обрабатываемой в ней информации и масштаба  
     информационной системы (федеральный, региональный, объектовый).

Устанавливаются четыре класса защищенности информационной  
системы, определяющие уровни защищенности содержащейся в ней  
информации. Самый низкий класс - четвертый, самый высокий - первый  
([Глава I. Раздел 8](#п1_8)).

Класс защищенности определяется для информационной системы в  
целом и, при необходимости, для ее отдельных сегментов (составных частей).  
Требование ([Глава I. Раздел 9](#п1_9)) к классу защищенности включается в  
техническое задание на создание информационной системы и (или)  
техническое задание (частное техническое задание) на создание системы  
защиты информации информационной системы, разрабатываемые с учетом  
ГОСТ 34.602 «Информационная технология. Комплекс стандартов на  
автоматизированные системы. Техническое задание на создание  
автоматизированной системы» (далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р  
51624.

Класс защищенности информационной системы подлежит пересмотру  
при изменении масштаба информационной системы или значимости  
обрабатываемой в ней информации.

Для проведения классификации информационной системы назначается  
комиссия по проведению классификации информационной системы  
([Приложение 2](#Приложение2)).

Результаты классификации информационной системы оформляются  
актом классификации ([Приложение 3](#Приложение3)).

* 1. Угрозы безопасности информации определяются по результатам  
     оценки возможностей (потенциала, оснащенности и мотивации) внешних и  
     внутренних нарушителей, анализа возможных уязвимостей информационной  
     системы, возможных способов реализации угроз безопасности информации и  
     последствий от нарушения свойств безопасности информации  
     (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются  
структурно-функциональные характеристики информационной системы,  
включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между  
сегментами информационной системы, с иными информационными системами  
и информационно-телекоммуникационными сетями, режимы обработки  
информации в информационной системе и в ее отдельных сегментах, а также  
иные характеристики информационной системы, применяемые  
информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при  
необходимости разрабатываются рекомендации по корректировке структурно-  
функциональных характеристик информационной системы, направленные на  
блокирование (нейтрализацию) отдельных угроз безопасности информации.

***Модель угроз безопасности*** информации должна содержать описание  
информационной системы и ее структурно-функциональных характеристик, а  
также описание угроз безопасности информации, включающее описание  
возможностей нарушителей (модель нарушителя), возможных уязвимостей  
информационной системы, способов реализации угроз безопасности  
информации и последствий от нарушения свойств безопасности информации  
([Приложение 4](#Приложение4)).

Для определения угроз безопасности информации и разработки модели  
угроз безопасности информации применяются методические документы,  
разработанные и утвержденные ФСТЭК России (Все методические документы  
можно найти на сайте ФСТЭК России: [http://fstec.ru/)](http://fstec.ru/).

* 1. Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной  
     системы и угроз безопасности информации, включенных в модель угроз  
     безопасности информации [(Глава I. Раздел 9)](#bookmark18).

Требования к системе защиты информации информационной системы  
включаются в техническое задание на создание информационной системы и  
(или) техническое задание (частное техническое задание) на создание системы  
защиты информации информационной системы, разрабатываемые с учетом  
ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

* цель и задачи обеспечения защиты информации в информационной  
  системе;
* класс защищенности информационной системы;
* перечень нормативных правовых актов, методических документов и  
  национальных стандартов, которым должна соответствовать информационная  
  система;
* перечень объектов защиты информационной системы;
* требования к мерам и средствам защиты информации,  
  применяемым в информационной системе;
* требования к защите информации при информационном  
  взаимодействии с иными информационными системами и информационно-  
  телекоммуникационными сетями, в том числе с информационными системами  
  уполномоченного лица, а также при применении вычислительных ресурсов  
  (мощностей), предоставляемых уполномоченным лицом для обработки  
  информации.

При определении требований к системе защиты информации  
информационной системы учитываются положения политик обеспечения  
информационной безопасности обладателя информации (заказчика) в случае их  
разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология.  
Методы и средства обеспечения безопасности. Системы менеджмента  
информационной безопасности. Требования», а также политик обеспечения  
информационной безопасности оператора и уполномоченного лица в части, не  
противоречащей политикам обладателя информации (заказчика).

1. Разработка системы защиты информации информационной системы
   1. Разработка ***системы защиты*** информации информационной  
      системы организуется обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы  
осуществляется в соответствии с техническим заданием на создание  
информационной системы и (или) техническим заданием (частным  
техническим заданием) на создание системы защиты информации  
информационной системы с учетом ГОСТ 34.601 «Информационная  
технология. Комплекс стандартов на автоматизированные системы.  
Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ  
Р 51583 и ГОСТ Р 51624 и в том числе включает:

* проектирование системы защиты информации информационной  
  системы;
* разработку эксплуатационной документации на систему защиты  
  информации информационной системы;
* макетирование и тестирование системы защиты информации  
  информационной системы (при необходимости).

Система защиты информации информационной системы не должна  
препятствовать достижению целей создания информационной системы и ее  
функционированию.

При разработке системы защиты информации информационной системы  
учитывается ее информационное взаимодействие с иными информационными  
системами и информационно-телекоммуникационными сетями, в том числе с  
информационными системами уполномоченного лица, а также применение  
вычислительных ресурсов (мощностей), предоставляемых уполномоченным  
лицом для обработки информации.

* 1. При проектировании системы защиты информации информационной системы:
* определяются типы субъектов доступа (пользователи, процессы и  
  иные субъекты доступа) и объектов доступа, являющихся объектами защиты  
  (устройства, объекты файловой системы, запускаемые и исполняемые модули,  
  объекты системы управления базами данных, объекты, создаваемые  
  прикладным программным обеспечением, иные объекты доступа);
* определяются методы управления доступом (дискреционный,  
  мандатный, ролевой или иные методы), типы доступа (чтение, запись,  
  выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности,  
  ролей и иных правил), подлежащие реализации в информационной системе;
* выбираются меры защиты информации, подлежащие реализации в  
  системе защиты информации информационной системы;
* определяются виды и типы средств защиты информации,  
  обеспечивающие реализацию технических мер защиты информации;
* определяется структура системы защиты информации  
  информационной системы, включая состав (количество) и места размещения ее  
  элементов;
* осуществляется выбор средств защиты информации,  
  сертифицированных на соответствие требованиям по безопасности  
  информации, с учетом их стоимости, совместимости с информационными  
  технологиями и техническими средствами, функций безопасности этих средств  
  и особенностей их реализации, а также класса защищенности информационной  
  системы;
* определяются параметры настройки программного обеспечения,  
  включая программное обеспечение средств защиты информации,  
  обеспечивающие реализацию мер защиты информации, а также устранение  
  возможных уязвимостей информационной системы, приводящих к  
  возникновению угроз безопасности информации;
* определяются меры защиты информации при информационном  
  взаимодействии с иными информационными системами и информационно-  
  телекоммуникационными сетями, в том числе с информационными системами  
  уполномоченного лица, а также при применении вычислительных ресурсов  
  (мощностей), предоставляемых уполномоченным лицом для обработки  
  информации.

Результаты проектирования системы защиты информации  
информационной системы отражаются в проектной документации (эскизном  
(техническом) проекте и (или) в рабочей документации) на информационную  
систему (систему защиты информации информационной системы),  
разрабатываемых с учетом ГОСТ 34.201 «Информационная технология.  
Комплекс стандартов на автоматизированные системы. Виды, комплектность и  
обозначение документов при создании автоматизированных систем» (далее -  
ГОСТ 34.201).

Проектная документация на информационную систему и (или) ее систему  
защиты информации подлежат согласованию с оператором информационной  
системы в случае, если он определен таковым в соответствии с

законодательством Российской Федерации к моменту окончания  
проектирования системы защиты информации информационной системы и не  
является заказчиком данной информационной системы.

При отсутствии необходимых средств защиты информации,  
сертифицированных на соответствие требованиям по безопасности  
информации, организуется разработка (доработка) средств защиты информации  
и их сертификация в соответствии с законодательством Российской Федерации  
или производится корректировка проектных решений по информационной  
системе и (или) ее системе защиты информации с учетом функциональных  
возможностей имеющихся сертифицированных средств защиты информации.

* 1. Разработка эксплуатационной документации на систему защиты  
     информации информационной системы осуществляется в соответствии с  
     техническим заданием на создание информационной системы и (или)  
     техническим заданием (частным техническим заданием) на создание системы  
     защиты информации информационной системы.

Эксплуатационная документация на систему защиты информации  
информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ  
34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

* структуры системы защиты информации информационной системы;
* состава, мест установки, параметров и порядка настройки средств  
  защиты информации, программного обеспечения и технических средств;
* правил эксплуатации системы защиты информации  
  информационной системы.

1. При макетировании и тестировании системы защиты информации  
   информационной системы в том числе осуществляются:

* проверка работоспособности и совместимости выбранных средств  
  защиты информации с информационными технологиями и техническими  
  средствами;
* проверка выполнения выбранными средствами защиты информации  
  требований к системе защиты информации информационной системы;
* корректировка проектных решений, разработанных при создании  
  информационной системы и (или) системы защиты информации  
  информационной системы;
* корректировка проектной и эксплуатационной документации на  
  систему защиты информации информационной системы.

Макетирование системы защиты информации информационной системы и ее тестирование может проводиться в том числе с использованием средств и методов моделирования информационных систем и технологий виртуализации.

1. **Внедрение системы защиты информации информационной системы**
   1. Внедрение системы защиты информации информационной системы  
      организуется обладателем информации (заказчиком).

Внедрение системы защиты информации информационной системы  
осуществляется в соответствии с проектной и эксплуатационной  
документацией на систему защиты информации информационной системы и в  
том числе включает:

* установку и настройку средств защиты информации в  
  информационной системе;
* разработку документов, определяющих правила и процедуры,  
  реализуемые оператором для обеспечения защиты информации в  
  информационной системе в ходе ее эксплуатации (далее - организационно-  
  распорядительные документы по защите информации);
* внедрение организационных мер защиты информации;
* предварительные испытания системы защиты информации  
  информационной системы;
* опытную эксплуатацию системы защиты информации  
  информационной системы;
* анализ уязвимостей информационной системы и принятие мер  
  защиты информации по их устранению;
* приемочные испытания системы защиты информации  
  информационной системы.

К внедрению системы защиты информации информационной системы  
привлекается оператор информационной системы в случае, если он определен  
таковым в соответствии с законодательством Российской Федерации к моменту  
внедрения системы защиты информации информационной системы и не  
является заказчиком данной информационной системы.

* 1. Установка и настройка средств защиты информации в  
     информационной системе должна проводиться в соответствии с  
     эксплуатационной документацией на систему защиты информации  
     информационной системы и документацией на средства защиты информации.
  2. Разрабатываемые организационно-распорядительные документы по  
     защите информации должны определять правила и процедуры:
* управления (администрирования) системой защиты информации  
  информационной системы;
* выявления инцидентов (одного события или группы событий),  
  которые могут привести к сбоям или нарушению функционирования  
  информационной системы и (или) к возникновению угроз безопасности  
  информации (далее - инциденты), и реагирования на них;
* управления конфигурацией аттестованной информационной  
  системы и системы защиты информации информационной системы;
* контроля (мониторинга) за обеспечением уровня защищенности  
  информации, содержащейся в информационной системе;
* защиты информации при выводе из эксплуатации информационной  
  системы или после принятия решения об окончании обработки информации.
  1. При внедрении организационных мер защиты информации  
     осуществляются:
* реализация правил разграничения доступа, регламентирующих  
  права доступа субъектов доступа к объектам доступа, и введение ограничений  
  на действия пользователей, а также на изменение условий эксплуатации,  
  состава и конфигурации технических средств и программного обеспечения;
* проверка полноты и детальности описания в организационно-  
  распорядительных документах по защите информации действий пользователей  
  и администраторов информационной системы по реализации организационных  
  мер защиты информации;
* отработка действий должностных лиц и подразделений,  
  ответственных за реализацию мер защиты информации.
  1. Предварительные испытания системы защиты информации  
     информационной системы проводятся с учетом ГОСТ 34.603  
     «Информационная технология. Виды испытаний автоматизированных систем»  
     (далее - ГОСТ 34.603) и включают проверку работоспособности системы  
     защиты информации информационной системы, а также принятие решения о  
     возможности опытной эксплуатации системы защиты информации  
     информационной системы.
  2. Опытная эксплуатация системы защиты информации  
     информационной системы проводится с учетом ГОСТ 34.603 и включает  
     проверку функционирования системы защиты информации информационной  
     системы, в том числе реализованных мер защиты информации, а также  
     готовность пользователей и администраторов к эксплуатации системы защиты  
     информации информационной системы.
  3. Анализ уязвимостей информационной системы проводится в целях  
     оценки возможности преодоления нарушителем системы защиты информации

информационной системы и предотвращения реализации угроз безопасности  
информации.

Анализ уязвимостей информационной системы включает анализ  
уязвимостей средств защиты информации, технических средств и  
программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется  
отсутствие известных уязвимостей средств защиты информации, технических  
средств и программного обеспечения, в том числе с учетом информации,  
имеющейся у разработчиков и полученной из других общедоступных  
источников, правильность установки и настройки средств защиты информации,  
технических средств и программного обеспечения, а также корректность  
работы средств защиты информации при их взаимодействии с техническими  
средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих  
к возникновению дополнительных угроз безопасности информации, проводится  
уточнение модели угроз безопасности информации и при необходимости  
принимаются дополнительные меры защиты информации, направленные на  
устранение выявленных уязвимостей или исключающие возможность  
использования нарушителем выявленных уязвимостей.

* 1. Приемочные испытания системы защиты информации  
     информационной системы проводятся с учетом ГОСТ 34.603 и включают  
     проверку выполнения требований к системе защиты информации  
     информационной системы в соответствии с техническим заданием на создание  
     информационной системы и (или) техническим заданием (частным  
     техническим заданием) на создание системы защиты информации  
     информационной системы.

1. Аттестация информационной системы и ввод ее в действие
   1. Аттестация информационной системы организуется обладателем  
      информации (заказчиком) или оператором и включает проведение комплекса  
      организационных и технических мероприятий (аттестационных испытаний), в  
      результате которых подтверждается соответствие системы защиты информации  
      информационной системы настоящим Рекомендациям.

Для аттестации информационной системы может привлекаться сторонняя  
организация, аккредитованная в качестве органа по аттестации объектов  
информатизации по требованиям безопасности информации в Системе  
сертификации средств защиты информации по требованиям безопасности  
информации № POCC RU.0001.01БИ00.

* 1. В качестве исходных данных, необходимых для аттестации  
     информационной системы, используются модель угроз безопасности  
     информации, акт классификации информационной системы, техническое  
     задание на создание информационной системы и (или) техническое задание  
     (частное техническое задание) на создание системы защиты информации  
     информационной системы, проектная и эксплуатационная документация на  
     систему защиты информации информационной системы, организационно-  
     распорядительные документы по защите информации, результаты анализа  
     уязвимостей информационной системы, материалы предварительных и  
     приемочных испытаний системы защиты информации информационной  
     системы, а также иные документы, разрабатываемые в соответствии с  
     настоящими Рекомендациями.
  2. Аттестация информационной системы проводится в соответствии с  
     программой и методиками аттестационных испытаний до начала обработки  
     информации, подлежащей защите в информационной системе. Для проведения  
     аттестации информационной системы применяются национальные стандарты, а  
     также методические документы, разработанные и утвержденные ФСТЭК  
     России.

По результатам аттестационных испытаний оформляются протоколы  
аттестационных испытаний, заключение о соответствии информационной  
системы требованиям о защите информации и аттестат соответствия в  
случае положительных результатов аттестационных испытаний.

* 1. Допускается аттестация информационной системы на основе  
     результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки  
     информации.

В этом случае распространение аттестата соответствия на другие  
сегменты информационной системы осуществляется при условии их  
соответствия сегментам информационной системы, прошедшим  
аттестационные испытания.

Сегмент считается соответствующим сегменту информационной  
системы, в отношении которого были проведены аттестационные испытания,  
если для указанных сегментов установлены одинаковые классы защищенности,  
угрозы безопасности информации, реализованы одинаковые проектные  
решения по информационной системе и ее системе защиты информации.

Соответствие сегмента, на который распространяется аттестат  
соответствия, сегменту информационной системы, в отношении которого были  
проведены аттестационные испытания, подтверждается в ходе приемочных  
испытаний информационной системы или сегментов информационной  
системы.

В сегментах информационной системы, на которые распространяется  
аттестат соответствия, оператором обеспечивается соблюдение  
эксплуатационной документации на систему защиты информации  
информационной системы и организационно-распорядительных документов по  
защите информации.

Особенности аттестации информационной системы на основе результатов  
аттестационных испытаний выделенного набора ее сегментов, а также условия  
и порядок распространения аттестата соответствия на другие сегменты  
информационной системы определяются в программе и методиках  
аттестационных испытаний, заключении и аттестате соответствия.

* 1. Повторная аттестация информационной системы осуществляется в  
     случае окончания срока действия аттестата соответствия или повышения  
     класса защищенности информационной системы. При увеличении состава  
     угроз безопасности информации или изменения проектных решений,  
     реализованных при создании системы защиты информации информационной  
     системы, проводятся дополнительные аттестационные испытания в рамках  
     действующего аттестата соответствия.
  2. Ввод в действие информационной системы осуществляется в  
     соответствии с законодательством Российской Федерации об информации,  
     информационных технологиях и о защите информации и с учетом ГОСТ 34.601  
     и при наличии аттестата соответствия.

1. Обеспечение защиты информации в ходе эксплуатации аттестованной

информационной системы

* 1. Обеспечение защиты информации в ходе эксплуатации аттестованной  
     информационной системы осуществляется оператором в соответствии с  
     эксплуатационной документацией на систему защиты информации и  
     организационно-распорядительными документами по защите информации и в  
     том числе включает:
* управление (администрирование) системой защиты информации  
  информационной системы;
* выявление инцидентов и реагирование на них
* управление конфигурацией аттестованной информационной  
  системы и ее системы защиты информации;
* контроль (мониторинг) за обеспечением уровня защищенности  
  информации, содержащейся в информационной системе.
  1. В ходе управления (администрирования) системой защиты  
     информации информационной системы осуществляются:
* заведение и удаление учетных записей пользователей, управление  
  полномочиями пользователей информационной системы и поддержание правил  
  разграничения доступа в информационной системе;
* управление средствами защиты информации в информационной  
  системе, в том числе параметрами настройки программного обеспечения,  
  включая программное обеспечение средств защиты информации, управление  
  учетными записями пользователей, восстановление работоспособности средств  
  защиты информации, генерацию, смену и восстановление паролей;
* установка обновлений программного обеспечения, включая  
  программное обеспечение средств защиты информации, выпускаемых  
  разработчиками (производителями) средств защиты информации или по их  
  поручению;
* централизованное управление системой защиты информации  
  информационной системы (при необходимости);
* регистрация и анализ событий в информационной системе,  
  связанных с защитой информации (далее - события безопасности);
* информирование пользователей об угрозах безопасности  
  информации, о правилах эксплуатации системы защиты информации  
  информационной системы и отдельных средств защиты информации, а также  
  их обучение;
* сопровождение функционирования системы защиты информации  
  информационной системы в ходе ее эксплуатации, включая корректировку  
  эксплуатационной документации на нее и организационно-распорядительных  
  документов по защите информации;
  1. В ходе выявления инцидентов и реагирования на них  
     осуществляются:
* определение лиц, ответственных за выявление инцидентов и  
  реагирование на них;
* обнаружение и идентификация инцидентов, в том числе отказов в  
  обслуживании, сбоев (перезагрузок) в работе технических средств,  
  программного обеспечения и средств защиты информации, нарушений правил  
  разграничения доступа, неправомерных действий по сбору информации,  
  внедрений вредоносных компьютерных программ (вирусов) и иных событий,  
  приводящих к возникновению инцидентов;
* своевременное информирование лиц, ответственных за выявление  
  инцидентов и реагирование на них, о возникновении инцидентов в  
  информационной системе пользователями и администраторами;
* анализ инцидентов, в том числе определение источников и причин  
  возникновения инцидентов, а также оценка их последствий;
* планирование и принятие мер по устранению инцидентов, в том  
  числе по восстановлению информационной системы и ее сегментов в случае  
  отказа в обслуживании или после сбоев, устранению последствий нарушения  
  правил разграничения доступа, неправомерных действий по сбору информации,  
  внедрения вредоносных компьютерных программ (вирусов) и иных событий,  
  приводящих к возникновению инцидентов;
* планирование и принятие мер по предотвращению повторного  
  возникновения инцидентов.
  1. В ходе управления конфигурацией аттестованной информационной  
     системы и ее системы защиты информации осуществляются:
* поддержание конфигурации информационной системы и ее  
  системы защиты информации (структуры системы защиты информации  
  информационной системы, состава, мест установки и параметров настройки  
  средств защиты информации, программного обеспечения и технических  
  средств) в соответствии с эксплуатационной документацией на систему защиты  
  информации (поддержание базовой конфигурации информационной системы и  
  ее системы защиты информации);
* определение лиц, которым разрешены действия по внесению  
  изменений в базовую конфигурацию информационной системы и ее системы  
  защиты информации;
* управление изменениями базовой конфигурации информационной  
  системы и ее системы защиты информации, в том числе определение типов  
  возможных изменений базовой конфигурации информационной системы и ее  
  системы защиты информации, санкционирование внесения изменений в  
  базовую конфигурацию информационной системы и ее системы защиты  
  информации, документирование действий по внесению изменений в базовую  
  конфигурацию информационной системы и ее системы защиты информации,  
  сохранение данных об изменениях базовой конфигурации информационной  
  системы и ее системы защиты информации, контроль действий по внесению  
  изменений в базовую конфигурацию информационной системы и ее системы  
  защиты информации;
* анализ потенциального воздействия планируемых изменений в  
  базовой конфигурации информационной системы и ее системы защиты  
  информации на обеспечение защиты информации, возникновение  
  дополнительных угроз безопасности информации и работоспособность  
  информационной системы;
* определение параметров настройки программного обеспечения,  
  включая программное обеспечение средств защиты информации, состава и  
  конфигурации технических средств и программного обеспечения до внесения  
  изменений в базовую конфигурацию информационной системы и ее системы  
  защиты информации;
* внесение информации (данных) об изменениях в базовой  
  конфигурации информационной системы и ее системы защиты информации в  
  эксплуатационную документацию на систему защиты информации  
  информационной системы;
* принятие решения по результатам управления конфигурацией о  
  повторной аттестации информационной системы или проведении  
  дополнительных аттестационных испытаний.
  1. В ходе контроля (мониторинга) за обеспечением уровня  
     защищенности информации, содержащейся в информационной системе,  
     осуществляются:
* контроль за событиями безопасности и действиями пользователей в  
  информационной системе;
* контроль (анализ) защищенности информации, содержащейся в  
  информационной системе;
* анализ и оценка функционирования системы защиты информации  
  информационной системы, включая выявление, анализ и устранение  
  недостатков в функционировании системы защиты информации  
  информационной системы;
* периодический анализ изменения угроз безопасности информации в  
  информационной системе, возникающих в ходе ее эксплуатации, и принятие  
  мер защиты информации в случае возникновения новых угроз безопасности  
  информации;
* документирование процедур и результатов контроля (мониторинга)  
  за обеспечением уровня защищенности информации, содержащейся в  
  информационной системе;
* принятие решения по результатам контроля (мониторинга) за  
  обеспечением уровня защищенности информации о доработке (модернизации)  
  системы защиты информации информационной системы, повторной аттестации  
  информационной системы или проведении дополнительных аттестационных  
  испытаний.

1. **Обеспечение защиты информации при выводе из эксплуатации  
   аттестованной информационной системы или после принятия решения об  
   окончании обработки информации**
   1. Обеспечение защиты информации при выводе из эксплуатации  
      аттестованной информационной системы или после принятия решения об  
      окончании обработки информации осуществляется оператором в соответствии  
      с эксплуатационной документацией на систему защиты информации  
      информационной системы и организационно-распорядительными документами  
      по защите информации и в том числе включает:

* архивирование информации, содержащейся в информационной  
  системе;
* уничтожение (стирание) данных и остаточной информации с  
  машинных носителей информации и (или) уничтожение машинных носителей  
  информации.
  1. Архивирование информации, содержащейся в информационной  
     системе, должно осуществляться при необходимости дальнейшего  
     использования информации в деятельности оператора.
  2. Уничтожение (стирание) данных и остаточной информации с  
     машинных носителей информации производится при необходимости передачи  
     машинного носителя информации другому пользователю информационной  
     системы или в сторонние организации для ремонта, технического  
     обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на  
которых осуществлялись хранение и обработка информации, осуществляется  
физическое уничтожение этих машинных носителей информации.

Организацию всех работ осуществляет структурное подразделение или  
должностное лицо (работник), ответственные за защиту информации.

1. Определение класса защищенности информационной системы
   1. Класс защищенности информационной системы (первый класс (К1),  
      второй класс (К2), третий класс (К3), четвертый класс (К4)) определяется в  
      зависимости от уровня значимости информации (УЗ), обрабатываемой в этой  
      информационной системе, и масштаба информационной системы  
      (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб  
системы].

* 1. Уровень значимости информации определяется степенью  
     возможного ущерба для обладателя информации (заказчика) и (или) оператора  
     от нарушения конфиденциальности (неправомерные доступ, копирование,  
     предоставление или распространение), целостности (неправомерные  
     уничтожение или модифицирование) или доступности (неправомерное  
     блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень  
ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации  
(заказчиком) и (или) оператором самостоятельно экспертным или иными  
методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности  
информации (конфиденциальности, целостности, доступности) возможны  
существенные негативные последствия в социальной, политической,  
международной, экономической, финансовой или иных областях деятельности  
и (или) информационная система и (или) оператор (обладатель информации) не  
могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности  
информации (конфиденциальности, целостности, доступности) возможны  
умеренные негативные последствия в социальной, политической,  
международной, экономической, финансовой или иных областях деятельности  
и (или) информационная система и (или) оператор (обладатель информации) не  
могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности  
информации (конфиденциальности, целостности, доступности) возможны  
незначительные негативные последствия в социальной, политической,  
международной, экономической, финансовой или иных областях деятельности  
и (или) информационная система и (или) оператор (обладатель информации)  
могут выполнять возложенные на них функции с недостаточной  
эффективностью или выполнение функций возможно только с привлечением  
дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ ***1***), если хотя бы для  
одного из свойств безопасности информации (конфиденциальности,  
целостности, доступности) определена высокая степень ущерба. Информация  
имеет средний уровень значимости (***УЗ 2***), если хотя бы для одного из свойств  
безопасности информации (конфиденциальности, целостности, доступности)  
определена средняя степень ущерба и нет ни одного свойства, для которого  
определена высокая степень ущерба. Информация имеет низкий уровень  
значимости (УЗ 3), если для всех свойств безопасности информации  
(конфиденциальности, целостности, доступности) определены низкие степени  
ущерба.

Информация имеет минимальный уровень значимости (***УЗ 4***), если  
обладателем информации (заказчиком) и (или) оператором степень ущерба от  
нарушения свойств безопасности информации (конфиденциальности,  
целостности, доступности) не может быть определена, но при этом информация  
подлежит защите в соответствии с законодательством Российской Федерации.

При обработке в информационной системе двух и более видов  
информации (служебная тайна, налоговая тайна и иные установленные  
законодательством Российской Федерации виды информации ограниченного  
доступа) уровень значимости информации (УЗ) определятся отдельно для  
каждого вида информации. Итоговый уровень значимости информации,  
обрабатываемой в информационной системе, устанавливается по наивысшим  
значениям степени возможного ущерба, определенным для  
конфиденциальности, целостности, доступности информации каждого вида  
информации.

* 1. Информационная система имеет федеральный масштаб, если она  
     функционирует на территории Российской Федерации (в пределах  
     федерального округа) и имеет сегменты в субъектах Российской Федерации,  
     муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она  
функционирует на территории субъекта Российской Федерации и имеет  
сегменты в одном или нескольких муниципальных образованиях и (или)  
подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она  
функционирует на объектах одного федерального органа государственной  
власти, органа государственной власти субъекта Российской Федерации,  
муниципального образования и (или) организации и не имеет сегментов в  
территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

* 1. Класс защищенности информационной системы определяется в  
     соответствии с таблицей 1.

Таблица 1. Класс защищенности информационной системы

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень  значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

*Пример классификации информационной системы*

Описание примера:

Комитетом по информатизации создается реестр  
нормативно-правовых актов Саратовской области. В соответствии с Приказом  
ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о  
защите информации, не составляющей государственную тайну, содержащейся в  
государственных информационных системах» необходимо произвести  
классификацию данной информационной системы.

Классификация примера:

Приведенная система имеет объектовый масштаб, она функционирует на  
объектах одного органа государственной власти субъекта Российской  
Федерации (Департамент связи и массовых коммуникаций Саратовской  
области), и не имеет сегментов в территориальных органах,  
представительствах, филиалах, подведомственных и иных организациях.

В информационной системе обрабатывается один вид информации:  
общедоступная информация.

Для каждого из свойств уровня значимости информации  
(конфиденциальность, целостность, доступность) устанавливается низкая  
степень возможного ущерба. В результате их нарушения возможны  
незначительные негативные последствия в социальной, политической,  
экономической или иных областях деятельности и информационная система и  
оператор (обладатель информации) могут выполнять возложенные на них  
функции с недостаточной эффективностью. На основании этого в  
информационной системе устанавливается 3 уровень значимости (УЗ 3)  
информации.

По результатам анализа исходных данных информационной системе  
«Реестр нормативно-правовых актов Саратовской области» присваивается 3  
класс защищенности (К3).

1. Требования к мерам защиты информации, содержащейся в

информационной системе

9.1 Организационные и технические меры защиты информации,  
реализуемые в информационной системе в рамках ее системы защиты  
информации, в зависимости от угроз безопасности информации, используемых  
информационных технологий и структурно-функциональных характеристик  
информационной системы должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов  
  доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* доступность информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и  
  передачи данных.

Состав мер защиты информации и их базовые наборы для  
соответствующих классов защищенности информационных систем приведены  
в таблице 3.

1. Меры по идентификации и аутентификации субъектов доступа и  
   объектов доступа должны обеспечивать присвоение субъектам и объектам  
   доступа уникального признака (идентификатора), сравнение предъявляемого  
   субъектом (объектом) доступа идентификатора с перечнем присвоенных  
   идентификаторов, а также проверку принадлежности субъекту (объекту)  
   доступа предъявленного им идентификатора (подтверждение подлинности).
2. Меры по управлению доступом субъектов доступа к объектам  
   доступа должны обеспечивать управление правами и привилегиями субъектов  
   доступа, разграничение доступа субъектов доступа к объектам доступа на  
   основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих  
   правил.
3. Меры по ограничению программной среды должны обеспечивать  
   установку и (или) запуск только разрешенного к использованию в  
   информационной системе программного обеспечения или исключать  
   возможность установки и (или) запуска запрещенного к использованию в  
   информационной системе программного обеспечения.

Перечисленные меры осуществляются с помощью введения системы  
разграничения прав доступа пользователей и применения групповых политик.

1. Меры по защите машинных носителей информации (средства  
   обработки (хранения) информации, съемные машинные носители информации)  
   должны исключать возможность несанкционированного доступа к машинным  
   носителям и хранящейся на них информации, а также несанкционированное  
   использование съемных машинных носителей информации.

Реализуются с помощью введения «Регламента учета средств защиты  
информации, эксплуатационной и технической документации к ним,  
электронных носителей» ([Приложение 30](#Приложение30). Пример с ПДн) и «Списка лиц,  
допущенных в защищаемое помещение» ([Приложение 5](#Приложение5)).

1. Меры по регистрации событий безопасности должны обеспечивать  
   сбор, запись, хранение и защиту информации о событиях безопасности в  
   информационной системе, а также возможность просмотра и анализа  
   информации о таких событиях и реагирование на них.

Данные меры реализуются с помощью электронного журнала  
регистрации и учета событий безопасности.

1. Меры по антивирусной защите должны обеспечивать обнаружение  
   в информационной системе компьютерных программ либо иной компьютерной  
   информации, предназначенной для несанкционированного уничтожения,  
   блокирования, модификации, копирования компьютерной информации или  
   нейтрализации средств защиты информации, а также реагирование на  
   обнаружение этих программ и информации.

Осуществляются с использованием антивирусного программного  
комплекса.

1. Меры по обнаружению (предотвращению) вторжений должны  
   обеспечивать обнаружение действий в информационной системе,  
   направленных на преднамеренный несанкционированный доступ к  
   информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования  
   доступа к информации, а также реагирование на эти действия.

Осуществляются с использованием систем обнаружения вторжения.

1. Меры по контролю (анализу) защищенности информации должны  
   обеспечивать контроль уровня защищенности информации, содержащейся в  
   информационной системе, путем проведения мероприятий по анализу  
   защищенности информационной системы и тестированию ее системы защиты  
   информации.

Данные меры осуществляются с помощью средств анализа защищенности

1. Меры по обеспечению целостности информационной системы и  
   информации должны обеспечивать обнаружение фактов несанкционированного  
   нарушения целостности информационной системы и содержащейся в ней  
   информации, а также возможность восстановления информационной системы и  
   содержащейся в ней информации.

Данные меры осуществляются с помощью средств фиксации и контроля  
исходного состояния программного комплекса.

1. Меры по обеспечению доступности информации должны  
   обеспечивать авторизованный доступ пользователей, имеющих права по такому  
   доступу, к информации, содержащейся в информационной системе, в штатном  
   режиме функционирования информационной системы.

Способы реализации, приведенные в п. 9.2.3.

1. Меры по защите среды виртуализации должны исключать  
   несанкционированный доступ к информации, обрабатываемой в виртуальной  
   инфраструктуре, и к компонентам виртуальной инфраструктуры, а также  
   воздействие на информацию и компоненты, в том числе к средствам  
   управления виртуальной инфраструктурой, монитору виртуальных машин  
   (гипервизору), системе хранения данных (включая систему хранения образов  
   виртуальной инфраструктуры), сети передачи данных через элементы  
   виртуальной или физической инфраструктуры, гостевым операционным  
   системам, виртуальным машинам (контейнерам), системе и сети репликации,  
   терминальным и виртуальным устройствам, а также системе резервного  
   копирования и создаваемым ею копиям.
2. Меры по защите технических средств должны исключать  
   несанкционированный доступ к стационарным техническим средствам,  
   обрабатывающим информацию, средствам, обеспечивающим  
   функционирование информационной системы (далее − средства обеспечения  
   функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту  
   информации, представленной в виде информативных электрических сигналов и  
   физических полей.
3. Меры по защите информационной системы, ее средств, систем  
   связи и передачи данных должны обеспечивать защиту информации при  
   взаимодействии информационной системы или ее отдельных сегментов с  
   иными информационными системами и информационно-  
   телекоммуникационными сетями посредством применения архитектуры  
   информационной системы, проектных решений по ее системе защиты  
   информации, направленных на обеспечение защиты информации.

Все перечисленные меры реализуются с использованием  
сертифицированных средств защиты информации. Список СЗИ доступен в  
Государственном реестре сертифицированных средств защиты информации N  
РОСС RU.0001.01БИ00 на [сайте ФСТЭК России.](http://fstec.ru/sistema-sertifikatsii-tzi/153-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00)

1. Выбор мер защиты информации для их реализации в  
   информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для  
  установленного класса защищенности информационной системы в  
  соответствии с базовыми наборами мер защиты информации, приведенными в  
  таблице 3;
* адаптацию базового набора мер защиты информации  
  применительно к структурно-функциональным характеристикам  
  информационной системы, информационным технологиям, особенностям  
  функционирования информационной системы (в том числе  
  предусматривающую исключение из базового набора мер защиты информации  
  мер, непосредственно связанных с информационными технологиями, не  
  используемыми в информационной системе, или структурно-функциональными  
  характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты  
  информации с учетом не выбранных ранее мер защиты информации,  
  приведенных в таблице 3, в результате чего определяются меры защиты  
  информации, обеспечивающие блокирование (нейтрализацию) всех угроз  
  безопасности информации, включенных в модель угроз безопасности  
  информации;
* дополнение уточненного адаптированного базового набора мер  
  защиты информации мерами, обеспечивающими выполнение требований о  
  защите информации, установленными иными нормативными правовыми

актами в области защиты информации, в том числе в области защиты  
персональных данных.

Для выбора мер защиты информации для соответствующего класса  
защищенности информационной системы применяются методические  
документы, разработанные и утвержденные ФСТЭК России.

1. В информационной системе соответствующего класса защищенности  
   в рамках ее системы защиты информации должны быть реализованы меры  
   защиты информации, выбранные в соответствии с пунктом 9.3 и  
   обеспечивающие блокирование (нейтрализацию) всех угроз безопасности  
   информации.

При этом в информационной системе должен быть, как минимум,  
реализован адаптированный базовый набор мер защиты информации,  
соответствующий установленному классу защищенности информационной  
системы.

1. При невозможности реализации в информационной системе в рамках  
   ее системы защиты информации отдельных выбранных мер защиты  
   информации на этапах адаптации базового набора мер защиты информации или  
   уточнения адаптированного базового набора мер защиты информации могут  
   разрабатываться иные (компенсирующие) меры защиты информации,  
   обеспечивающие адекватное блокирование (нейтрализацию) угроз  
   безопасности информации.

В этом случае в ходе разработки системы защиты информации  
информационной системы должно быть проведено обоснование применения  
компенсирующих мер защиты информации, а при аттестационных испытаниях  
оценена достаточность и адекватность данных компенсирующих мер для  
блокирования (нейтрализации) угроз безопасности информации.

1. Меры защиты информации выбираются и реализуются в  
   информационной системе в рамках ее системы защиты информации с учетом  
   угроз безопасности информации применительно ко всем объектам и субъектам  
   доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе  
   в среде виртуализации и облачных вычислений.
2. Выбранные и реализованные в информационной системе в рамках ее  
   системы защиты информации меры защиты информации должны обеспечивать:

в информационных системах 1 класса защищенности - нейтрализацию  
(блокирование) угроз безопасности информации, связанных с действиями  
нарушителя с высоким потенциалом;

в информационных системах 2 класса защищенности - нейтрализацию  
(блокирование) угроз безопасности информации, связанных с действиями  
нарушителя с потенциалом не ниже среднего;

в информационных системах 3 и 4 классов защищенности -  
нейтрализацию (блокирование) угроз безопасности информации, связанных с  
действиями нарушителя с низким потенциалом.

Потенциал нарушителя определяется в ходе оценки его возможностей,  
проводимой при определении угроз безопасности информации в соответствии с  
пунктом 2.4 Главы I.

Оператором может быть принято решение о применении в  
информационной системе соответствующего класса защищенности мер защиты  
информации, обеспечивающих защиту от угроз безопасности информации,  
реализуемых нарушителем с более высоким потенциалом.

1. Технические меры защиты информации реализуются посредством  
   применения средств защиты информации, имеющих необходимые функции  
   безопасности (Таблица 2).

В этом случае в информационных системах 1 и 2 класса защищенности  
применяются:

* средства вычислительной техники не ниже 5 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 4 класса;
* межсетевые экраны не ниже 3 класса в случае взаимодействия  
  информационной системы с информационно-телекоммуникационными сетями  
  международного информационного обмена и не ниже 4 класса в случае  
  отсутствия взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена.

В информационных системах 3 класса защищенности применяются:

* средства вычислительной техники не ниже 5 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 4 класса в случае взаимодействия информационной системы с  
  информационно-телекоммуникационными сетями международного  
  информационного обмена и не ниже 5 класса в случае отсутствия  
  взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена;
* межсетевые экраны не ниже 3 класса в случае взаимодействия  
  информационной системы с информационно-телекоммуникационными сетями  
  международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена.

В информационных системах 4 класса защищенности применяются:

* средства вычислительной техники не ниже 5 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 5 класса;
* межсетевые экраны не ниже 4 класса.

В информационных системах 1 и 2 классов защищенности применяются  
средства защиты информации, программное обеспечение которых прошло  
проверку не ниже чем по 4 уровню контроля отсутствия недекларированных  
возможностей.

Таблица 2. Тип применяемых средств защиты информации, в  
зависимости от уровня защищенности персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Средства защиты информации** | **Классы защищенности** | | | |
| **1** | **2** | **3** | **4** |
| Средства  вычислительной  техники | 5+ | 5+ | 5+ | 5+ |
| Системы  обнаружения  вторжений | 4+ | 4+ | 4+ / 5+\* | 5+ |
| Средства  антивирусной  защиты | 4 + | 4 + | 4+ / 5+\* | 5+ |
| Межсетевые  экраны | 3 + / 4+\* | 3 + / 4+\* | 3 + / 4+\* | 4+ |
|  | | | | |
| Недекларированные  возможности | 4+ | 4+ | - | - |

\* (в случае актуальности угроз 1-го или 2-го типа или взаимодействия  
ИС с информационно-телекоммуникационными сетям международного  
информационного обмена) /

(в случае актуальности угроз 3-го типа и отсутствия взаимодействия с информационно-телекоммуникационными сетям международного

информационного обмена)

1. В случае обработки в информационной системе информации,  
   содержащей персональные данные, реализуемые в соответствии с пунктами 9.3  
   и 9.4:

* для информационной системы 1 класса защищенности  
  обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных;
* для информационной системы 2 класса защищенности  
  обеспечивают 2, 3 и 4 уровни защищенности персональных данных\*;
* для информационной системы 3 класса защищенности  
  обеспечивают 3 и 4 уровни защищенности персональных данных\*;
* для информационной системы 4 класса защищенности,  
  обеспечивают 4 уровень защищенности персональных данных\*.

1. При использовании в информационных системах новых  
   информационных технологий и выявлении дополнительных угроз безопасности  
   информации, для которых не определены меры защиты информации, должны  
   разрабатываться компенсирующие меры в соответствии с пунктом 9.5.

* Устанавливается в соответствии с Требованиями к защите  
  персональных данных при их обработке в информационных системах  
  персональных данных, утвержденными постановлением Правительства  
  Российской Федерации от 1 ноября 2012 г. № 1119

Таблица 3. Состав мер защиты информации и их базовые наборы для  
соответствующего класса защищенности информационной системы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Условное обозначе- ние и номер меры** | **Меры защиты информации в информационных**  **системах** | **Классы**  **защищенности**  **информационной**  **системы** | | | |
| **4** | **3** | **2** | **1** |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |  |  | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |  |  |  |  |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |  |  | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |  | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |  | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации |  |  |  |  |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |  |  |  |  |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |  |  |  | + |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |  | + | + | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + | + | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |  |  |  |  |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |  |  | + | + |
| III. Ограничение программной среды (ОПС) | | | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за |  |  |  | + |
|  | запуском компонентов программного обеспечения |  |  |  |  |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |  |  | + | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | + | + | + | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |  |  |  |  |
| IV. Защита машинных носителей информации (ЗНИ) | | | | | |
| ЗНИ.1 | Учет машинных носителей информации | + | + | + | + |
| ЗНИ.2 | Управление доступом к машинным носителям информации | + | + | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |  |  |  |  |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |  |  |  |  |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |  |  | + | + |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |  |  |  |  |
| ЗНИ.7 | Контроль подключения машинных носителей информации |  |  |  |  |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) | + | + | + | + |
| V. Регистрация событий безопасности (РСБ) | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | + | + | + | + |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + | + | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | + | + | + | + |
| РСБ.7 | Защита информации о событиях безопасности | + | + | + | + |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |  |  |  |  |
| VI. Антивирусная защита (АВЗ) | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + |
| VII. Обнаружение вторжений (СОВ) | | | | | |
| СОВ.1 | Обнаружение вторжений |  |  | + | + |
| СОВ.2 | Обновление базы решающих правил |  |  | + | + |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |  | + | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования |  | + | + | + |
|  | программного обеспечения и средств защиты информации |  |  |  |  |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |  | + | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |  | + | + | + |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |  |  | + | + |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |  |  |  |  |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | + | + | + | + |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |  |  | + | + |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |  |  |  |  |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |  |  |  | + |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |  |  |  |  |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |  |  |  |  |
| X. Обеспечение доступности информации (ОДТ) | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств |  |  |  | + |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |  |  |  | + |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  | + | + |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |  |  | + | + |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |  |  | + | + |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |  |  |  |  |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |  |  | + | + |
| XI. Защита среды виртуализации (ЗСВ) | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |  | + | + | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной |  |  | + | + |
|  | инфраструктуры, а также по периметру виртуальной инфраструктуры |  |  |  |  |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |  |  |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |  |  | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |  |  | + | + |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |  |  | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |  | + | + | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |  |  | + | + |
| XII. Защита технических средств (ЗТС) | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |  |  |  |  |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | + | + | + | + |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены | + | + | + | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |  |  |  | + |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной  системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |  |  | + | + |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |  |  |  |  |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + | + | + |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |  |  |  |  |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | + | + | + | + |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |  |  | + | + |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |  |  | + | + |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |  |  | + | + |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |  |  |  |  |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |  |  | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |  |  | + | + |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |  |  | + | + |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |  |  |  |  |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |  |  | + | + |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |  |  | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |  |  |  |  |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |  |  |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |  | + | + | + |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |  |  |  | + |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |  |  | + | + |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |  |  | + | + |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |  |  | + | + |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |  |  |  |  |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |  |  |  |  |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз |  |  |  |  |
|  | безопасности информации |  |  |  |  |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |  |  |  |  |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации,  в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |  |  |  |  |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |  | + | + | + |

«+» - мера защиты информации включена в базовый набор мер для  
соответствующего класса защищенности информационной системы.

Меры защиты информации, не обозначенные знаком «+», применяются  
при адаптации базового набора мер и уточнении адаптированного базового  
набора мер, а также при разработке компенсирующих мер защиты информации  
в информационной системе соответствующего класса защищенности.

1. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИ  
   АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ  
   В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ ПРАВИТЕЛЬСТВА ОБЛАСТИ, ИСПОЛНИТЕЛЬНЫХ ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ ОБЛАСТИ, ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ ОБЛАСТИ И ПОДВЕДОМСТВЕННЫХ ИМ ОРГАНИЗАЦИЯХ САРАТОВСКОЙ

ОБЛАСТИ

**ВВЕДЕНИЕ**

В настоящее время, на территории Российской Федерации  
осуществляется государственное регулирование в области обеспечения  
безопасности персональных данных (далее - ПДн). Правовое регулирование  
вопросов обработки ПДн осуществляется в соответствии с Конституцией  
Российской Федерации и международными договорами Российской Федерации,  
на основании вступившего в силу с 2007 года Федерального закона от 27 июля  
2006 г. № 152-ФЗ «О персональных данных» и принятых во исполнение его  
положений, нормативно-правовых актов и методических документов.

Настоящий документ представляет собой методические рекомендации,  
разъясняющие последовательность действий для приведения информационных  
систем персональных данных (далее - ИСПДн) в соответствие требованиям  
законодательства Российской Федерации.

Данные методические рекомендации разработаны на основании  
Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных  
данных», Постановления Правительства РФ от 21.03.2012 № 211 "Об  
утверждении перечня мер, направленных на обеспечение выполнения  
обязанностей, предусмотренных Федеральным законом "О персональных  
данных" и принятыми в соответствии с ним нормативными правовыми актами,  
операторами, являющимися государственными или муниципальными  
органами», Постановления Правительства Российской Федерации от 1 ноября  
2012 г. № 1119 «Об утверждении требований к защите персональных данных  
при их обработке в информационных системах персональных данных»,  
Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава  
и содержания организационных и технических мер по обеспечению  
безопасности персональных данных при их обработке в информационных  
системах персональных данных» и с учетом иных нормативных и  
методических документов ФСТЭК России, ФСБ России и Роскомнадзора.

Настоящие Рекомендации применяются наряду с Рекомендациями по  
требованиям защиты информации, не составляющей государственную тайну,  
содержащейся в государственных информационных системах ([Глава I](#Глава1)).

В настоящем документе не рассматриваются вопросы обеспечения  
безопасности персональных данных, отнесенных в установленном порядке к  
сведениям, составляющим государственную тайну, а также меры, связанные с  
применением шифровальных (криптографических) средств защиты информации.

Обеспечение безопасности ПДн при их обработке без использования  
средств автоматизации, осуществляется в соответствии с требованиями  
постановления Правительства Российской Федерации от 15 сентября 2008 г. №  
687«Об утверждении Положения об особенностях обработки персональных  
данных, осуществляемой без использования средств автоматизации».

1. **Понятие и состав персональных данных**
   1. Персональные данные - любая информация, относящаяся к  
      определенному или определяемому на основании такой информации  
      физическому лицу (субъекту персональных данных.
   2. ПДн могут включать в себя:

* фамилия, имя, отчество;
* сведения о смене фамилии, имени, отчества;
* пол;
* фотографическое изображение работника;
* табельный номер работника;
* число, месяц, год рождения;
* место рождения;
* гражданство;
* паспортные данные;
* адрес места жительства по паспорту;
* адрес места жительства фактический;
* номера контактных телефонов;
* адрес электронной почты;
* индивидуальный номер налогоплательщика;
* страховой номер индивидуального лицевого счета застрахованного

лица;

* характеристика работника;
* сведения об испытательном сроке работника;
* сведения о воинском учете;
* данные, содержащиеся в военном билете;
* сведения о знании иностранного языка;
* сведения о повышении квалификации и профессиональной  
  переподготовке, наличии специальных знаний;
* сведения о профессиональной пригодности;
* сведения о фактах прохождения профессиональных медицинских  
  осмотров;
* сведения об инвалидности;
* сведения о наградах, поощрениях, почетных званиях;
* сведения о льготах;
* сведения о месте работы (должность, структурное подразделение,

категория квалификации, период работы, стаж, сведения об аттестации);

* учетная степень, звание;
* информация о трудовой деятельности;
* данные о предыдущих местах работы;
* семейное положение;
* сведения о близких родственниках (фамилия, имя, отчество,  
  степень родства, год рождения, место работы, должность, сведения о доходах,  
  номер контактного телефона);
* сведения об образовании;
* сведения об отпуске;
* сведения о командировках;
* сведения о временной нетрудоспособности;
* доходы;
* сведения об удержаниях из заработной платы;
* сведения о выданных подотчетных суммах;
* сведения о лицевом счете в банке;
* сведения о выданных банковских картах;
* сведения о выплачиваемых алиментах;
* сведения об исправительных работах;
* основание прекращения трудового договора (увольнения);
  1. Информация о ПДн может содержаться:
* на бумажных носителях;
* на электронных носителях;
* в информационно-телекоммуникационных сетях и ИСПДн.

1.4. Оператор самостоятельно устанавливает способы обработки ПДн в  
зависимости от целей такой обработки и материально-технических  
возможностей.

1.5. При обработке персональных данных с использованием средств  
вычислительной техники должностные лица, осуществляющие такую  
обработку (пользователи объектов вычислительной техники), должны быть  
ознакомлены под роспись с локальными нормативными актами Оператора,  
устанавливающими порядок использования объектов вычислительной техники.

1. ПДн работников Оператора могут содержаться в следующих  
   документах (копиях указанных документов):

* приказы;
* служебные записки;
* заявления, обращения работников;
* доверенности;
* служебные задания для направления в командировку;
* командировочные удостоверения;
* авансовые отчеты;
* расчетные листки;
* расходные кассовые ордеры;
* справки о выплаченных алиментах;
* реестры на получение заработной платы;
* опись документов в кредитном досье по банковским картам в  
  рамках зарплатных проектов;
* графики отпусков;
* табели учета рабочего времени;
* расчетные ведомости заработной платы;
* лицевые счета;
* справки о сумме заработной платы;
* листки нетрудоспособности;
* справки о сумме заработной платы, иных выплат и вознаграждений,  
  на которую были начислены страховые взносы на обязательное социальное  
  страхование на случай временной нетрудоспособности и в связи с  
  материнством, за два календарных года, предшествующих году прекращения  
  работы (службы, иной деятельности) или году обращения за справкой, и  
  текущий календарный год;
* справки о доходах физических лиц;
* реестр сведений о начисленных и уплаченных страховых взносах на  
  обязательное пенсионное страхование застрахованных лиц (СЗВ-6-2);
* трудовые договоры работников;
* договоры о временном трудоустройстве;
* личные карточки работников;
* Формы Т1 -Т11а;
* фотографические изображения;
* копии дипломов, сертификатов, удостоверений, аттестатов,  
  нагрудные знаки;
* документы об аттестации (переаттестации) работников;
* копии свидетельств о повышении квалификации;
* копии свидетельств о постановке на учет физического лица в

налоговом органе на территории Российской Федерации;

* копии страховых свидетельств государственного пенсионного  
  страхования;
* копии паспортов работников;
* копии свидетельств о заключении/расторжении брака;
* копии свидетельств о рождении детей;
* личный листок по учету кадров;
* направление для участия во временном трудоустройстве;
* трудовые книжки;
* журнал выдачи трудовых книжек;
* согласие на обработку персональных данных;
* лист ознакомления;
* обязательство о неразглашении;
* справки о прохождении медосмотра;
* исполнительные листы (копии), выданные судами общей  
  юрисдикции;
* судебные приказы (копии);
* сведения о гражданине, подлежащем воинскому учету, и принятии  
  его на работу (увольнении его с работы);
* акты (копии) органов, осуществляющих контрольные функции по  
  взысканию денежных средств;
* судебные акты (копии), акты других органов и должностных лиц по  
  делам о правонарушениях;
* постановления (копии) судебного пристава-исполнителя;
* копии приговоров (определений, постановлений) суда;
* грамоты, благодарности;
* документы о конкурсах на должности;
* документы о награждении;
* документы о развитии;
* журналы учета входящих/ исходящих документов;
* журналы учета служебных командировок;
* другие документы, содержащие ПДн.

1. ПДн других лиц могут содержаться в следующих документах (копиях  
   указанных документов):

* платежные документы;
* документы, подтверждающие правомочность законного  
  представителя физического лица;
* исполнительные листы (копии), выданные судами общей  
  юрисдикции;
* копии судебных приказов;
* заявления, обращения законных представителей физических лиц;
* копии паспортов;
* копии приказов о назначении на должность;
* доверенности;
* другие документы, содержащие ПДн.

1. Основные мероприятия по приведению информационных систем  
   персональных данных в соответствие требованиям

Структурные подразделения правительства области, исполнительные  
органы государственной власти области, органы местного самоуправления  
области и подведомственные им организации (далее - операторы) при  
обработке ПДн обязаны принимать необходимые организационные и  
технические меры для защиты ПДн от неправомерного или случайного доступа  
к ним, уничтожения, изменения, блокирования, копирования, распространения  
ПДн, а также от иных неправомерных действий.

На основании принятых во исполнение положений Федерального закона № 152-ФЗ «О персональных данных», нормативно-правовых актов и методических документов операторы, эксплуатирующие ИСПДн, обязаны выполнить следующую последовательность действий для приведения ИСПДн в соответствие требованиям законодательства Российской Федерации:

1. Актом руководителя государственного или муниципального органа  
   утвердить следующие документы:

* Приказ о назначении ответственного за организацию обработки  
  персональных данных в государственном или муниципальном органе из числа  
  служащих данного органа (Приложение 5).
* Приказ о создании комиссии по определению уровня  
  защищенности ИСПДн ([Приложение 12](#Приложение12)).
* Правила обработки персональных данных, устанавливающие  
  процедуры, направленные на выявление и предотвращение нарушений  
  законодательства Российской Федерации в сфере персональных данных, а  
  также определяющие для каждой цели обработки персональных данных  
  содержание обрабатываемых персональных данных, категории субъектов,  
  персональные данные которых обрабатываются, сроки их обработки и  
  хранения, порядок уничтожения при достижении целей обработки или при  
  наступлении иных законных оснований ([Глава II. Разделы 1](#п2_1),[3](#п2_3),[10](#п2_10)).
* Правила рассмотрения запросов субъектов персональных данных  
  или их представителей ([Глава II. Раздел 12](#п2_12)).
* Правила осуществления внутреннего контроля соответствия  
  обработки персональных данных требованиям к защите персональных данных,  
  установленным Федеральным законом "О персональных данных", принятыми в  
  соответствии с ним нормативными правовыми актами и локальными актами  
  оператора ([Глава II. Раздел 14](#п2_14)).
* Правила работы с обезличенными данными ([Глава II. Раздел 11](#п2_11));
* Перечень информационных систем персональных данных  
  ([Приложение 7](#Приложение7)).
* Перечни персональных данных, обрабатываемых в  
  государственном или муниципальном органе в связи с реализацией трудовых  
  отношений, а также в связи с оказанием государственных или муниципальных  
  услуг и осуществлением государственных или муниципальных функций ([Глава  
  II. Раздел 4](#п2_4)).
* Перечень должностей служащих государственного или  
  муниципального органа, ответственных за проведение мероприятий по  
  обезличиванию обрабатываемых персональных данных ([Приложение 11](#Приложение11)).
* Перечень должностей служащих государственного или  
  муниципального органа, замещение которых предусматривает осуществление  
  обработки персональных данных либо осуществление доступа к персональным  
  данным ([Приложение 10](#Приложение10)).
* Должностная инструкция ответственного за организацию обработки  
  персональных данных в государственном или муниципальном органе  
  ([Приложение 14](#Приложение14)).
* Должностная инструкция администратора безопасности  
  информационных систем персональных данных ([Приложение 15](#Приложение15)).
* Типовое обязательство служащего государственного или  
  муниципального органа, непосредственно осуществляющего обработку  
  персональных данных, в случае расторжения с ним государственного или  
  муниципального контракта прекратить обработку персональных данных,  
  ставших известными ему в связи с исполнением должностных обязанностей  
  ([Глава II. Раздел 8](#п2_8)).
* Типовая форма согласия на обработку персональных данных  
  служащих государственного или муниципального органа, иных субъектов  
  персональных данных, а также типовая форма разъяснения субъекту  
  персональных данных юридических последствий отказа предоставить свои ПДн  
  ([Глава II. Раздел 9](#п2_9)).
* Порядок доступа служащих государственного или муниципального  
  органа в помещения, в которых ведется обработка персональных данных  
  ([Приложение 21](#Приложение21)).

Рекомендуется список допущенных лиц оформить в виде Разрешительной  
системы доступа к информационным ресурсам, программным и техническим

средствам информационных систем персональных данных, которая включает  
уровень прав доступа допущенных лиц к ресурсам ИСПДн. Разрешительная  
система доступа доводится до всех сотрудников оператора, допущенных к  
обработке ПДн, под роспись ([Приложение 20](#Приложение20)).

1. Определить тип угроз и установить уровень защищенности для ИСПДн  
   различного типа ([Глава II. Раздел 5](#п2_5)).
2. Реализовать методы и способы защиты ПДн в ИСПДн  
   ([Глава II. Раздел 6](#п2_6)).
3. Зарегистрироваться в качестве оператора ПДн - подготовить и  
   направить уведомление в территориальный орган Федеральной службы по  
   надзору в сфере связи, информационных технологий и массовых коммуникаций

* уполномоченный орган по защите прав субъектов ПДн ([Глава II. Раздел 7](#п2_7)).

1. Получить согласие субъектов ПДн на обработку их ПДн, если иное не  
   предусмотрено законом ([Глава II. Раздел 9](#п2_9)).
2. Разработать и утвердить форму журнала регистрации и учета  
   обращений субъектов персональных данных ([Приложение 28](#Приложение28)).
3. Подготовить и утвердить для каждого типа применяемых СЗИ  
   инструкции по их использованию, предназначенные для ответственных за  
   обеспечение безопасности ПДн, администраторов безопасности ИСПДн.
4. Разработать и утвердить модель УБПДн при их обработке в ИСПДн  
   ([Глава II. Раздел 13](#п2_13)).
5. Разработать регламент учета средств защиты информации,  
   эксплуатационной и технической документации к ним, электронных носителей  
   персональных данных ([Приложение 30](#Приложение30)).
6. Разработать и утвердить Положение по обеспечению безопасности  
   ПДн при их обработке в ИСПДн ([Приложение 31](#Приложение31)).

Положение определяет порядок организации и проведения работ по  
обеспечению безопасности ПДн при их обработке в ИСПДн и содержит общие  
принципы защиты ПДн.

1. **Правовое основание обработки персональных данных**

Правовым основанием обработки ПДн работников и других лиц  
являются требования:

* Конституции Российской Федерации;
* Трудового кодекса Российской Федерации;
* Гражданского кодекса Российской Федерации;
* Гражданско-правового кодекса Российской Федерации;
* Федерального закона от 27 июля 2006 года № 152-ФЗ «О  
  персональных данных»;
* Федерального закона от 27 июля 2004 г. № 79-ФЗ "О  
  государственной гражданской службе Российской Федерации";
* Федерального закона от 27 мая 2003 г. № 58-ФЗ "О системе  
  государственной службы Российской Федерации";
* Федерального закона от 26 декабря 2008 г. № 294-ФЗ "О защите  
  прав юридических лиц и индивидуальных предпринимателей при проведении  
  государственного контроля (надзора)" и муниципального контроля;
* Федерального закона от 2 мая 2006 г. № 59-ФЗ "О порядке  
  рассмотрения обращений граждан Российской Федерации";
* других нормативных и правовых актов Российской Федерации.

1. **Перечень персональных данных, обрабатываемых в государственном  
   или муниципальном органе в связи с реализацией трудовых отношений, а  
   также в связи с оказанием государственных или муниципальных услуг и  
   осуществлением государственных или муниципальных функций**

Перечень персональных данных − подробный, четко структурированный  
документ, содержащий информацию обо всех категориях и видах ПДн,  
обрабатываемых оператором с применением средств автоматизации или без  
таковых, как являющихся собственностью оператора, так и передаваемые  
(предоставляемые) в распоряжение (пользование) другими операторами  
([Приложение 8](#Приложение8)).

Для составления Перечня привлекается широкий круг должностных лиц  
структурных подразделений, отделов оператора с тем, чтобы ни одно из  
возможных направлений его деятельности не было упущено при его  
разработке.

В ходе подготовки Перечня должностные лица проводят анализ всех  
сторон деятельности оператора с целью определения состава обрабатываемых  
ПДн, целей (трудовые отношения, сбор данных граждан, оформление  
пропусков, договор оказания услуг и т.п.) и условий их обработки, сроков  
обработки и хранения ПДн различных категорий.

В результате данного шага оператор получает сформированное мнение о  
составе и содержании обрабатываемых в его структуре ПДн, оформленное в  
виде Перечня ПДн, подлежащих защите, утвержденного руководителем  
оператора и доведенного до всех сотрудников оператора, допущенных к  
обработке ПДн, под роспись.

Следует особое внимание уделять обоснованию сроков обработки и  
хранения всех ПДн, так согласно части 2 статьи 5 Федерального закона № 152-  
ФЗ «О персональных данных» хранение ПДн должно осуществляться в форме,  
позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели  
их обработки, и они подлежат уничтожению по достижении целей обработки  
или в случае утраты необходимости в их достижении. В соответствии с частью 4 статьи 21 закона в случае достижения цели обработки ПДн оператор обязан  
незамедлительно прекратить обработку ПДн и уничтожить соответствующие  
ПДн в срок, не превышающий трех рабочих дней с даты достижения цели  
обработки ПДн, если иное не предусмотрено федеральными законами, и  
уведомить об этом субъекта ПДн или его законного представителя, а в случае,  
если обращение или запрос были направлены уполномоченным органом по  
защите прав субъектов ПДн, - также указанный орган.

1. **Определение типа угроз и установление уровня защищенности  
   персональных данных при их обработке в информационных системах  
   персональных данных, в зависимости от угроз безопасности этих данных**
   1. Безопасность ПДн при их обработке в ИСПДн обеспечивается с  
      помощью системы защиты ПДн, нейтрализующей актуальные угрозы,  
      определенные в соответствии с частью 5 статьи 19 Федерального закона "О  
      персональных данных".

Система защиты ПДн включает в себя организационные и (или)  
технические меры, определенные с учетом актуальных угроз безопасности ПДн  
и информационных технологий, используемых в информационных системах.

* 1. Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор  
     этой системы, который обрабатывает ПДн (далее - оператор), или лицо,  
     осуществляющее обработку ПДн по поручению оператора на основании  
     заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор  
     между оператором и уполномоченным лицом должен предусматривать  
     обязанность уполномоченного лица обеспечить безопасность ПДн при их  
     обработке в ИСПДн.

Для выполнения работ по обеспечению безопасности ПДн при их  
обработке в информационной системе в соответствии с законодательством  
Российской Федерации могут привлекаться на договорной основе юридическое  
лицо или индивидуальный предприниматель, имеющие лицензию на  
деятельность по технической защите конфиденциальной информации.

* 1. Выбор средств защиты информации для системы защиты ПДн  
     осуществляется оператором в соответствии с нормативными правовыми  
     актами, принятыми Федеральной службой безопасности Российской Федерации  
     и Федеральной службой по техническому и экспортному контролю во  
     исполнение части 4 статьи 19 Федерального закона "О персональных данных"  
     ([Глава II. Раздел 6](#п2_6)).
  2. Информационная система является информационной системой,  
     обрабатывающей специальные категории персональных данных, если в ней  
     обрабатываются ПДн, касающиеся расовой, национальной принадлежности,  
     политических взглядов, религиозных или философских убеждений, состояния  
     здоровья, интимной жизни субъектов ПДн.

Информационная система является информационной системой,  
обрабатывающей биометрические персональные данные, если в ней  
обрабатываются сведения, которые характеризуют физиологические и

биологические особенности человека, на основании которых можно установить  
его личность и которые используются оператором для установления личности  
субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным  
категориям ПДн.

Информационная система является информационной системой,  
обрабатывающей общедоступные персональные данные, если в ней  
обрабатываются ПДн субъектов ПДн, полученные только из общедоступных  
источников ПДн, созданных в соответствии со статьей 8 Федерального закона  
"О персональных данных".

Информационная система является информационной системой,  
обрабатывающей иные категории персональных данных, если в ней не  
обрабатываются ПДн, указанные в абзацах первом - третьем настоящего  
пункта.

Информационная система является информационной системой,  
обрабатывающей ПДн сотрудников оператора, если в ней обрабатываются ПДн  
только указанных сотрудников. В остальных случаях ИСПДн является  
информационной системой, обрабатывающей ПДн субъектов ПДн, не  
являющихся сотрудниками оператора.

* 1. Под актуальными угрозами безопасности ПДн понимается  
     совокупность условий и факторов, создающих актуальную опасность  
     несанкционированного, в том числе случайного, доступа к персональным  
     данным, результатом которого могут стать уничтожение, изменение,  
     блокирование, копирование, предоставление, распространение ПДн, а также  
     иные неправомерные действия при их обработке в ИСПДн;

Угрозы 1-го типа актуальны для ИСПДн, если для нее, в том числе,  
актуальны угрозы, связанные с наличием недокументированных  
(недекларированных) возможностей в системном программном обеспечении,  
используемом в составе ИСПДн;

Угрозы 2-го типа актуальны для ИСПДн, если для нее, в том числе,  
актуальны угрозы, связанные с наличием недокументированных  
(недекларированных) возможностей в прикладном программном обеспечении,  
используемом в составе ИСПДн;

Угрозы 3-го типа актуальны для ИСПДн, если для нее не актуальны  
угрозы, связанные с наличием недокументированных (недекларированных)  
возможностей в системном и прикладном программном обеспечении,  
используемом в составе ИСПДн.

Под актуальными угрозами, связанными с наличием  
недокументированных (недекларированных) возможностей в системном и  
прикладном программном обеспечении подразумевается возможность  
возникновения данных угроз по причине использование не  
сертифицированного системного или прикладного программного обеспечения.

[Список сертифицированных ФСТЭК системных и прикладных](http://www.microsoft.com/rus/government/certificate/)  
[программных продуктов компании Microsoft](http://www.microsoft.com/rus/government/certificate/)

* 1. При обработке ПДн в информационных системах устанавливаются 4  
     уровня защищенности ПДн.
  2. Необходимость обеспечения 1-го уровня защищенности ПДн при  
     их обработке в информационной системе устанавливается при наличии хотя бы  
     одного из следующих условий:

а) для информационной системы актуальны угрозы 1 -го типа и  
информационная система обрабатывает либо специальные категории ПДн, либо  
биометрические персональные данные, либо иные категории ПДн;

б) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает специальные категории ПДн более чем  
100000 субъектов ПДн, не являющихся сотрудниками оператора.

* 1. Необходимость обеспечения 2-го уровня защищенности ПДн при их  
     обработке в информационной системе устанавливается при наличии хотя бы  
     одного из следующих условий:

а) для информационной системы актуальны угрозы 1 -го типа и  
информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает специальные категории ПДн  
сотрудников оператора или специальные категории ПДн менее чем 100000  
субъектов ПДн, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает общедоступные персональные данные  
более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает иные категории ПДн более чем 100000  
субъектов ПДн, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает специальные категории ПДн более чем  
100000 субъектов ПДн, не являющихся сотрудниками оператора.

* 1. Необходимость обеспечения 3-го уровня защищенности ПДн при их  
     обработке в информационной системе устанавливается при наличии хотя бы  
     одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает общедоступные персональные данные  
сотрудников оператора или общедоступные персональные данные менее чем  
100000 субъектов ПДн, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и  
информационная система обрабатывает иные категории ПДн сотрудников  
оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не  
являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает специальные категории ПДн  
сотрудников оператора или специальные категории ПДн менее чем 100000  
субъектов ПДн, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает иные категории ПДн более чем 100000  
субъектов ПДн, не являющихся сотрудниками оператора.

* 1. Необходимость обеспечения 4-го уровня защищенности ПДн при  
     их обработке в информационной системе устанавливается при наличии хотя бы  
     одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и  
информационная система обрабатывает иные категории ПДн сотрудников  
оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не  
являющихся сотрудниками оператора.

В таблице 3 приведены уровни защищенности ПДн при их обработке в  
ИСПДн в зависимости от угроз безопасности этих данных.

* 1. Для обеспечения 4-го уровня защищенности ПДн при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых  
размещена информационная система, препятствующего возможности  
неконтролируемого проникновения или пребывания в этих помещениях лиц, не  
имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей ПДн;

в) утверждение руководителем оператора документа, определяющего  
перечень лиц, доступ которых к персональным данным, обрабатываемым в  
информационной системе, необходим для выполнения ими служебных  
(трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру  
оценки соответствия требованиям законодательства Российской Федерации в  
области обеспечения безопасности информации, в случае, когда применение  
таких средств необходимо для нейтрализации актуальных угроз.

* 1. Для обеспечения 3-го уровня защищенности ПДн при их обработке в  
     информационных системах помимо выполнения требований, предусмотренных  
     пунктом 5.11, необходимо, чтобы было назначено должностное лицо  
     (работник), ответственный за обеспечение безопасности ПДн в  
     информационной системе.
  2. Для обеспечения 2-го уровня защищенности ПДн при их обработке  
     в информационных системах помимо выполнения требований,  
     предусмотренных пунктом 5.12 настоящего документа, необходимо, чтобы  
     доступ к содержанию электронного журнала сообщений был возможен  
     исключительно для должностных лиц (работников) оператора или  
     уполномоченного лица, которым сведения, содержащиеся в указанном  
     журнале, необходимы для выполнения служебных (трудовых) обязанностей.
  3. Для обеспечения 1-го уровня защищенности ПДн при их обработке  
     в информационных системах помимо требований, предусмотренных пунктом  
     5.13 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности  
изменения полномочий сотрудника оператора по доступу к персональным  
данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение  
безопасности ПДн в информационной системе, либо возложение на одно из  
структурных подразделений функций по обеспечению такой безопасности.

В таблице 4 приведены Требования к защите ПДн при их обработке в  
ИСПДн, исполнение которых обеспечивает установленные уровни  
защищенности ПДн.

Таблица 3. Уровни защищенности ПДн при их обработке в ИСПДн в  
зависимости от угроз безопасности этих данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ИСПДн** | **Категории**  **субъектов** | **Количество**  **субъектов** | **Тип актуальных угроз** | | |
| **1 тип** | **2 тип** | **3 тип** |
| **ИСПДн- Специальные** | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 1 | УЗ 2 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| **ИСПДн- Биометрические** | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| **ИСПДн-Иные категории** | Не сотрудники | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| Сотрудники | Более 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| **ИСПДн- Общедоступные** | Не сотрудники | Более 100 000 | УЗ 2 | УЗ 2 | УЗ 4 |
| Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| Сотрудники | Более 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |

На основании полученных данных составляется Акт определения уровня  
защищенности ИСПДн ([Приложение 13](#Приложение13)).

Таблица 4. Требования к защите персональных данных при их обработке в  
информационных системах персональных данных, исполнение которых  
обеспечивает установленные уровни защищенности персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Требования** | **Уровни**  **защищенности** | | | |
| **1** | **2** | **3** | **4** |
| Организован режим обеспечения безопасности помещений, в которых размещена информационная система персональных данных, исключающий возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц; | + | + | + | + |
| Обеспечена сохранность носителей персональных данных; | + | + | + | + |
| Руководителем оператора утвержден документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей; | + | + | + | + |
| Назначено должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе персональных данных; | + | + | + | - |
| Доступ к содержанию электронного журнала сообщений возможен только должностному лицу (работнику) оператора или уполномоченного лица; | + | + | + | - |
| Применение средств защиты информации, успешно прошедших процедуру оценки соответствия в соответствии с законодательством Российской Федерации; | + | + | - | - |
| Факт изменения полномочий субъектов доступа к объектам доступа регистрировался автоматизированными средствами информационной системы персональных данных в электронном журнале безопасности; | + | - | - | - |
| Назначено структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе персональных данных. | + | - | - | - |

1. Контроль за выполнением настоящих требований организуется и  
   проводится оператором (уполномоченным лицом) самостоятельно и (или) с  
   привлечением на договорной основе юридических лиц и индивидуальных  
   предпринимателей, имеющих лицензию на осуществление деятельности по  
   технической защите конфиденциальной информации. Указанный контроль  
   проводится не реже 1 раза в 3 года в сроки, определяемые оператором  
   (уполномоченным лицом).
2. **Состав и содержание организационных и технических мер по  
   обеспечению безопасности персональных данных при их обработке в  
   информационных системах персональных данных**
   1. Меры по обеспечению безопасности ПДн принимаются для защиты  
      ПДн от неправомерного или случайного доступа к ним, уничтожения,  
      изменения, блокирования, копирования, предоставления, распространения  
      ПДн, а также от иных неправомерных действий в отношении ПДн.
   2. Меры по обеспечению безопасности ПДн реализуются в рамках  
      системы защиты ПДн и должны быть направлены на нейтрализацию  
      актуальных угроз безопасности персональных данных.
   3. Меры по обеспечению безопасности ПДн реализуются в том числе  
      посредством применения в информационной системе средств защиты  
      информации, прошедших в установленном порядке процедуру оценки  
      соответствия, в случаях, когда применение таких средств необходимо для  
      нейтрализации актуальных угроз безопасности ПДн.
   4. Оценка эффективности реализованных в рамках системы защиты  
      ПДн мер по обеспечению безопасности ПДн проводится оператором  
      самостоятельно или с привлечением на договорной основе юридических лиц и  
      индивидуальных предпринимателей, имеющих лицензию на осуществление  
      деятельности по технической защите конфиденциальной информации.  
      Указанная оценка проводится не реже одного раза в 3 года.
   5. Меры по обеспечению безопасности ПДн при их обработке в  
      государственных информационных системах принимаются в соответствии с  
      требованиями о защите информации, содержащейся в государственных  
      информационных системах, устанавливаемыми ФСТЭК России в пределах  
      своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от  
      27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о  
      защите информации".
   6. На основании Приказа ФСТЭК России от 18 февраля 2013 г. № 21  
      «Об утверждении Состава и содержания организационных и технических мер  
      по обеспечению безопасности персональных данных при их обработке в  
      информационных системах персональных данных» в состав мер по  
      обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн с  
      учетом актуальных угроз безопасности ПДн и применяемых информационных  
      технологий, входят:

* идентификация и аутентификация субъектов доступа и объектов  
  доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защита машинных носителей информации, на которых хранятся и  
  (или) обрабатываются ПДн (далее - машинные носители ПДн);
* регистрация событий безопасности;
* антивирусная защита;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищенности ПДн;
* обеспечение целостности информационной системы и ПДн;
* обеспечение доступности ПДн;
* защита среды виртуализации;
* защита технических средств;
* защита информационной системы, ее средств, систем связи и  
  передачи данных;
* выявление инцидентов (одного события или группы событий),  
  которые могут привести к сбоям или нарушению функционирования  
  информационной системы и (или) к возникновению угроз безопасности ПДн  
  (далее - инциденты), и реагирование на них;
* управление конфигурацией информационной системы и системы  
  защиты ПДн.

Состав и содержание мер по обеспечению безопасности ПДн,  
необходимых для обеспечения каждого из уровней защищенности ПДн,  
приведены в таблице 6.

1. Меры по идентификации и аутентификации субъектов доступа и  
   объектов доступа должны обеспечивать присвоение субъектам и объектам  
   доступа уникального признака (идентификатора), сравнение предъявляемого  
   субъектом (объектом) доступа идентификатора с перечнем присвоенных  
   идентификаторов, а также проверку принадлежности субъекту (объекту)  
   доступа предъявленного им идентификатора (подтверждение подлинности).
2. Меры по управлению доступом субъектов доступа к объектам  
   доступа должны обеспечивать управление правами и привилегиями субъектов  
   доступа, разграничение доступа субъектов доступа к объектам доступа на  
   основе совокупности установленных в информационной системе правил  
   разграничения доступа, а также обеспечивать контроль за соблюдением этих  
   правил.
3. Меры по ограничению программной среды должны обеспечивать  
   установку и (или) запуск только разрешенного к использованию в  
   информационной системе программного обеспечения или исключать  
   возможность установки и (или) запуска запрещенного к использованию в  
   информационной системе программного обеспечения.

Перечисленные меры осуществляются с помощью введения системы  
разграничения прав доступа пользователей и применения групповых политик.

1. Меры по защите машинных носителей ПДн (средств обработки  
   (хранения) ПДн, съемных машинных носителей ПДн) должны исключать  
   возможность несанкционированного доступа к машинным носителям и  
   хранящимся на них персональным данным, а также несанкционированное  
   использование съемных машинных носителей ПДн.

Реализуются с помощью введения «Регламента учета средств защиты  
информации, эксплуатационной и технической документации к ним,  
электронных носителей» [(Приложение 30. Пример с ПДн)](#Приложение30) и «Списка лиц,  
допущенных в защищаемое помещение» [(Приложение 5)](#bookmark73).

1. Меры по регистрации событий безопасности должны обеспечивать  
   сбор, запись, хранение и защиту информации о событиях безопасности в  
   информационной системе, а также возможность просмотра и анализа  
   информации о таких событиях и реагирование на них.

Данные меры реализуются с помощью электронного журнала  
регистрации и учета событий безопасности.

1. Меры по антивирусной защите должны обеспечивать обнаружение  
   в информационной системе компьютерных программ либо иной компьютерной  
   информации, предназначенной для несанкционированного уничтожения,  
   блокирования, модификации, копирования компьютерной информации или  
   нейтрализации средств защиты информации, а также реагирование на  
   обнаружение этих программ и информации.

Осуществляются с использованием антивирусного программного  
комплекса.

1. Меры по обнаружению (предотвращению) вторжений должны  
   обеспечивать обнаружение действий в информационной системе,  
   направленных на несанкционированный доступ к информации, специальные  
   воздействия на информационную систему и (или) ПДн в целях добывания,  
   уничтожения, искажения и блокирования доступа к персональным данным, а  
   также реагирование на эти действия.

Осуществляются с использованием систем обнаружения вторжения.

1. Меры по контролю (анализу) защищенности ПДн должны  
   обеспечивать контроль уровня защищенности ПДн, обрабатываемых в  
   информационной системе, путем проведения систематических мероприятий по  
   анализу защищенности информационной системы и тестированию  
   работоспособности системы защиты ПДн.

Данные меры осуществляются с помощью средств анализа защищенности

1. Меры по обеспечению целостности информационной системы и  
   ПДн должны обеспечивать обнаружение фактов несанкционированного  
   нарушения целостности информационной системы и содержащихся в ней ПДн,  
   а также возможность восстановления информационной системы и  
   содержащихся в ней ПДн.

Данные меры осуществляются с помощью средств фиксации и контроля  
исходного состояния программного комплекса.

1. Меры по обеспечению доступности ПДн должны обеспечивать  
   авторизованный доступ пользователей, имеющих права по доступу, к  
   персональным данным, содержащимся в информационной системе, в штатном  
   режиме функционирования информационной системы.

Способы реализации, приведенные в п. 6.6.3.

1. Меры по защите среды виртуализации должны исключать  
   несанкционированный доступ к персональным данным, обрабатываемым в  
   виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и  
   (или) воздействие на них, в том числе к средствам управления виртуальной  
   инфраструктурой, монитору виртуальных машин (гипервизору), системе  
   хранения данных (включая систему хранения образов виртуальной  
   инфраструктуры), сети передачи данных через элементы виртуальной или  
   физической инфраструктуры, гостевым операционным системам, виртуальным  
   машинам (контейнерам), системе и сети репликации, терминальным и  
   виртуальным устройствам, а также системе резервного копирования и  
   создаваемым ею копиям.
2. Меры по защите технических средств должны исключать  
   несанкционированный доступ к стационарным техническим средствам,  
   обрабатывающим ПДн, средствам, обеспечивающим функционирование  
   информационной системы (далее - средства обеспечения функционирования), и  
   в помещения, в которых они постоянно расположены, защиту технических  
   средств от внешних воздействий, а также защиту ПДн, представленных в виде  
   информативных электрических сигналов и физических полей.
3. Меры по защите информационной системы, ее средств, систем  
   связи и передачи данных должны обеспечивать защиту ПДн при  
   взаимодействии информационной системы или ее отдельных сегментов с  
   иными информационными системами и информационно-  
   телекоммуникационными сетями посредством применения архитектуры  
   информационной системы и проектных решений, направленных на обеспечение безопасности ПДн.

Все перечисленные меры реализуются с использованием  
сертифицированных средств защиты информации. Список СЗИ доступен в  
Государственном реестре сертифицированных средств защиты информации N  
РОСС RU.0001.01БИ00 на [сайте ФСТЭК России.](http://fstec.ru/sistema-sertifikatsii-tzi/153-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00)

1. Меры по выявлению инцидентов и реагированию на них должны  
   обеспечивать обнаружение, идентификацию, анализ инцидентов в  
   информационной системе, а также принятие мер по устранению и  
   предупреждению инцидентов.
2. Меры по управлению конфигурацией информационной системы и  
   системы защиты ПДн должны обеспечивать управление изменениями  
   конфигурации информационной системы и системы защиты ПДн, анализ  
   потенциального воздействия планируемых изменений на обеспечение  
   безопасности ПДн, а также документирование этих изменений.
   1. Выбор мер по обеспечению безопасности ПДн, подлежащих  
      реализации в информационной системе в рамках системы защиты ПДн,  
      включает:

* определение базового набора мер по обеспечению безопасности  
  ПДн для установленного уровня защищенности ПДн в соответствии с базовыми наборами мер по обеспечению безопасности ПДн, приведенными в таблице 6;
* адаптацию базового набора мер по обеспечению безопасности ПДн  
  с учетом структурно-функциональных характеристик информационной  
  системы, информационных технологий, особенностей функционирования  
  информационной системы (в том числе исключение из базового набора мер,  
  непосредственно связанных с информационными технологиями, не  
  используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер по обеспечению  
  безопасности ПДн с учетом не выбранных ранее мер, приведенных в таблице 6,  
  в результате чего определяются меры по обеспечению безопасности ПДн,

направленные на нейтрализацию всех актуальных угроз безопасности ПДн для  
конкретной информационной системы;

* дополнение уточненного адаптированного базового набора мер по  
  обеспечению безопасности ПДн мерами, обеспечивающими выполнение  
  требований к защите ПДн, установленными иными нормативными правовыми  
  актами в области обеспечения безопасности ПДн и защиты информации.
  1. При невозможности технической реализации отдельных выбранных  
     мер по обеспечению безопасности ПДн, а также с учетом экономической  
     целесообразности на этапах адаптации базового набора мер и (или) уточнения  
     адаптированного базового набора мер могут разрабатываться иные  
     (компенсирующие) меры, направленные на нейтрализацию актуальных угроз  
     безопасности ПДн.

В этом случае в ходе разработки системы защиты ПДн должно быть  
проведено обоснование применения компенсирующих мер для обеспечения  
безопасности ПДн.

* 1. В случае определения в соответствии с Требованиями к защите  
     персональных при их обработке в ИСПДн, утвержденными постановлением  
     Правительства Российской Федерации от 1 ноября 2012 г. №1119, в качестве  
     актуальных угроз безопасности ПДн 1-го и 2-го типов дополнительно к мерам  
     по обеспечению безопасности ПДн, указанным в пункте 6.1, могут  
     применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения,  
включая программный код, на отсутствие недекларированных возможностей с  
использованием автоматизированных средств и (или) без использования  
таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или)  
прикладного программного обеспечения, разработанного с использованием  
методов защищенного программирования.

* 1. При использовании в информационных системах  
     сертифицированных по требованиям безопасности информации средств защиты  
     информации (Таблица 5):

а) для обеспечения 1 и 2 уровней защищенности ПДн применяются:

* средства вычислительной техники не ниже 5 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 4 класса;
* межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с  
  информационно - телекоммуникационными сетями международного  
  информационного обмена и межсетевые экраны не ниже 4 класса в случае  
  актуальности угроз 3-го типа и отсутствия взаимодействия информационной  
  системы с информационно-телекоммуникационными сетями международного  
  информационного обмена;

б) для обеспечения 3 уровня защищенности ПДн применяются:

* средства вычислительной техники не ниже 5 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 4 класса защиты в случае актуальности угроз 2-го типа или  
  взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена и  
  системы обнаружения вторжений и средства антивирусной защиты не ниже 5  
  класса защиты в случае актуальности угроз 3-го типа и отсутствия  
  взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена;
* межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-  
  го типа или взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена и  
  межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и  
  отсутствия взаимодействия информационной системы с информационно-  
  телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности ПДн применяются:

* средства вычислительной техники не ниже 6 класса;
* системы обнаружения вторжений и средства антивирусной защиты  
  не ниже 5 класса;
* межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности ПДн, а также для  
обеспечения 3 уровня защищенности ПДн в информационных системах, для  
которых к актуальным отнесены угрозы 2-го типа, применяются средства  
защиты информации, программное обеспечение которых прошло проверку не  
ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Таблица 5. Тип применяемых средств защиты информации, в  
зависимости от уровня защищенности персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Средства защиты информации** | **Уровни защищенности** | | | |
| **1** | **2** | **3** | **4** |
| Средства  вычислительной  техники | 5+ | 5+ | 5+ | 6+ |
| Системы  обнаружения  вторжений | 4+ | 4+ | 4+ / 5+\* | 5+ |
| Средства  антивирусной  защиты | 4 + | 4 + | 4+ / 5+\* | 5+ |
| Межсетевые  Экраны | 3 + / 4+\* | 3 + / 4+\* | 3 + / 4+\* | 5 |
| Недекларированные  возможности | 4+ | 4+ | - / 4+ (АУ) | - |

* (в случае актуальности угроз 1-го или 2-го типа или взаимодействия  
  ИС с информационно-телекоммуникационными сетям международного  
  информационного обмена) /

(в случае актуальности угроз 3-го типа и отсутствия взаимодействия с информационно-телекоммуникационными сетям международного

информационного обмена)

* 1. При использовании в информационных системах новых  
     информационных технологий и выявлении дополнительных угроз безопасности ПДн, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 6.3.

Таблица 6. Состав и содержание мер по, обеспечению безопасности  
персональных данных, необходимых для обеспечения каждого из уровней

защищенности персональных данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Условное обозначение и номер меры** | **Содержание мер по обеспечению безопасности персональных данных** | **Уровни защищенности персональных данных** | | | |
| **4** | **3** | **2** | **1** |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |  |  | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных |  |  |  |  |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |  |  |  |  |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |  |  |  |  |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |  | + | + | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |  | + | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |  |  |  |  |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних | + | + | + | + |
|  | организаций (внешние информационные системы) |  |  |  |  |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |  |  | + | + |
| III. Ограничение программной среды (ОПС) | | | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |  |  |  |  |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |  |  | + | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |  |  |  | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |  |  |  |  |
| IV. Защита машинных носителей персональных данных (ЗНИ) | | | | | |
| ЗНИ.1 | Учет машинных носителей персональных данных |  |  | + | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных |  |  | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны |  |  |  |  |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах |  |  |  |  |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода)информации на машинные носители персональных данных |  |  |  |  |
| ЗНИ.6 | Контроль ввода (вывода) информации на |  |  |  |  |
|  | машинные носители персональных данных |  |  |  |  |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных |  |  |  |  |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |  | + | + | + |
| V. Регистрация событий безопасности (РСБ) | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости)памяти |  |  |  |  |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |  |  | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |  |  |  |  |
| РСБ.7 | Защита информации о событиях безопасности | + | + | + | + |
| VI. Антивирусная защита (АВЗ) | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + |
| VII. Обнаружение вторжений (СОВ) | | | | | |
| СОВ.1 | Обнаружение вторжений |  |  | + | + |
| СОВ.2 | Обновление базы решающих правил |  |  | + | + |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |  | + | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + |
| АНЗ.З | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |  | + | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |  | + | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |  |  | + | + |
| IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ) | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |  |  | + | + |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы |  |  |  |  |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |  |  |  |  |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |  |  | + | + |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение |  |  |  |  |
|  | неправомерной передачи информации из информационной системы |  |  |  |  |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |  |  |  |  |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |  |  |  |  |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях |  |  |  |  |
| X. Обеспечение доступности персональных данных (ОДТ) | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств |  |  |  |  |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |  |  |  |  |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |  | + |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |  |  | + | + |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |  |  | + | + |
| XI. Защита среды виртуализации (ЗСВ) | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной |  | + | + | + |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | инфраструктуре |  |  |  |  |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |  |  |  |  |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |  |  |
| ЗСВ.6 | Управление перемещением виртуальных машин(контейнеров) и обрабатываемых на них данных |  |  | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |  |  | + | + |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |  |  | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |  | + | + | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |  | + | + | + |
| XII. Защита технических средств (ЗТС) | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |  |  |  |  |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |  |  |  |  |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, | + | + | + | + |
|  | средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |  |  |  |  |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |  |  |  |  |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (3ИС) | | | | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы |  |  |  | + |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |  |  |  |  |
| ЗИС.З | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче)по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + | + | + |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |  |  |  |  |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |  |  |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с |  |  |  |  |
|  | персональными данными, при обмене ими с иными информационными системами |  |  |  |  |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |  |  |  |  |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |  |  |  |  |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |  |  |  |  |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |  |  |  |  |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |  |  | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю |  |  |  |  |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя |  |  |  |  |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных |  |  |  |  |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |  |  | + | + |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |  |  |  |  |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |  |  | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения |  |  |  |  |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |  |  |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |  | + | + | + |
| XIV. Выявление инцидентов и реагирование на них (ИНЦ) | | | | | |
| ИНЦ1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них |  |  | + | + |
| ИНЦ2 | Обнаружение, идентификация и регистрация инцидентов |  |  | + | + |
| ИНЦ3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами |  |  | + | + |
| ИНЦ4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий |  |  | + | + |
| ИНЦ5 | Принятие мер по устранению последствий инцидентов |  |  | + | + |
| ИНЦ6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов |  |  | + | + |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | | | | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты |  | + | + | + |
|  | персональных данных |  |  |  |  |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |  | + | + | + |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |  | + | + | + |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |  | + | + | + |

«+» - мера по обеспечению безопасности ПДн включена в базовый набор  
мер для соответствующего уровня защищенности ПДн.

Меры по обеспечению безопасности ПДн, не обозначенные знаком «+»,  
применяются при адаптации базового набора мер и уточнении адаптированного  
базового набора мер, а также при разработке компенсирующих мер по  
обеспечению безопасности ПДн.

1. **Регистрация в качестве оператора персональных данных**

Оператор до начала обработки ПДн обязан направить уведомление в  
уполномоченный орган по защите прав субъектов ПДн о своем намерении  
осуществлять обработку ПДн, что является заявкой на получение статуса  
оператора ПДн ([Приложение 9](#Приложение9)).

Оператор вправе осуществлять без уведомления уполномоченного органа  
по защите прав субъектов ПДн обработку ПДн:

1. относящихся к субъектам ПДн, которых связывают с оператором  
   трудовые отношения;
2. полученных оператором в связи с заключением договора, стороной  
   которого является субъект ПДн, если ПДн не распространяются, а также не  
   предоставляются третьим лицам без согласия субъекта ПДн, и используются  
   оператором исключительно для исполнения указанных договоров и заключения  
   договоров с субъектом ПДн;
3. относящихся к членам (участникам) общественного объединения или  
   религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться без согласия в письменной форме субъектов ПДн;
4. являющихся общедоступными ПДн;
5. включающих в себя только фамилии, имена и отчества субъектов ПДн;
6. необходимых в целях однократного пропуска субъекта ПДн на  
   территорию, на которой находится оператор, или в иных аналогичных целях;
7. включенных в ИСПДн, имеющие в соответствии с федеральными  
   законами статус федеральных автоматизированных информационных систем, а  
   также в государственные ИСПДн, созданные в целях защиты безопасности  
   государства и общественного порядка;
8. обрабатываемых без использования средств автоматизации в  
   соответствии с федеральными законами или иными нормативными правовыми  
   актами Российской Федерации, устанавливающими требования к обеспечению  
   безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн.

Уполномоченным органом по защите прав субъектов ПДн, на который  
возлагается обеспечение контроля и надзора за соответствием обработки ПДн  
требованиям Федерального закона № 152-ФЗ «О персональных данных»,  
является федеральный орган исполнительной власти, осуществляющий

функции по контролю и надзору в сфере информационных технологий и связи

* Федеральная служба по надзору в сфере связи, информационных технологий  
  и массовых коммуникаций.

При подготовке уведомления необходимо опираться на документы  
Роскомнадзора, размещенные на ведомственном сайте

<http://www.pd.rsoc.ru/operators-registry/operators-registry-documents/>:

* образец уведомления об обработке (о намерении осуществлять  
  обработку) ПДн;
* рекомендации по заполнению образца формы уведомления об  
  обработке (о намерении осуществлять обработку) ПДн.

Заполненное уведомление должно быть направлено в письменной форме  
и подписано уполномоченным лицом или направлено в электронной форме и  
подписано электронной цифровой подписью в соответствии с  
законодательством Российской Федерации в управление Федеральной службы  
по надзору в сфере связи, информационных технологий и массовых  
коммуникаций по Саратовской области, адрес управления:  410056, г. Саратов, ул. Рабочая, дом 61 телефон (845-2) 22-55-77, факс (845-2) 52-13-00, e-  
mail: [rsockanc64@rsoc.ru](mailto:rsockanc64@rsoc.ru), сайт [64.rkn.gov.ru](http://64.rkn.gov.ru/).

В случае изменения сведений, содержащихся в уведомлении, оператор  
обязан уведомить об изменениях Роскомнадзор в течение десяти рабочих дней  
с даты возникновения таких изменений.

1. **Условия обеспечения конфиденциальности информации и  
   Ответственность за нарушения требований  
   Федерального закона № 152-ФЗ**
   1. Должностные лица Оператора, имеющие в силу исполнения ими  
      своих должностных обязанностей доступ к персональным данным, при их  
      обработке должны обеспечивать конфиденциальность этих данных  
      ([Приложение 16](#Приложение16)).
   2. Обеспечение конфиденциальности ПДн не требуется:

* в случае обезличивания ПДн ([Глава II.Раздел11](#п2_11));
* для общедоступных ПДн, то есть данных включенных в целях  
  информационного обеспечения в общедоступные источники ПДн (в том числе  
  справочники, адресные книги и т.п.) с письменного согласия субъекта ПДн. В  
  общедоступные источники ПДн могут включаться его фамилия, имя, отчество,  
  год и место рождения, адрес, абонентский номер, сведения о профессии и иные  
  ПДн, сообщаемые субъектом ПДн.
  1. Лица, виновные в нарушении требований Федерального закона №  
     79-ФЗ, Федерального закона № 152-ФЗ, ТК РФ, в том числе лица,  
     ответственные за организацию обработки ПДн, имеющие доступ к  
     персональным данным, несут дисциплинарную, административную,  
     уголовную ответственность в соответствии с действующим законодательством  
     Российской Федерации.

1. **Получение согласия субъекта персональных данных на обработку его  
   персональных данных**

Основной целью Федерального закона № 152-ФЗ является обеспечение  
защиты прав и свобод человека и гражданина при обработке его ПДн, поэтому  
в нем четко определены права субъектов ПДн и соответствующие обязанности  
оператора.

Одним из условий обработки ПДн является ее осуществление с согласия  
субъекта ПДн, за исключением случаев, предусмотренных частью 2 статьи 6  
Федерального закона № 152-ФЗ «О персональных данных», когда:

1. обработка ПДн осуществляется на основании федерального закона,  
   устанавливающего ее цель, условия получения ПДн и круг субъектов, ПДн  
   которых подлежат обработке, а также определяющего полномочия оператора;
2. обработка ПДн необходима в связи с реализацией международных  
   договоров Российской Федерации о реадмиссии;
3. обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн;
4. обработка ПДн осуществляется для статистических или иных научных целей при условии обязательного обезличивания;
5. обработка ПДн необходима для защиты жизни, здоровья или иных  
   жизненно важных интересов субъекта ПДн, если получение согласия субъекта  
   ПДн невозможно;
6. обработка ПДн необходима для доставки почтовых отправлений  
   организациями почтовой связи, для осуществления операторами электросвязи  
   расчетов с пользователями услуг связи за оказанные услуги связи, а также для  
   рассмотрения претензий пользователей услугами связи;
7. обработка ПДн осуществляется в целях профессиональной деятельности  
   журналиста либо в целях научной, литературной или иной творческой  
   деятельности при условии, что при этом не нарушаются права и свободы  
   субъекта ПДн;
8. осуществляется обработка ПДн, подлежащих опубликованию в  
   соответствии с федеральными законами, в том числе ПДн лиц, замещающих  
   государственные должности, должности государственной гражданской службы, ПДн кандидатов на выборные государственные или муниципальные должности.

Во всех других случаях необходимо провести комплекс мероприятий по  
получению согласия на обработку ПДн.

Необходимо обратить внимание на то, что в случаях, предусмотренных

Федеральным законом № 152-ФЗ «О персональных данных», обработка ПДн  
осуществляется только с согласия в письменной форме субъекта ПДн, так  
согласно статьям 10 и 11 специальные категории ПДн и биометрические ПДн  
могут обрабатываться только при наличии согласии в письменной форме субъекта ПДн.

Письменное согласие субъекта ПДн (Приложения 11-13) на обработку  
своих ПДн должно включать в себя:

1. фамилию, имя, отчество, адрес субъекта ПДн, номер основного  
   документа, удостоверяющего его личность, сведения о дате выдачи указанного  
   документа и выдавшем его органе;
2. наименование (фамилию, имя, отчество) и адрес оператора,  
   получающего согласие субъекта ПДн;
3. цель обработки ПДн;
4. перечень ПДн, на обработку которых дается согласие субъекта ПДн;
5. перечень действий с ПДн, на совершение которых дается согласие,  
   общее описание используемых оператором способов обработки ПДн;
6. срок, в течение которого действует согласие, а также порядок его  
   отзыва.

Согласие на обработку ПДн может быть отозвано субъектом  
ПДн([Приложение 22](#Приложение22)). Обязанность предоставить доказательство получения  
согласия субъекта ПДн на обработку его ПДн, а в случае обработки  
общедоступных ПДн обязанность доказывания того, что обрабатываемые ПДн  
являются общедоступными, возлагается на оператора.

Субъект ПДн имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора ПДн, относящихся к соответствующему  
субъекту ПДн, а также на ознакомление с такими ПДн, за исключением  
случаев, предусмотренных частью 5 статьи 14 Федерального закона № 152-ФЗ  
«О персональных данных».

Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их  
блокирования или уничтожения в случае, если ПДн являются неполными,  
устаревшими, недостоверными, незаконно полученными или не являются  
необходимыми для заявленной цели обработки, а также принимать  
предусмотренные законом меры по защите своих прав.

В целях обеспечения максимальной юридической чистоты в вопросах  
соблюдения прав субъектов ПДн и во избежание инцидентов, связанных с  
нарушением этих прав, порядок реагирования на запросы со стороны субъектов  
ПДн, внесения изменений в ПДн, а также условия прекращения обработки ПДн

должны быть определены документально в соответствующих приказах,  
регламентах и инструкциях, определяющих в том числе степень участия  
должностных лиц в обработке ПДн и характер их взаимодействия между собой.

1. **Правила обработки персональных данных**
   1. Действия (операции) с персональными данными. Оператор  
      совершаются следующие действия (операции) или совокупность действий  
      (операций) с персональными данными субъектов ПДн: сбор, запись,  
      систематизация, накопление, хранение, уточнение (обновление, изменение),  
      извлечение, использование, передача (распространение, предоставление,  
      доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
   2. Оператор использует следующие способы обработки ПДн:

* с использованием средств вычислительной техники  
  (автоматизированная обработка);
* обработка без использования средств вычислительной техники  
  (неавтоматизированная обработка).
  1. Создание ПДн.
     1. Документы, в том числе и в электронном виде, содержащие ПДн,  
        создаются путём:
* получения оригиналов необходимых документов;
* копирования оригиналов документов;
* внесения сведений в учётные формы (на бумажных и электронных  
  носителях).
  + 1. Оператор получает ПДн субъектов ПДн:
* непосредственно от самих субъектов ПДн;
* от третьих лиц (например, федеральных органов исполнительной  
  власти, муниципальных органов, судов общей юрисдикции; органов,  
  осуществляющих контрольные функции по взысканию денежных средств;  
  органов уголовно-исполнительной системы).
  + 1. При сборе ПДн Оператор предоставляет субъекту ПДн по его  
       просьбе следующую информацию:
* подтверждение факта обработки ПДн;
* правовые основания и цели обработки ПДн;
* цели и применяемые способы обработки ПДн;
* наименование и место нахождения Оператора (за исключением  
  работников), которые имеют доступ к персональным данным или которым  
  могут быть раскрыты ПДн на основании договора с Оператором или на  
  основании федерального закона;
* обрабатываемые ПДн, относящиеся к соответствующему субъекту  
  ПДн, источник их получения, если иной порядок представления таких данных

не предусмотрен федеральным законом;

* сроки обработки ПДн, в том числе сроки их хранения;
* порядок осуществления субъектом ПДн прав, предусмотренных  
  настоящим Федеральным законом;
* информацию об осуществлённой или о предполагаемой  
  трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица,  
  осуществляющего обработку ПДн по поручению Оператора, если обработка  
  поручена или будет поручена такому лицу;
* иные сведения, предусмотренные федеральными законами РФ.
  + 1. Оператор вправе ограничить право субъекта ПДн на доступ к его  
       персональным данным в соответствии с федеральными законами, в том числе  
       если доступ субъекта ПДн к его персональным данным нарушает права и  
       законные интересы третьих лиц.
    2. Если ПДн получены не от субъекта ПДн, Оператор, до начала  
       обработки таких ПДн предоставляет субъекту ПДн следующую информацию:
* наименование либо фамилия, имя, отчество и адрес Оператора или  
  его представителя;
* цель обработки ПДн и ее правовое основание;
* предполагаемые пользователи ПДн;
* права субъекта ПДн;
* источник получения ПДн.

Оператор освобождается от обязанности предоставить субъекту ПДн  
указанные сведения в случаях, если:

* субъект ПДн уведомлен об осуществлении обработки его ПДн  
  Оператором;
* ПДн получены Оператором на основании федерального закона или  
  в связи с исполнением договора, стороной которого либо  
  выгодоприобретателем или поручителем по которому является субъект ПДн;
* ПДн сделаны общедоступными субъектом ПДн или получены из  
  общедоступного источника;
* Оператор осуществляет обработку ПДн для статистических или  
  иных исследовательских целей, для осуществления профессиональной  
  деятельности журналиста либо научной, литературной или иной творческой  
  деятельности, если при этом не нарушаются права и законные интересы  
  субъекта ПДн;
* предоставление субъекту ПДн сведений нарушает права и законные  
  интересы третьих лиц.
  1. Оператор предоставляет ПДн субъектов ПДн непосредственно  
     самим субъектам ПДн.
  2. Трансграничная передача ПДн

Трансграничная передача обрабатываемых ПДн работников Оператора не  
осуществляется.

* 1. Сроки обработки ПДн.
     1. Общий срок обработки ПДн определяется периодом времени, в  
        течение которого Оператор осуществляет действия (операции) в отношении  
        ПДн, обусловленные заявленными целями их обработки, в том числе хранение  
        ПДн.
     2. Обработка ПДн начинается с момента их получения Оператором и  
        заканчивается:
* по достижении конкретных, заранее определенных и законных  
  целей;
* по факту утраты необходимости в достижении заранее заявленных  
  целей обработки.
  + 1. Оператор осуществляет хранение ПДн в форме, позволяющей  
       определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн.
    2. Сроки хранения ПДн определяются в соответствии с Приказом  
       Минкультуры РФ от 25.08.2010 №558 «Об утверждении «Перечня типовых  
       управленческих архивных документов, образующихся в процессе деятельности  
       государственных органов, органов местного самоуправления и организаций, с  
       указанием сроков хранения», сроком исковой давности, требований  
       действующих нормативных и правовых актов Российской Федерации и  
       локальных документов Оператора
  1. Согласие субъекта ПДн на обработку его ПДн.
     1. Субъект ПДн принимает решение о предоставлении его ПДн и  
        дает согласие Оператору на их обработку свободно, своей волей и в своем  
        интересе. Согласие на обработку ПДн должно быть конкретным,  
        информированным и сознательным. Согласие на обработку ПДн может быть  
        дано субъектом ПДн или его представителем в любой позволяющей  
        подтвердить факт его получения форме, если иное не установлено  
        федеральным законом. В случае получения согласия на обработку ПДн от  
        представителя субъекта ПДн полномочия данного представителя на дачу  
        согласия от имени субъекта ПДн проверяются Оператором.
     2. Согласие на обработку ПДн может быть отозвано субъектом ПДн.  
        В случае отзыва субъектом ПДн согласия на обработку ПДн Оператор вправе  
        продолжить обработку ПДн без согласия субъекта ПДн при наличии  
        соответствующих оснований, предусмотренных действующим  
        законодательством в области ПДн.
     3. Обязанность предоставить доказательство получения согласия  
        субъекта ПДн на обработку его ПДн или доказательство наличия оснований,  
        предусмотренных действующим законодательством в области ПДн, возлагается  
        на Оператора.
     4. В случаях, предусмотренных федеральным законом, обработка  
        ПДн осуществляется только с согласия в письменной форме субъекта ПДн.  
        Равнозначным содержащему собственноручную подпись субъекта ПДн  
        согласию в письменной форме на бумажном носителе признается согласие в  
        форме электронного документа, подписанного в соответствии с федеральным  
        законом электронной подписью. Согласие в письменной форме субъекта ПДн  
        на обработку его ПДн должно включать в себя, в частности:
* фамилию, имя, отчество, адрес субъекта ПДн, номер основного  
  документа, удостоверяющего его личность, сведения о дате выдачи указанного  
  документа и выдавшем его органе;
* фамилию, имя, отчество, адрес представителя субъекта ПДн, номер  
  основного документа, удостоверяющего его личность, сведения о дате выдачи  
  указанного документа и выдавшем его органе, реквизиты доверенности или  
  иного документа, подтверждающего полномочия этого представителя (при  
  получении согласия от представителя субъекта ПДн);
* наименование и адрес Оператора, получающего согласие субъекта ПДн;
* цель обработки ПДн;
* перечень ПДн, на обработку которых дается согласие субъекта ПДн;
* наименование или фамилию, имя, отчество и адрес лица,  
  осуществляющего обработку ПДн по поручению Оператора, если обработка  
  будет поручена такому лицу;
* перечень действий с персональными данными, на совершение  
  которых дается согласие, общее описание используемых Оператором способов  
  обработки ПДн;
* срок, в течение которого действует согласие субъекта ПДн, а также  
  способ его отзыва;
* подпись субъекта ПДн.
  + 1. В случае недееспособности субъекта ПДн согласие на обработку  
       его ПДн дает законный представитель субъекта ПДн.
    2. В случае смерти субъекта ПДн согласие на обработку его ПДн  
       дают наследники субъекта ПДн, если такое согласие не было дано субъектом  
       ПДн при его жизни.
    3. ПДн могут быть получены Оператором от лица, не являющегося  
       субъектом ПДн, при условии предоставления оператору подтверждения  
       наличия соответствующих оснований, предусмотренных действующим  
       законодательством в области ПДн.
  1. Доступ к персональным данным
     1. Доступ к персональным данным работников Оператора имеют  
        должностные лица Оператора, непосредственно использующие эти данные в  
        рамках выполнения своих должностных обязанностей.
     2. Доступ к персональным данным других лиц имеют должностные  
        лица Оператора, непосредственно использующие их в рамках выполнения  
        своих должностных обязанностей.
     3. Доступ к персональным данным других лиц и третьих лиц  
        разрешается только при наличии официального заявления запросившего их  
        лица с указанием перечня необходимой информации, целей для которых она  
        будет использована, с согласия субъекта ПДн, ПДн которого затребованы.
     4. Сообщение сведений о ПДн субъекта ПДн его родственникам,  
        членам семьи, иным близким ему людям также производится Оператором  
        только при наличии письменного согласия субъекта ПДн.
     5. При передаче ПДн другим лицам, третьим лицам, в том числе  
        представителям субъектов ПДн, в порядке, установленном нормативными  
        правовыми актами РФ и настоящими Правилами, передаваемая информация  
        ограничивается только теми персональными данными, которые необходимы  
        для выполнения другими лицами и третьими лицами их функций.
     6. Субъект ПДн, о котором запрашиваются сведения, относящиеся к  
        персональным данным, должен быть уведомлён о передаче его ПДн другим  
        лицам и третьим лицам.
     7. Запрещается передача ПДн, в том числе их распространение,  
        предоставление и доступ к ним в коммерческих целях без согласия субъекта  
        ПДн, а также иное использование ПДн в неслужебных целях.
  2. Устранение Оператором нарушений законодательства, допущенных  
     при обработке ПДн. Уточнение, блокирование и уничтожение ПДн.
     1. В случае выявления неправомерной обработки ПДн при  
        обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн  
        или его представителя либо уполномоченного органа по защите прав субъектов  
        ПДн Оператор осуществляет блокирование неправомерно обрабатываемых  
        ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование  
        (если обработка ПДн осуществляется другим лицом, действующим по  
        поручению Оператора) с момента такого обращения или получения указанного  
        запроса на период проверки.
     2. В случае выявления неточных ПДн при обращении субъекта ПДн  
        или его представителя либо по их запросу или по запросу уполномоченного  
        органа по защите прав субъектов ПДн Оператор осуществляет блокирование  
        ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование  
        (если обработка ПДн осуществляется другим лицом, действующим по  
        поручению Оператора) с момента такого обращения или получения указанного  
        запроса на период проверки, если блокирование ПДн не нарушает права и  
        законные интересы субъекта ПДн или третьих лиц.
     3. В случае выявления неправомерной обработки ПДн,  
        осуществляемой Оператором или лицом, действующим по поручению  
        Оператора, в срок, не превышающий трех рабочих дней с даты этого  
        выявления, прекращает неправомерную обработку ПДн или обеспечивает  
        прекращение неправомерной обработки ПДн лицом, действующим по  
        поручению Оператора. В случае, если обеспечить правомерность обработки  
        ПДн невозможно, в срок, не превышающий десяти рабочих дней с даты  
        выявления неправомерной обработки ПДн, уничтожает такие ПДн или  
        обеспечивает их уничтожение. Об устранении допущенных нарушений или об  
        уничтожении ПДн Оператор уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос  
        уполномоченного органа по защите прав субъектов ПДн были направлены  
        уполномоченным органом по защите прав субъектов ПДн, также указанный  
        орган.
     4. В случае достижения цели обработки ПДн Оператор прекращает  
        обработку ПДн или обеспечивает ее прекращение (если обработка ПДн  
        осуществляется другим лицом, действующим по поручению Оператора) и  
        уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн  
        осуществляется другим лицом, действующим по поручению Оператора) в срок,  
        не превышающий тридцати дней с даты достижения цели обработки ПДн, если  
        иное не предусмотрено договором, стороной которого, выгодоприобретателем

или поручителем по которому является субъект ПДн, иным соглашением  
между Операторами субъектом ПДн, либо если Оператор не вправе  
осуществлять обработку ПДн без согласия субъекта ПДн на основаниях,  
предусмотренных действующим законодательством в области ПДн.

1. **Правила работы с обезличенными персональными данными**

Условия обезличивания

* 1. Обезличивание ПДн может быть проведено с целью ведения  
     статистических данных, снижения ущерба от разглашения защищаемых ПДн,  
     снижения класса информационных систем персональных данных и по  
     достижению целей обработки или в случае утраты необходимости в  
     достижении этих целей, если иное не предусмотрено федеральным законом.
  2. Способы обезличивания при условии дальнейшей обработки ПДн:
* уменьшение перечня обрабатываемых сведений;
* замена части сведений идентификаторами;
* обобщение - понижение точности некоторых сведений;
* понижение точности некоторых сведений (например, «Место  
  жительства» может состоять из страны, индекса, города, улицы, дома и  
  квартиры, а может быть указан только город)
* деление сведений на части и обработка в разных информационных  
  системах;
* другие способы.
  1. Способом обезличивания в случае достижения целей обработки или  
     в случае утраты необходимости в достижении этих целей является сокращение  
     перечня ПДн.
  2. Для обезличивания ПДн годятся любые способы явно не  
     запрещенные законодательно.
  3. Перечень должностей государственных гражданских служащих,  
     ответственных за проведение мероприятий по обезличиванию обрабатываемых  
     ПДн ([Приложение 11](#Приложение11));
  4. Руководитель учреждения принимает решение о необходимости  
     обезличивания ПДн;
  5. Начальники отделов, непосредственно осуществляющие обработку  
     ПДн, готовят предложения по обезличиванию ПДн, обоснование такой  
     необходимости и способ обезличивания;
  6. Сотрудники подразделений, обслуживающих базы данных с  
     персональными данными, совместно с ответственным за организацию  
     обработки ПДн, осуществляют непосредственное обезличивание выбранным  
     способом.

Порядок работы с обезличенными персональными данными

* 1. Обезличенные ПДн не подлежат разглашению и нарушению  
     конфиденциальности.
  2. Обезличенные ПДн могут обрабатываться с использования и без  
     использования средств автоматизации.
  3. При обработке обезличенных ПДн с использованием средств  
     автоматизации необходимо соблюдение:
* парольной политики;
* антивирусной политики;
* правил работы со съемными носителями (если они используется);
* правил резервного копирования;
* правил доступа в помещения, где расположены элементы  
  информационных систем;
  1. При обработке обезличенных ПДн без использования средств  
     автоматизации необходимо соблюдение:
* правил хранения бумажных носителей;
* правил доступа к ним и в помещения, где они хранятся.

1. **Правила рассмотрения операторами запросов субъектов персональных  
   данных или их представителей**
2. В случае обращения субъекта ПДн либо при получении запроса  
   субъекта ПДн или его представителя, а также уполномоченного органа по  
   защите прав субъектов ПДн оператор обязан:
3. сообщить субъекту ПДн или его представителю информацию о  
   наличии ПДн, относящихся к соответствующему субъекту ПДн, а также о  
   возможности ознакомления с этими персональными данными при обращении  
   субъекта ПДн или его представителя в течение 30 дней с даты получения  
   запроса субъекта ПДн или его представителя;
4. в случае отказа в предоставлении информации о наличии ПДн о  
   соответствующем субъекте ПДн дать в письменной форме мотивированный  
   ответ, содержащий ссылку на норму Федерального закона № 152-ФЗ,  
   являющуюся основанием для такого отказа в срок, не превышающий 30 дней со  
   дня обращения субъекта ПДн или его представителя, либо с даты получения  
   запроса субъекта ПДн или его представителя;
5. предоставить безвозмездно субъекту ПДн или его представителю  
   возможность ознакомления с персональными данными, относящимися к этому  
   субъекту ПДн;
6. в срок, не превышающий семи рабочих дней со дня предоставления  
   субъектом ПДн или его представителем сведений, подтверждающих, что ПДн  
   являются неполными, неточными или неактуальными, внести в них  
   необходимые изменения;
7. в срок, не превышающий семи рабочих дней со дня предоставления  
   субъектом ПДн или его представителем сведений, подтверждающих, что ПДн  
   являются незаконно полученными или не являются необходимыми для  
   заявленной цели обработки, уничтожить такие ПДн;
8. уведомить субъекта ПДн или его представителя о внесенных  
   изменениях и предпринятых мерах и принять разумные меры для уведомления  
   третьих лиц, которым ПДн этого субъекта были переданы.
9. В случае получения запроса уполномоченного органа по защите  
   прав субъектов ПДн оператор обязан направить необходимую информацию в  
   течение 30 дней с даты получения такого запроса.

Право субъекта персональных данных на доступ к его персональным данным

1. Субъект ПДн имеет право на получение следующих сведений  
   ([Приложение 27](#Приложение27)):

* подтверждение факта обработки ПДн оператором;
* правовые основания и цели обработки ПДн;
* цели и применяемые оператором способы обработки ПДн;
* наименование и место нахождения оператора, сведения о лицах (за  
  исключением работников оператора), которые имеют доступ к персональным  
  данным или которым могут быть раскрыты ПДн на основании договора с  
  оператором или на основании федерального закона;
* обрабатываемые ПДн, относящиеся к соответствующему субъекту  
  ПДн, источник их получения, если иной порядок представления таких данных  
  не предусмотрен федеральным законом;
* сроки обработки ПДн, в том числе сроки их хранения;
* порядок осуществления субъектом ПДн прав, предусмотренных  
  настоящим Федеральным законом;
* информацию об осуществленной или о предполагаемой  
  трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица,  
  осуществляющего обработку ПДн по поручению оператора, если обработка  
  поручена или будет поручена такому лицу.

1. Субъект ПДн вправе требовать от оператора уточнения  
   ([Приложение 26](#Приложение26)) его ПДн, их блокирования ([Приложение 25](#Приложение25)) или уничтожения  
   ([Приложение 24](#Приложение24)) в случае, если ПДн являются неполными, устаревшими,  
   неточными, незаконно полученными или не являются необходимыми для  
   заявленной цели обработки, а также принимать предусмотренные законом  
   меры по защите своих прав.
2. Сведения о ПДн должны быть предоставлены субъекту ПДн  
   оператором в доступной форме, и в них не должны содержаться ПДн,  
   относящиеся к другим субъектам ПДн, за исключением случаев, если имеются  
   законные основания для раскрытия таких ПДн.
3. ПДн предоставляются субъекту ПДн или его представителю  
   оператором при обращении либо при получении запроса субъекта ПДн или его  
   представителя. Запрос должен содержать номер основного документа,  
   удостоверяющего личность субъекта ПДн или его представителя, сведения о  
   дате выдачи указанного документа и выдавшем его органе, сведения,  
   подтверждающие участие субъекта ПДн в отношениях с оператором (номер  
   договора, дата заключения договора, условное словесное обозначение и (или)  
   иные сведения), либо сведения, иным образом подтверждающие факт  
   обработки ПДн оператором, подпись субъекта ПДн или его представителя.

Запрос может быть направлен в форме электронного документа и подписан  
электронной подписью в соответствии с законодательством Российской  
Федерации.

1. В случае если ПДн, а также обрабатываемые ПДн были  
   предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн  
   вправе обратиться повторно к оператору или направить ему повторный запрос в  
   целях получения ПДн и ознакомления с такими персональными данными не  
   ранее чем через тридцать дней после первоначального обращения или  
   направления первоначального запроса, если более короткий срок не установлен  
   федеральным законом, принятым в соответствии с ним нормативным правовым  
   актом или договором, стороной которого либо выгодоприобретателем или  
   поручителем по которому является субъект ПДн.
2. Субъект ПДн вправе обратиться повторно к оператору или  
   направить ему повторный запрос в целях получения сведений, указанных в  
   пункте 12.3, а также в целях ознакомления с обрабатываемыми персональными  
   данными до истечения срока, указанного в пункте 12.5, в случае, если такие  
   сведения и (или) обрабатываемые ПДн не были предоставлены ему для  
   ознакомления в полном объеме по результатам рассмотрения первоначального  
   обращения. Повторный запрос наряду со сведениями, указанными в пункте

2.3, должен содержать обоснование направления повторного запроса.

1. Оператор вправе отказать субъекту ПДн в выполнении повторного  
   запроса, не соответствующего условиям, предусмотренным пунктами 12.3 и

2.4. Такой отказ должен быть мотивированным. Обязанность представления  
доказательств обоснованности отказа в выполнении повторного запроса лежит  
на операторе.

Ограничения на право субъекта персональных данных на доступ к его

персональным данным

1. Право субъекта ПДн на доступ к его персональным данным может  
   быть ограничено в соответствии с федеральными законами, в том числе если:
2. обработка ПДн, включая ПДн, полученные в результате оперативно

* розыскной, контрразведывательной и разведывательной деятельности,  
  осуществляется в целях обороны страны, безопасности государства и охраны  
  правопорядка;

1. обработка ПДн осуществляется органами, осуществившими  
   задержание субъекта ПДн по подозрению в совершении преступления, либо

предъявившими субъекту ПДн обвинение по уголовному делу, либо  
применившими к субъекту ПДн меру пресечения до предъявления обвинения,  
за исключением предусмотренных уголовно-процессуальным

законодательством Российской Федерации случаев, если допускается  
ознакомление подозреваемого или обвиняемого с такими персональными  
данными;

1. обработка ПДн осуществляется в соответствии с законодательством  
   о противодействии легализации (отмыванию) доходов, полученных  
   преступным путем, и финансированию терроризма;
2. доступ субъекта ПДн к его персональным данным нарушает права и  
   законные интересы третьих лиц;
3. обработка ПДн осуществляется в случаях, предусмотренных  
   законодательством Российской Федерации о транспортной безопасности, в  
   целях обеспечения устойчивого и безопасного функционирования  
   транспортного комплекса, защиты интересов личности, общества и государства  
   в сфере транспортного комплекса от актов незаконного вмешательства.
4. **Разработка модели угроз безопасности персональных данных при их  
   обработке в информационной системе персональных данных**

Модель УБПДн при их обработке в ИСПДн определяет перечень  
актуальных УБПДн, позволяет выявить маловероятные УБПДн, что дает  
возможность существенно снизить затраты на реализацию механизмов защиты  
ПДн на дальнейших этапах работ и разрабатывается в соответствии с  
методическими документами ФСТЭК России «Базовая модель угроз  
безопасности персональных данных при их обработке в информационных  
системах персональных данных» и в случае, когда для обеспечения  
безопасности ПДн используются СКЗИ, ФСБ России «Методические  
рекомендации по обеспечению с помощью криптосредств безопасности ПДн  
при их обработке в информационных системах персональных данных с  
использованием средств автоматизации».

В соответствии с п. 2.4. Методических рекомендации по обеспечению с  
помощью криптосредств безопасности ПДн при их обработке в ИСПДн с  
использованием средств автоматизации:

«В случае обеспечения безопасности персональных данных без  
использования криптосредств при формировании модели угроз используются  
методические документы ФСТЭК России.

В случае определения оператором необходимости обеспечения  
безопасности персональных данных с использованием криптосредств при  
формировании модели угроз используются методические документы ФСТЭК  
России и настоящие Методические рекомендации. При этом из двух  
содержащихся в документах ФСТЭК России и Методических рекомендациях  
однотипных угроз выбирается более опасная.

По согласованию с ФСТЭК России и ФСБ России допускается  
формирование модели угроз только на основании настоящих Методических  
рекомендаций.

При обеспечении безопасности персональных данных при обработке в  
информационных системах, отнесенных к компетенции ФСБ России, модели  
угроз формируются только на основании настоящих Методических  
рекомендаций».

Частная модель УБПДн при их обработке в ИСПДн зависит от  
используемых технологических решений (однопользовательский  
(многопользовательский) режим работы, подключение к ЛВС, подключение к

сети международного обмена Интернет, использование технологии  
удаленного доступа) и от функционального назначения конкретной ИСПДн.

Модель УБПДн составляется для каждой выявленной ИСПДн и  
оформляется в виде документа ([Приложение 29](#Приложение29)).

Модель УБПДн при их обработке в ИСПДн должна:

1. Утверждаться руководителем или начальником подразделения,  
   ответственного за обеспечение безопасности ПДн.
2. Содержать структуру ИСПДн, с указанием характеристик режима  
   обработки ПДн.
3. На основании состава ПДн содержать вывод о категории  
   обрабатываемых ПДн.
4. Содержать объем записей ПДн.
5. Содержать конфигурацию ИСПДн - схематичное взаиморасположение  
   элементов ИСПДн.

При составлении конфигурации необходимо учесть следующие  
элементы:

* группа пользователей ИСПДн;
* АРМ пользователей ИСПДн;
* сервер, например, почтовый, файловый, proxy сервер, сервер  
  приложений, баз данных и другие;
* МЭ;
* сеть общего доступа и (или) международного обмена, например,  
  Интернет.

Пример конфигурации ИСПДн приведен на рисунке 1. Здесь показана  
ИСПДн, основным элементом которой является сервер баз данных. К базе  
данных осуществляют доступ операторы и разработчики ИСПДн, авторизуясь  
под своими доменными учетными записями.

К базе данных также имеют удаленный доступ пользователи филиала.  
Удаленный доступ организуется по сети общего пользования и  
международного обмена Интернет.

1. Содержать в схематичном виде территориальное расположение  
   ИСПДн относительно КЗ.

Пример расположения ИСПДн относительно КЗ приведен на рисунке 2.



Рисунок 1

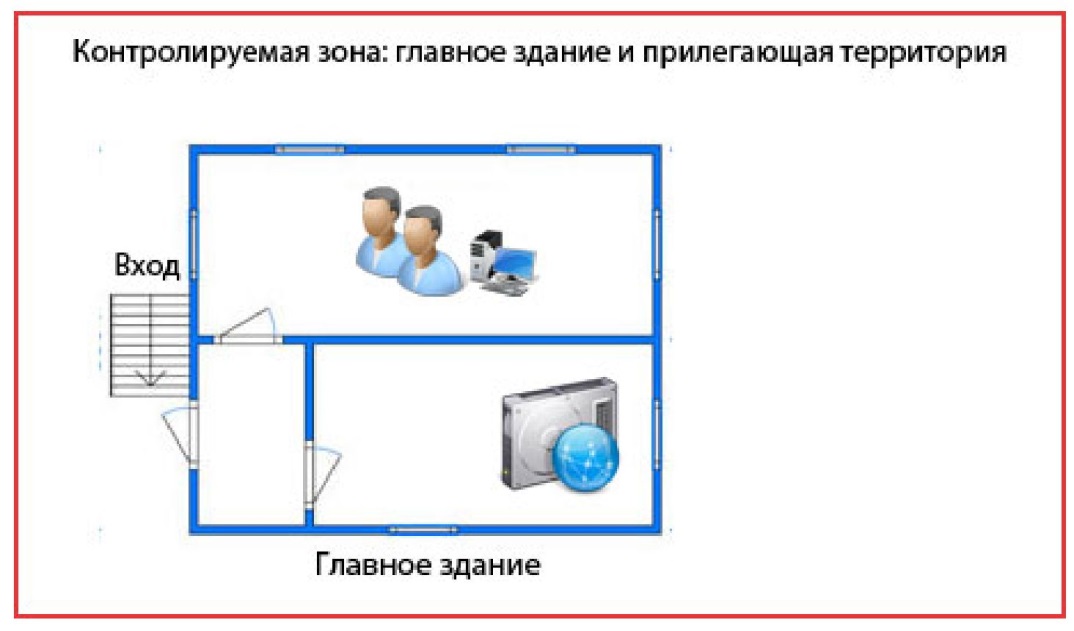


Рисунок 2

1. Содержать описание процесса обработки ПДн в ИСПДн.

Процесс обработки должна включать всю последовательность шагов по  
вводу ПДн, их обработке, передаче в другие ИСПДн и другим процессам.

Пример описания структуры ИСПДн:

* сотрудник отдела кадров авторизуется на своем рабочем месте в ОС Windows XP, рабочей группе, домене;
* сотрудник авторизуется в программном обеспечении  
  автоматизированной информационной системы «TOPAZ:Кадры»;
* сотрудник вносит в программу данные из личного дела  
  работника;
* данные хранятся на сервере MSSQL Server.

1. Содержать поименный список сотрудников, участвующих в обработке  
   ПДн в ИСПДн.
2. Содержать группы пользователей участвующие в обработке ПДн в  
   ИСПДн. Для всех групп должен быть определен перечень прав и уровень  
   доступа. Все это необходимо отразить в матрице доступа.

Пример матрицы доступа:

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия | Сотрудники |
| Системные  администраторы  ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн.  Обладают полной информацией о технических средствах и конфигурации ИСПДн.  Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.  Обладают правами конфигурирования и административной настройки технических средств ИСПДн. | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Администраторы  безопасности  ИСПДн | Обладают правами администратора ИСПДн.  Обладают полной информацией об ИСПДн.  Имеют доступ к СЗИ, средствам  протоколирования и к части ключевых элементов ИСПДн.  Не имеют прав доступа к конфигурированию технических средств сети за исключением контрольных  (инспекционных). | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Ответственные за  обеспечение  безопасности  ПДн | Обладают полной информацией об ИСПДн.  Не имеют прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Операторы  ИСПДн с  правами записи | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Операторы  ИСПДн с  правами чтения | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - использование |  |

1. Содержать классификацию нарушителей.
2. Содержать определение актуальности УБПДн при их обработке в  
   ИСПДн на основании методического документа ФСТЭК России «Методика  
   определения актуальных угроз безопасности персональных данных при их  
   обработке в информационных системах персональных данных».
3. Содержать необходимые меры по снижению опасности актуальных  
   УБПДн при их обработке в ИСПДн в виде перечня реализуемых  
   организационных и технических мероприятий.

С использованием данных об уровне защищенности ИСПДн и  
составленного перечня актуальных угроз, на основании «Состава и содержания  
организационных и технических мер по обеспечению безопасности  
персональных данных при их обработке в информационных системах  
персональных данных», утвержденным приказом директора ФСТЭК России от  
18 февраля 2013 г. № 21 формулируются конкретные организационные,  
технические требования по защите ИСПДн от утечки информации по  
техническим каналам, от НСД и осуществляется выбор программных и

технических СЗИ, которые должны быть внедрены при создании и дальнейшей  
эксплуатации ИСПДн.

Требования к защите, определенные для ИСПДн согласно частной  
модели УБПДн при их обработке в ИСПДн, сопоставляются и суммируются с  
требованиями, определенными для нее согласно ее уровню защищенности.  
При сопоставлении однотипных требований в качестве окончательного  
требования выбирается более жесткое.

1. Содержать сводную таблицу УБПДн при их обработке в ИСПДн.
2. На основании полученных данных содержать заключение об уровне  
   защищенности ИСПДн.

Пример заключения:

В соответствии с Постановлением Правительства Российской Федерации  
от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите  
персональных данных при их обработке в информационных системах  
персональных данных», Приказа ФСТЭК России от 18 февраля 2013 г. № 21  
«Об утверждении Состава и содержания организационных и технических мер  
по обеспечению безопасности персональных данных при их обработке в  
информационных системах персональных данных» и в соответствии с моделью  
угроз безопасности персональных данных информационная система персональных данных (указывается наименование ИСПДн) присваивается уровень защищенности.

1. **Правила осуществления внутреннего контроля соответствия  
   обработки персональных данных требованиям к защите персональных  
   данных**

Настоящие Правила осуществления внутреннего контроля соответствия  
обработки ПДн требованиям к защите ПДн разработаны с учетом Федерального  
закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления  
Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении  
перечня мер, направленных на обеспечение выполнения обязанностей,  
предусмотренных Федеральным Законом «О персональных данных» и  
принятыми в соответствии с ним нормативными правовыми актами,  
операторами, являющимися государственными или муниципальными  
органами» и постановления Правительства Российской Федерации от 1 ноября  
2012 г. № 1119 «Об утверждении требований к защите персональных данных  
при их обработке в информационных системах персональных данных».

В целях осуществления внутреннего контроля соответствия обработки  
ПДн установленным требованиям Оператор организует проведение  
периодических проверок условий обработки ПДн. Проверки осуществляются  
ответственным за организацию обработки ПДн (далее Ответственный) либо  
комиссией, образуемой руководителем учреждения.

Внутренние проверки проводятся по необходимости в соответствии с  
поручением руководителя учреждения.

Проверки осуществляются Ответственным либо комиссией  
непосредственно на месте обработки ПДн путем опроса либо, при  
необходимости, путем осмотра рабочих мест сотрудников, участвующих в  
процессе обработки ПДн.

Для каждой проверки составляется Протокол ([Приложение 32](#Приложение32))  
проведения внутренней проверки. Форма Протокола приведена в Приложении  
к настоящим Правилам.

При выявлении в ходе проверки нарушений, Ответственным либо  
Председателем комиссии в Протоколе делается запись о мероприятиях по  
устранению нарушений и сроках исполнения.

Протоколы хранятся у Ответственного либо Председателя комиссии в  
течение текущего года. Уничтожение Протоколов проводится Ответственным  
либо комиссией самостоятельно в январе следующего за проверочным годом.

О результатах проверки и мерах, необходимых для устранения

нарушений, руководителю учреждения докладывает Ответственный либо  
Председатель комиссии.

*Тематика внутреннего контроля*

Тематика проверок обработки ПДн с использованием средств  
автоматизации:

* соответствие полномочий пользователя матрице доступа;
* соблюдение пользователями информационных систем  
  персональных данных парольной политики;
* соблюдение пользователями информационных систем  
  персональных данных антивирусной политики;
* соблюдение пользователями информационных систем  
  персональных данных правил работы со съемными носителями ПДн;
* соблюдение порядка доступа в помещения, где расположены  
  элементы информационных систем персональных данных;
* соблюдение порядка резервирования баз данных и хранения  
  резервных копий;
* соблюдение порядка работы со средствами защиты информации;
* знание пользователей информационных систем персональных  
  данных о своих действиях во внештатных ситуациях.

Тематика проверок обработки ПДн без использования средств  
автоматизации:

* хранение бумажных носителей с персональными данными;
* доступ к бумажным носителям с персональными данными;
* доступ в помещения, где обрабатываются и хранятся бумажные  
  носители с персональными данными.

1. **Перечень нормативных правовых актов и документов, используемых  
   при организации и проведении мероприятий по обеспечению безопасности  
   персональных данных при их обработке в информационных системах  
   персональных данных**
2. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по  
   обеспечению информационной безопасности Российской Федерации при  
   использовании информационно-телекоммуникационных сетей международного информационного обмена»;
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных  
   данных»;
4. Постановления Правительства Российской Федерации от 1 ноября  
   2012 г. № 1119 «Об утверждении требований к защите персональных данных  
   при их обработке в информационных системах персональных данных»;
5. Постановление Правительства Российской Федерации от 15 сентября

2008г. № 687 «Об утверждении Положения об особенностях обработки  
персональных данных, осуществляемой без использования средств  
автоматизации»;

1. Постановление Правительства Российской Федерации от 6 июля 2008  
   г. № 512 «Об утверждении требований к материальным носителям  
   биометрических персональных данных и технологиям хранения таких данных  
   вне информационных систем персональных данных»;
2. Постановление Правительства РФ от 21.03.2012 № 211 "Об  
   утверждении перечня мер, направленных на обеспечение выполнения  
   обязанностей, предусмотренных Федеральным законом "О персональных  
   данных" и принятыми в соответствии с ним нормативными правовыми актами,  
   операторами, являющимися государственными или муниципальными  
   органами";
3. Указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении  
   Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении  
   Состава и содержания организационных и технических мер по обеспечению  
   безопасности персональных данных при их обработке в информационных  
   системах персональных данных»;
5. Приказ ФСБ России от 9 февраля 2005 г., «Об утверждении  
   Положения о разработке, производстве, реализации и эксплуатации

шифровальных (криптографических) средств защиты информации (Положение  
ПКЗ-2005);

1. Методический документ «Методика определения актуальных угроз  
   безопасности персональных данных при их обработке в информационных  
   системах персональных данных», ФСТЭК России, 14 февраля 2008 г. (пометка  
   «для служебного пользования» снята решением ФСТЭК России от 16 ноября
2. г.), Документ доступен в сети Интернет по адресу:  
   <http://www.fstec.ru/_razd/_isp0o.htm>;
3. Методический документ «Базовая модель угроз безопасности  
   персональных данных при их обработке в информационных системах  
   персональных данных», ФСТЭК России, 14 февраля 2008 г. (для служебного  
   пользования). Выписка из документа доступна в сети Интернет по адресу:  
   <http://www.fstec.ru/_razd/_isp0o.htm>.
4. 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, 21 февраля  
   2008 г., № 149/6/6-622.
5. Методические рекомендации по обеспечению с помощью  
   криптосредств безопасности персональных данных при их обработке в  
   информационных системах персональных данных с использованием средств  
   автоматизации». ФСБ России, 21 февраля 2008 г, № 149/5-144.
6. Приказ Федеральной службы по надзору в сфере связи и массовых  
   коммуникаций от 17 июля 2008 г. № 8 «Об утверждении образца формы  
   уведомления об обработке персональных данных».

**Приложение 1. ПРОЕКТ**

Приказ

о назначении ответственного за защиту информации

(Приказ на бланке организации-оператора)

**О назначении ответственного за защиту информации**

В целях исполнения Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об  
утверждении требований о защите информации, не составляющей государственную тайну,  
содержащейся в государственных информационных системах в (наименование оператора):

ПРИКАЗЫВАЮ:

1. Назначить ответственного за защиту информации в(наименование оператора):  
   Иванова И.И. - занимаемая должность;
2. Ответственному за организацию защиты информации, в срок до

организовать проведение работ по защите информации в соответствие с

требованиями действующего законодательства.

1. Контроль за исполнением настоящего приказа возложить на

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 2. ПРОЕКТ**

Приказ

о создании комиссии по классификации государственной информационной системы

**О создании комиссии по классификации государственной**

**информационной системы**

В целях исполнения Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об  
утверждении требований о защите информации, не составляющей государственную тайну,  
содержащейся в государственных информационных системах в (наименование оператора):

ПРИКАЗЫВАЮ:

1. Создать комиссию по классификации государственной информационной системы  
   составе:

председатель комиссии:

Иванов И.И. - занимаемая должность;

члены комиссии:

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность.

1. Членам комиссии в срок до \_\_\_\_\_\_\_\_\_\_\_ произвести анализ исходных данных и составить акт классификации государственной информационный системы.
2. Контроль за исполнением настоящего приказа возложить на

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 3. ПРОЕКТ**

**Акт классификации государственной информационной системы в**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Комиссия в составе,

председатель комиссии:

Иванов И.И. - занимаемая должность;

члены комиссии:

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность.

в ходе своей работы установила следующее:

1. уровень значимости информации − \_\_\_;
2. масштаб информационной системы − \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

По результатам анализа исходных данных государственной информационной системе присваивается \_\_\_ класс защищенности.

Требования по защищенности для класса защищенности (Согласно Приказу

ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите  
информации, не составляющей государственную тайну, содержащейся в государственных  
информационных системах»):

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Председатель комиссии | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| Члены комиссии: | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| (должность) | (подпись) | (Ф.И.О.) |
| (должность) | (подпись) | (Ф.И.О.) |

**Приложение 4. ПРОЕКТ**

Типовая форма

модели угроз безопасности информации и модели нарушителя в

государственной информационной системе

*(наименование ИС)*

1. Введение

Настоящий документ подготовлен в рамках выполнения работ по построению  
системы защиты информации, не содержащей сведений, составляющих государственную  
тайну.

Настоящий документ содержит модель угроз безопасности и вероятного нарушителя  
(далее - модель угроз) для государственной информационной системы (наименование ИС)  
(далее - ИС).

Модель угроз - документ, определяющий основные исходные условия для проверки  
соответствия СЗ ИС заданным к ней требованиям.

1. **Назначение, структура и основные характеристики ИС**
   1. **Назначение ИС**

Автоматизированная информационная система ИС − это информационный ресурс,

содержащий данные:\_\_\_\_\_\_\_\_\_\_

Автоматизированная система предназначена для\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. **Структура ИС**

Автоматизированная информационная система функционирует на трех уровнях:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Рисунок 1. Схема ИС

Объектами автоматизации в составе ИС являются

Программно-технический комплекс ИС состоит из следующих функциональных  
составляющих:

* серверной части;
* автоматизированные рабочие места администраторов;
* автоматизированные рабочие места пользователей.

Сеть передачи данных (каналы связи) образуют среду функционирования ИС.

В свою очередь, серверная часть программно-технического комплекса  
автоматизировано информационной системы содержит:

* серверы базы данных и хранилища - серверы, отвечающий за хранение всей  
  информации;
* серверы приложений - серверы, обеспечивающий клиент-серверное  
  взаимодействие пользователей с базой и хранилищем данных;
* консолидированное оборудование хранения данных - дисковые массивы,  
  хранящие данные и управляемые сервером базы и хранилища данных.
  1. **Основные характеристики ИС**

Хранимая и обрабатываемая в автоматизированной информационной системе

информация относится к информации составляющей \_\_\_\_\_\_\_\_\_\_.

Автоматизированная информационная система является многопользовательской ИС  
с различными правами доступа пользователей к информационным ресурсам.

Информация консолидировано хранится и обрабатывается на вычислительных  
средствах, расположенных в физически выделенных центрах обработки данных (серверные  
помещения), расположенных в контролируемых зонах. По отношению к указанным центрам  
обработки данных реализован достаточный набор организационных и режимных мер защиты  
информации.

Пользователи осуществляют доступ к информационным ресурсам  
автоматизированной информационной системы в объеме предоставленных полномочий с

АРМ, расположенных в подразделениях . Указанные АРМ расположены в

контролируемых зонах.

Автоматизированная информационная система имеет «частную облачную»  
архитектуру с реализацией клиентских АРМ по принципу работы «тонкий» клиент.  
Обработка и хранение КИ и коммерческой тайны на клиентских АРМ не предусматривается.

Подключения к системе ИС и доступ к информационным ресурсам осуществляется  
установленным порядком с обязательной процедурой согласования.

1. **Определение модели вероятного нарушителя**

Все угрозы безопасности информации ИС подразделяются на два класса:

* **непреднамеренные угрозы** (угрозы, не связанные с деятельностью человека;  
  угрозы социально-политического характера; ошибочные действия персонала и  
  пользователей АИТС; угрозы техногенного характера);
* **атаки**.

**Непреднамеренные угрозы** по своей природе не связаны со злонамеренными  
действиями человека по отношению к АИТС. Но эти угрозы могут не только привести к  
потере, искажению или компрометации информационных активов ИС, но и создать условия,  
которые может использовать в своих целях нарушитель.

Предполагается, что защита от непреднамеренных угроз в основном  
регламентируется инструкциями, разработанными и утвержденными подразделениями,  
эксплуатирующими различные компоненты ИС с учетом особенностей эксплуатации этих  
компонентов и действующей нормативной базы. Поэтому непреднамеренные угрозы далее  
детально не рассматриваются.

Как показывает мировой и отечественный опыт, **атаки** являются наиболее  
опасными угрозами безопасности информации, что обусловлено их тщательной  
подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак.

Атаки готовятся и проводятся нарушителем. При этом возможности проведения атак  
определяются соответствующими возможностями нарушителя.

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках  
разработки модели угроз и нарушителя.

Разработанная и приведенная в настоящем документе модель угроз для ИС  
предназначена для использования при формировании требований информационной  
безопасности и проектных решений по СЗ ИС.

Модель вероятного нарушителя включает:

* описание возможных нарушителей;
* предположения об имеющейся у нарушителя информации об объектах атак;
* предположения об имеющихся у нарушителя средствах атак;
* описание объектов и целей атак;
* описание каналов атак.

Разработка модели угроз базируется на следующих принципах:

* безопасность информации АИТС обеспечивается СЗ ИС, а также используемыми в  
  АИТС информационными технологиями. Технические и программные средства должны  
  удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям,  
  обеспечивающим защиту информации (в т.ч. ПДн);
* СЗ ИС не предназначена для защиты информации от действий, выполняемых в  
  рамках предоставленных субъекту действий полномочий;
* нарушитель может действовать на различных этапах жизненного цикла  
  программных и технических средств АИТС, включая СЗ (разработка, производство,  
  хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических  
  средств АИТС).

На этапах разработки, производства, хранения, транспортировки, ввода в  
эксплуатацию программных и технических средств СЗ ИС не производится обработка  
защищаемой ИКХ. Поэтому объектами атак могут быть только сами эти средства и  
документация на них.

В связи с выше изложенным, на указанных этапах жизненного цикла возможны  
следующие атаки:

* внесение негативных (как правило, недекларированных) функциональных  
  возможностей, в том числе с использованием вредоносного программного обеспечения;
* внесение несанкционированных изменений в документацию на компоненты АИТС  
  и СЗ ИС.

Более сложным для анализа возможностей нарушителя является этап эксплуатации  
СЗ ИС. Именно этот этап жизненного цикла АИТС рассмотрен далее более подробно.

Модель угроз в СЗ ИС разработана на основе данных, полученных в ходе  
информационного обследования СЗ ИС, проведенного в рамках работ по обеспечению  
информационной безопасности СЗ ИС, в том числе обеспечению безопасности КИ при их  
обработке в СЗ ИС.

1. **Описание возможных нарушителей**

По признаку принадлежности к СЗ ИС все нарушители делятся на две группы:

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

Установлены следующие условия функционирования ИС:

* автоматизированные рабочие места ИС функционируют на контролируемых и  
  охраняемых объектах (зданиях, помещениях);
* серверная составляющая ИС, консолидирующая информационные ресурсы (в том  
  числе ПДн), расположена в серверных помещениях, где реализуется весь необходимый и  
  достаточный комплекс программно-технических средств и поддерживающих их  
  организационных мер, в том числе режимных мероприятий;
* подключения к системе ИС и доступ к информационным ресурсам осуществляется  
  установленным в порядком с обязательной процедурой согласования;
* информационные ресурсы ИС не имеют подключений к сетям общего  
  пользования.

Учитывая указанные условия функционирования ИС, предполагается, что  
возможные действия внешнего нарушителя приемлемо нейтрализуются и в дальнейшем  
анализ их действий исключается из рассмотрения в настоящей модели.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от  
действующих в пределах контролируемой зоны ограничительных факторов, из которых  
основным является реализация комплекса режимных и 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 несанкционированных  
действий.

Исходя из особенностей функционирования ИС, допущенные к ней физические  
лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и  
другим ресурсам АИТС в соответствии с принятой политикой информационной  
безопасности (правилами). К внутренним нарушителям могут относиться:

* администраторы ИС (категория I);
* технический персонал ИС сотрудники эксплуатационных подразделений,  
  осуществляющие техническое сопровождение оборудования, программного обеспечения и  
  средств защиты информации) (категория II);
* пользователи ИС (категория III);
* пользователи других АИТС, являющихся внешними по отношению к ИС  
  (категория IV);
* сотрудники, имеющие санкционированный доступ в служебных целях в  
  помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам  
  (категория V);
* обслуживающий персонал (охрана, работники инженерно-технических служб и  
  т.д.) (категория VI);
* уполномоченный персонал разработчиков ИС, который на договорной основе  
  имеет право на техническое обслуживание и модификацию компонентов ИС (категория VII).

На лиц категории I и II возложены задачи по администрированию и техническому  
сопровождению программно-аппаратных средств ИС. Администраторы и технический

персонал ИС потенциально могут проводить атаки, используя возможности по  
непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИС,  
а также к техническим и программным средствам ИС, включая средства защиты,  
используемые в ИС, в соответствии с установленными для них административными  
полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и  
используемыми в ИС, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для  
идентификации уязвимостей, либо для проведения атак. Данное оборудование может быть  
как частью штатных средств, так и может относиться к легко получаемому (например,  
программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать  
специализированным оборудованием.

К лицам категории I и II ввиду их исключительной роли в 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 категории I и II будут включаться только  
доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей исключается  
организационными и режимными мерами.

1. **Предположения об имеющейся у нарушителя информации об объектах атак**

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

* **общая информация** - информация о назначения и общих характеристиках АИТС;
* **эксплуатационная информация** - информация, полученная из эксплуатационной  
  документации;
* **чувствительная информация** - информация, дополняющая эксплуатационную  
  информацию об АИТС (например, сведения из проектной документации АИТС).

В частности, нарушитель может иметь:

* данные об организации работы, структуре и используемых технических,  
  программных и программно-технических средствах ИС;
* сведения об информационных ресурсах 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 ИС;
* данные о реализованных в СЗ принципах и алгоритмах;
* исходные тексты программного обеспечения ИС;
* сведения о возможных каналах атак;
* информацию о способах атак.

Предполагается, что преимущественное большинство лиц категории III и все лица  
категории IV владеют только эксплуатационной информацией, что обеспечивается  
организационными мерами. При этом лица категории IV не владеют парольной,  
аутентифицирующей и ключевой информацией, используемой в ИС, к которой они не имеют  
санкционированного доступа. Однако предполагается, что имеется возможность  
ознакомления незначительного круга лиц категории III с чувствительной информацией о ИС.

Предполагается, что лица категории V владеют в той или иной части  
эксплуатационной и общей информацией об ИС, что обеспечивается организационными  
мерами. При этом лица категории V не владеют парольной, аутентифицирующей и ключевой  
информацией, используемой в ИС, использующих систему передачи информации.

Предполагается, что лица категории VI по уровню знаний не превосходят лица  
категории V.

Предполагается, что лица категории VII обладают чувствительной информацией об  
ИС, включая информацию об уязвимостях технических и программных средств ИС.  
Организационными мерами предполагается исключить доступ лиц категории VII к  
техническим и программным средствам ИС в период обработки защищаемой информации.

Таким образом, наиболее информированными об ИС являются лица категории III и  
лица категории VII.

Степень информированности нарушителя зависит от многих факторов, включая  
реализованные на объектах ИС 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 проведения атак, за исключением информации, доступ к которой со стороны  
нарушителя исключается системой защиты информации. К такой информации, например,  
относится парольная (аутентифицирующая) информация.

1. **Предположения об имеющихся у нарушителя средствах атак**

Предполагается, что внутренний нарушитель имеет:

* программные и аппаратные компоненты СЗИ и СФ СЗИ (штатные средства);
* доступные в свободной продаже технические средства и программное  
  обеспечение;
* специально разработанные технические средства и программное обеспечение.

Состав имеющихся у нарушителя средств, которые он может использовать для

проведения атак, а также возможности по их применению зависят от многих факторов,  
включая реализованные на объектах ИС конкретные организационные меры, финансовые  
возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся  
у нарушителя средств атак в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности  
предполагается, что вероятный нарушитель имеет все необходимые для проведения атак  
средства, возможности которых не превосходят возможности аналогичных средств атак на

информацию, содержащую сведения, составляющие государственную тайну и технические и  
программные средства, обрабатывающие эту информацию.

Вместе с тем (с учетом реализации на объектах функционирования ИС необходимых  
режимных мероприятий) предполагается, что нарушитель не имеет:

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

Предполагается, что наиболее совершенными средствами атак обладают лица

категории III и лица категории VII.

1. **Описание объектов и целей атак**

Основными объектами атак являются:

* защищаемая информация (в том числе ПДн);
* документация на СЗИ и на технические и программные компоненты СФ СЗИ;
* СЗИ (программные и аппаратные компоненты СЗИ);
* технические и программные компоненты СФ СЗИ;
* каналы связи (внутри контролируемой зоны), не защищенные от НСД к  
  информации организационно-техническими мерами;
* помещения, в которых находятся защищаемые ресурсы ИС.

Кроме этого, к объектам атак можно отнести и некоторые каналы атак. К таким  
каналам атак относятся:

* съемные носители информации;
* носители информации, находящиеся за пределами контролируемой зоны в связи с  
  их ремонтом, обслуживанием или передачи для использования;
* носители информации, выведенные из употребления;
* штатные средства ИС.

Дополнительно к возможным объектам атак можно отнести печатные материалы,  
содержащие ИКХ.

Основными информационными активами в ИС являются следующие:

1. Целевая информация:

* коммерческая тайна;
* служебная информация;
* другие виды ИКХ.

1. Технологическая информация:

* защищаемая управляющая информация (конфигурационные файлы, настройки  
  системы защиты и пр.);
* защищаемая технологическая информация средств доступа к системе управления  
  ИС (аутентификационная информация и др.);
* информационные ресурсы ИС на съемных носителях информации (бумажные,  
  магнитные, оптические и пр.), содержащие защищаемую технологическую информацию

системы управления ресурсами ИС(программное обеспечение, конфигурационные файлы,  
настройки системы защиты и пр.) или средств доступа к этим системам управления  
(аутентификационная информация и др.);

* информация о ПСЗИ, их структуре, принципах и технических решениях защиты.

1. Программное обеспечение:

* программные информационные ресурсы ИС, содержащие общее и специальное  
  программное обеспечение, резервные копии общесистемного программного обеспечения,  
  инструментальные средства и утилиты систем управления ресурсами ИС, чувствительные по  
  отношению к случайным и несанкционированным воздействиям, программное обеспечение  
  СЗИ.

Предполагается (с учетом реализации на объектах функционирования ИС  
необходимых режимных мероприятий), что не являются объектами атак:

* технические каналы утечки информации;
* сигнальные цепи (информационные и управляющие интерфейсы СВТ);
* источники и цепи электропитания;
* цепи заземления.

Целью атаки является нарушение определенных для объекта атаки характеристик  
безопасности или создание условий для нарушения характеристик безопасности объекта  
атаки.

1. **Описание каналов атак**

Возможными каналами атак являются:

* каналы непосредственного доступа к объекту атаки (акустический, визуальный,  
  физический);
* штатные средства;
* съемные носители информации;
* носители информации, находящиеся за пределами контролируемой зоны в связи с  
  их ремонтом, обслуживанием или передачей для использования;
* носители информации, выведенные из употребления;
* каналы связи (внутри контролируемой зоны), не защищенные от НСД к  
  информации организационно-техническими мерами;
* канал утечки за счет электронных устройств негласного получения информации.

Предполагается (с учетом реализации на объектах функционирования ИС

необходимых режимных мероприятий), что не являются каналами атак:

* технические каналы утечки;
* сигнальные цепи;
* источники и цепи электропитания;
* цепи заземления;
* каналы активного воздействия на технические средства с помощью облучения.

1. **Основные способы атак**

При определении основных способов атак учитывался принцип защиты на всех  
этапах жизненного цикла ИС и ее компонентов, условия функционирования ИС, а также  
предположения о возможных нарушителях, сформулированные в подразделах 3.1 - 3.3.

Возможны следующие атаки:

1. атаки, основанные на использовании СЗИ с уязвимостями и  
   недокументированными (недекларированными) возможностями, внесенными на этапах  
   разработки, производства, хранения, транспортировки, ввода в эксплуатацию программных и  
   технических средств ИС;
2. перехват разглашаемых сведений о защищаемой информации, о ИС и ее  
   компонентах, включая СЗИ и СФ СЗИ;
3. атаки, основанные на документированных и недокументированных  
   (недекларированных) возможностях оборудования (в том числе за счет модификации IP-  
   трафика при несанкционированном подключении к каналу связи в пределах контролируемой  
   зоны);
4. хищение производственных отходов (распечаток, записей, списанных носителей

и т.п.);

1. восстановление (в том числе и фрагментарное) защищаемой информации и  
   информации о АИТС путем анализа выведенных из употребления и ставших после этого  
   доступными нарушителю съемных носителей информации;
2. считывание или восстановление информации (в том числе и фрагментарное) по  
   остаточным следам на носителях защищаемой информации, сданных в ремонт, на  
   обслуживание, переданных для использования другими пользователями или для  
   использования за пределами ИС;
3. негласное (скрытое) временное изъятие или хищение съемных носителей  
   защищаемой информации, аутентифицирующей или ключевой информации;
4. негласная (скрытая) модификация защищаемой информации, хранящейся на  
   носителях информации (в том числе на съемных носителях информации);
5. визуальный просмотр защищаемой информации, отображаемой на средствах  
   отображения (экранах мониторов);
6. ознакомление с распечатанными документами, содержащими защищаемую  
   информацию;
7. перехват защищаемой информации из каналов связи в пределах контролируемой  
   зоны, незащищенных от НСД к информации организационно-техническими мерами;
8. целенаправленное искажение защищаемой информации в каналах связи в  
   пределах контролируемой зоны, незащищенных от НСД к информации организационно-  
   техническими мерами;
9. навязывание ложной (специально сформированной нарушителем) информации  
   через каналы связи в пределах контролируемой зоны, не защищенные от НСД к информации  
   организационно-техническими мерами;
10. перенаправление потоков данных путем воздействия через каналы связи в  
    пределах контролируемой зоны, незащищенные от НСД к информации организационно-  
    техническими мерами;
11. целенаправленное искажение команд управления, передаваемых по каналам  
    связи в пределах контролируемой зоны, не защищенным от НСД к информации  
    организационно-техническими мерами;
12. нарушение связи за счет преднамеренной загрузки трафика ложными  
    сообщениями, приводящее к исчерпанию пропускной способности каналов связи;
13. доступ к оставленным без присмотра функционирующим штатным средствам;
14. несанкционированное изменение конфигурации технических средств;
15. подбор аутентифицирующей информации пользователей;
16. модификация ведущихся в электронном виде регистрационных протоколов  
    (журналов регистрации);
17. модификация технических средств;
18. модификация программных средств с использованием штатных средств,  
    включая нелегальное внедрение и использование неучтенных программ;
19. модификация программных средств ИС с использованием вредоносных  
    программ, размещенных на съемных носителях информации;
20. модификация программных средств с использованием внедренных в ЕК ИСУ ТР  
    компьютерных вирусов;
21. вызывание сбоев технических средств ИС;
22. внесение неисправностей в технические средства ИС;
23. утечка, модификация, блокирование или уничтожение защищаемой информации  
    с использованием штатных средств;
24. утечка, модификация, блокирование или уничтожение защищаемой информации  
    с использованием вредоносных программ, размещенных на съемных носителях информации;
25. блокирование или уничтожение технических, программных и программно-  
    технических компонентов ИС;
26. несанкционированный доступ к защищаемой информации в процессе ремонтных  
    и регламентных работ;
27. методы социальной инженерии для получения сведений об ИС, способствующих  
    созданию благоприятных условий для применения других методов;
28. несанкционированный доступ к защищаемой информации за счет внедренных в  
    технические средства специальных закладочных устройств, предназначенные для  
    бесконтрольного съема информации.
29. **Модель угроз безопасности информации**

К основным угрозам безопасности информации ИС относятся следующие:

**Угроза 1**

1. **Аннотация угрозы** - осуществление несанкционированного доступа  
   (ознакомления) с целевой информацией при ее обработке и хранении в ИС.
2. **Возможные источники** угрозы - пользователи ИС.
3. **Способ реализации угрозы** - осуществление доступа к целевой информации с  
   использованием штатных средств, предоставляемых ИС.
4. **Используемые уязвимости** - недостатки механизмов разграничения доступа к  
   целевой информации, связанные с возможностью предоставления доступа к целевой  
   информации неуполномоченным на это лицам.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение служебной информации и персональных данных, используемых в ИС.

**Угроза 2**

1. **Аннотация угрозы** - осуществление несанкционированного копирования  
   (хищения) информации, содержащей конфиденциальные сведения (в том числе баз данных  
   ИС).
2. **Возможные источники угрозы**- пользователи ИС.
3. **Способ реализации угрозы** - осуществление действий с использованием  
   штатных средств (предоставляемых ИС), направленных на копирование (выгрузку)  
   информации из баз данных ИС.
4. **Используемые уязвимости** - недостатки механизмов безопасного  
   взаимодействия АРМ пользователей с серверами ИС.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение персональных данных и коммерческой тайны, используемых в ИС.

**Угроза 3**

1. **Аннотация угрозы** - осуществление необнаруженной несанкционированной  
   модификации (подмены) целевой информации (прежде всего, персональных данных и  
   коммерческой тайны).
2. **Возможные источники угрозы** - пользователи ИС.
3. **Способ реализации угрозы** - осуществление необнаруженной модификации  
   (подмены) целевой информации с использованием штатных средств, предоставляемых ИС.
4. **Используемые уязвимости** - недостатки механизмов разграничения доступа к  
   целевой информации и механизмов аудита, связанные с возможностью необнаруженной  
   модификации (подмены) целевой информации неуполномоченными на это лицами.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том  
   числе ПДн и коммерческая тайна).
6. **Нарушаемые характеристики безопасности активов** - целостность;  
   достоверность.
7. **Возможные последствия реализации угрозы** - навязывание должностным  
   лицам модифицированной (ложной) информации; передача по запросам модифицированной  
   (ложной) информации и нарушение режимов функционирования ИС.

**Угроза 4**

1. **Аннотация угрозы** - осуществление необнаруженного несанкционированного  
   блокирования (нарушения доступности) целевой информации.
2. **Возможные источники угрозы** - пользователи ИС; пользователи других АИТС,  
   являющихся внешними по отношению к ИС.
3. **Способ реализации угрозы** - осуществление необнаруженного блокирования  
   доступности целевой информации с использованием штатных средств ИС, предоставляемых ИС, а также с использованием специализированных инструментальных средств.
4. **Используемые уязвимости** - недостатки механизмов безопасного  
   администрирования сервисов, предоставляемых ИС а также механизмов аудита, связанные с возможностью бесконтрольного несанкционированного блокирования доступности целевой информации.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том  
   числе служебная информация и ПДн).
6. **Нарушаемые характеристики безопасности активов** - доступность.
7. **Возможные последствия реализации угрозы** - непредставление целевой  
   информации заинтересованным лицам в отведенные временные интервалы; нарушение  
   штатного режима функционирования ИС.

**Угроза 5**

1. **Аннотация угрозы** - перехват защищаемой информации в каналах связи (каналах  
   передачи данных) с использованием специально разработанных технических средств и  
   программного обеспечения (специализированных программно-технических средств).
2. **Возможные источники угрозы** - пользователи ИС; пользователи других АИТС,  
   являющихся внешними по отношению к ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - перехват целевой и технологической информации с  
   использованием специально разработанных технических средств и программного  
   обеспечения, не входящих в состав ИС.
4. **Используемые уязвимости** - недостатки механизмов защиты передаваемой  
   информации, связанные с возможностью ее перехвата из каналов связи и последующего с  
   ней ознакомления.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том  
   числе ПДн и коммерческая информация); технологическая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение персональных данных и коммерческой информации,  
   используемых в ИС; несанкционированное ознакомление с принципами функционирования  
   механизмов защиты в ИС, создание предпосылок к подготовке и проведению атак на  
   информационные ресурсы ИС.

**Угроза 6**

1. **Аннотация угрозы** - внедрение в ИС компьютерных вирусов.
2. **Возможные источники угрозы** - пользователи ИС; уполномоченный персонал  
   разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - внедрение компьютерных вирусов при  
   взаимодействии с внешними системами (выгрузка баз данных, файловый обмен и т.п.), а

также при использовании съемных носителей информации на автоматизированных рабочих  
местах пользователей ИС.

1. **Используемые уязвимости**- недостатки механизмов защиты информационных  
   ресурсов ИС от компьютерных вирусов.
2. **Вид активов, потенциально подверженных угрозе** - программное обеспечение.
3. **Нарушаемые характеристики безопасности активов** - целостность.
4. **Возможные последствия реализации угрозы** - нарушение режимов  
   функционирование ИС; реализация различного рода негативных информационных  
   воздействий на целевую, технологическую информацию и программное обеспечение ИС.

**Угроза 7**

1. **Аннотация угрозы** - осуществление необнаруженных несанкционированных  
   информационных воздействий (направленных на «отказ в обслуживании» для сервисов,  
   модификацию конфигурационных данных программно-аппаратных средств, подбор  
   аутентификационной информации и т.п.) на программно-аппаратные элементы ИС.
2. **Источники угрозы** - пользователи ИС; пользователи других АИТС, являющихся внешними по отношению к ИС.
3. **Способ (метод) реализации угрозы** - несанкционированные информационные  
   воздействия (направленные на «отказ в обслуживании» для сервисов, модификацию  
   конфигурационных данных программно-аппаратных средств, подбор аутентификационной  
   информации и т.п.) с использованием специализированного программно-аппаратного  
   обеспечения.
4. **Используемые уязвимости** - недостатки механизмов защиты программно-  
   аппаратных элементов ИС от несанкционированных внешних воздействий.
5. **Вид активов, потенциально подверженных угрозе** - технологическая  
   информация; программное обеспечение.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность,  
   целостность.
7. **Возможные последствия реализации угрозы** - нарушение режимов  
   функционирования ИС; снижение уровня защищенности ИС; подготовка к последующим  
   воздействиям и осуществление несанкционированного доступа к защищаемым  
   информационным ресурсам ЕК ИСУ ТР.

**Угроза 8**

1. **Аннотация угрозы** - осуществление несанкционированного доступа к  
   информационным активам, основанное на использовании СЗИ, телекоммуникационного  
   оборудования с уязвимостями и недокументированными (недекларированными)  
   возможностями, внесенными на этапах разработки, производства, хранения,  
   транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и  
   технических средств ЕК ИСУ ТР.
2. **Возможные источники угрозы** - пользователи ИС, уполномоченный персонал  
   разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - использование необнаруженных уязвимостей и  
   недокументированных (недекларированных) возможностей СЗИ, телекоммуникационного  
   оборудования.
4. **Используемые уязвимости** - наличие недокументированных  
   (недекларированных) возможностей, внесенных на этапах разработки, производства,  
   хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств ИС.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том  
   числе ПДн и коммерческая тайна), технологическая информация, программное обеспечение.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность,  
   целостность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации; нарушение режимов  
   функционирования ИС.

**Угроза 9**

1. **Аннотация угрозы** - осуществление несанкционированного доступа к  
   защищаемой информации, основанное на восстановлении (в том числе фрагментарном)  
   остаточной информации путем анализа выведенных из употребления, сданных в ремонт, на  
   обслуживание, переданных для использования другим пользователям или для использования за пределами ИС носителей информации.
2. **Возможные источники угрозы** - пользователи ИС, уполномоченный персонал  
   разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - восстановление остаточной информации на  
   носителях защищаемой информации с использованием специализированных  
   инструментальных средств.
4. **Используемые уязвимости** - недостатки механизмов гарантированного  
   уничтожения защищаемой информации, связанные с возможностью ее последующего  
   несанкционированного восстановления.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе ПДн и коммерческая тайна), технологическая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации.

**Угроза 10**

1. **Аннотация угрозы** - целенаправленное искажение, навязывание ложной  
   (специально сформированной нарушителем) защищаемой информации в каналах связи  
   (каналах передачи данных), с использованием специально разработанных технических  
   средств и программного обеспечения (специализированных программно-технических  
   средств).
2. **Возможные источники угрозы** - пользователи ИС; пользователи других АИТС,  
   являющихся внешними по отношению к ИС; персонал разработчиков ИС, который на

договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.

1. **Способ реализации угрозы** - осуществление целенаправленного искажения,  
   навязывание ложной (специально сформированной нарушителем) защищаемой информации  
   с использованием специально разработанных технических средств и программного  
   обеспечения (специализированных программно-технических средств), не входящих в состав ИС.
2. **Используемые уязвимости** - недостатки механизмов защиты информации,  
   передаваемой по каналам связи, связанные с возможностью ее искажения и навязывания  
   ложной информации.
3. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе ПДн и коммерческая тайна); технологическая информация.
4. **Нарушаемые характеристики безопасности активов** - целостность,  
   достоверность.
5. **Возможные последствия реализации угрозы** - навязывание должностным  
   лицам искаженной, ложной (специально сформированной нарушителем) информации;  
   нарушение режимов функционирования ИС.

**Угроза 11**

1. **Аннотация угрозы** - целенаправленное блокирование защищаемой информации  
   в каналах связи (каналах передачи данных), с использованием специально разработанных  
   технических средств и программного обеспечения (специализированных программно-  
   технических средств).
2. **Возможные источники угрозы** - пользователи ИС; пользователи других АИТС,  
   являющихся внешними по отношению к ИС; уполномоченный персонал разработчиков ИС,  
   который на договорной основе имеет право на техническое обслуживание и модификацию  
   компонентов ИС.
3. **Способ реализации угрозы** - осуществление целенаправленного блокирования  
   защищаемой информации с использованием специально разработанных технических средств  
   и программного обеспечения (специализированных программно-технических средств), не  
   входящих в состав ИС.
4. **Используемые уязвимости** - недостатки механизмов защиты передаваемой  
   информации, связанные с возможностью ее блокирования в каналах связи.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе ПДн и коммерческая тайна); технологическая информация.
6. **Нарушаемые характеристики безопасности активов** - доступность.
7. **Возможные последствия реализации угрозы** - непредставление целевой  
   информации заинтересованным лицам в отведенные временные интервалы; нарушение  
   штатного режима функционирования ИС; срыв выполнения поставленных задач.

**Угроза 12**

1. **Аннотация угрозы** - внедрение в ИС вредоносного программного обеспечения.
2. **Возможные источники угрозы** - пользователи ИС; уполномоченный персонал  
   разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - внедрение вредоносного программного  
   обеспечения при взаимодействии с внешними системами (выгрузка баз данных, файловый  
   обмен и т.п.), а также при использовании съемных носителей информации на  
   автоматизированных рабочих местах пользователей и администраторов ИС.
4. **Используемые уязвимости** - недостатки механизмов защиты информационных  
   ресурсов ИС от вредоносного программного обеспечения.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация;  
   технологическая информация; программное обеспечение.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность;  
   целостность; доступность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение коммерческой тайны и персональных данных; создание  
   предпосылок к подготовке и проведению атак на информационные ресурсы ИС; нарушение  
   режимов функционирование ИС; реализация различного рода негативных воздействий на  
   целевую, технологическую информацию и программное обеспечение ИС.

**Угроза 13**

1. **Аннотация угрозы** - перехват разглашаемых сведений о защищаемой  
   информации, о ИС и ее компонентах, включая СЗИ и СФ СЗИ.
2. **Возможные источники угрозы** - сотрудники, имеющие санкционированный  
   доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие  
   права доступа к активам; обслуживающий персонал (охрана, работники инженерно-  
   технических служб и т.д.); уполномоченный персонал разработчиков ИС, который на  
   договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - осуществление перехвата разглашаемых сведений о  
   защищаемой информации, о ИС и ее компонентах, включая СЗИ и СФ СЗИ путем прямого  
   прослушивания, а также с использованием специализированных инструментальных средств.
4. **Используемые уязвимости** - недостатки реализации необходимых  
   организационно-режимных мероприятий на объектах ИС, связанные с возможностью  
   перехвата разглашаемой защищаемой информации.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе ПДн и коммерческая тайна); аутентификационная информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации; создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС.

**Угроза 14**

1. **Аннотация угрозы** - хищение производственных отходов (распечаток, записей,  
   списанных носителей) с целью последующего анализа и несанкционированного  
   ознакомления с целевой и технологической информацией.
2. **Возможные источники угрозы** - сотрудники, имеющие санкционированный  
   доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие  
   права доступа к активам; обслуживающий персонал (охрана, работники инженерно-

технических служб и т.д.); уполномоченный персонал разработчиков ИС, который на  
договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.

1. **Способ реализации угрозы** - осуществление прямого хищения  
   производственных отходов (распечаток, записей, списанных носителей).
2. **Используемые уязвимости** - недостатки организационно-технических мер,  
   обеспечивающих гарантированное уничтожение производственных отходов в ИС, связанные  
   с возможностью их несанкционированного хищения и последующего использования для  
   проведения аналитических исследований.
3. **Вид активов, потенциально подверженных угрозе** - целевая информация (в т.ч. ПДн и коммерческая тайна); технологическая информация.
4. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
5. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС.

**Угроза 15**

1. **Аннотация угрозы** - осуществление несанкционированного визуального  
   просмотра защищаемой информации, отображаемой на средствах отображения (экранах  
   мониторов), а также несанкционированное ознакомление с распечатываемыми документами, содержащими защищаемую информацию.
2. **Возможные источники угрозы** - сотрудники, имеющие санкционированный  
   доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие  
   права доступа к активам; обслуживающий персонал (охрана, работники инженерно-  
   технических служб и т.д.); уполномоченный персонал разработчиков ИС, который на  
   договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - осуществление несанкционированного визуального  
   просмотра защищаемой информации, отображаемой на средствах отображения (экранах  
   мониторов), несанкционированного ознакомления с распечатываемыми документами,  
   содержащими защищаемую информацию.
4. **Используемые уязвимости** - недостатки реализации необходимых  
   организационно-режимных мероприятий на объектах ИС, связанные с возможностью  
   несанкционированного визуального просмотра защищаемой информации на средствах  
   отображения (экранах мониторов), а так же несанкционированного ознакомления с  
   распечатываемыми документами, содержащими защищаемую информацию.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе ПДн и коммерческая тайна); технологическая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС.

**Угроза 16**

1. **Аннотация угрозы** - преднамеренное осуществление сбоев, внесение  
   неисправностей, уничтожение технических и программно-технических компонентов ИС.
2. **Возможные источники угрозы** - пользователи ИС; уполномоченный персонал  
   разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.
3. **Способ реализации угрозы** - осуществление сбоев, внесение неисправностей,  
   уничтожение технических и программно-технических компонентов ИС путем  
   непосредственного физического воздействия.
4. **Используемые уязвимости** - недостатки механизмов физической защиты  
   компонентов ИС, связанные с возможностью осуществления сбоев, внесения  
   неисправностей, уничтожения технических, и программно-технических компонентов ИС.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в т.ч. ПДн и коммерческая тайна), технологическая информация, программное обеспечение.
6. **Нарушаемые характеристики безопасности активов** - доступность,  
   целостность.
7. **Возможные последствия реализации угрозы** - непредоставление целевой  
   информации заинтересованным лицам в отведенные временные интервалы; нарушение  
   штатного режима функционирования ИС; срыв выполнения поставленных задач.

**Угроза 17**

1. **Аннотация угрозы** - осуществление несанкционированного доступа к  
   защищаемой информации в процессе ремонтных и регламентных работ.
2. **Возможные источники угрозы** - уполномоченный персонал разработчиков ИС,  
   который на договорной основе имеет право на техническое обслуживание и модификацию  
   компонентов ИС.
3. **Способ реализации угрозы** - осуществление несанкционированного доступа к  
   защищаемой информации в процессе ремонтных и регламентных работ.
4. **Используемые уязвимости** -доступ лиц, имеющих право на техническое  
   обслуживание, к техническим и программным средствам ИС в момент обработки с  
   использованием этих средств защищаемой информации.
5. **Вид активов, потенциально подверженных угрозе** - целевая информация (в т.ч. ПДн и коммерческая тайна), технологическая информация.
6. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
7. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке  
   и проведению атак на информационные ресурсы ИС; нарушение режимов  
   функционирование ИС.

**Угроза 18**

1. **Аннотация угрозы** - осуществление несанкционированного доступа к  
   оставленным без присмотра функционирующим штатным средствам.
2. **Возможные источники угрозы** - сотрудники, имеющие санкционированный  
   доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие  
   права доступа к активам; обслуживающий персонал (охрана, работники инженерно-

технических служб и т.д.); уполномоченный персонал разработчиков ИС, который на  
договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС.

1. **Способ реализации угрозы** - осуществление несанкционированного доступа к  
   оставленным без присмотра функционирующим штатным средствам.
2. **Используемые уязвимости** - недостатки реализации необходимых  
   организационно-режимных мероприятий на объектах ИС, связанные с возможностью  
   несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам.
3. **Вид активов, потенциально подверженных угрозе** - целевая информация (в том числе служебная информация и ПДн); технологическая информация.
4. **Нарушаемые характеристики безопасности активов** - конфиденциальность.
5. **Возможные последствия реализации угрозы** - несанкционированное  
   ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС.
6. **Выводы**

Учитывая, что ИС является ИС с архитектурой и

консолидированным хранением и обработкой информации не составляющей  
государственную тайну в физически выделенных центрах обработки данных с реализацией  
необходимого объема организационных и режимных мер защиты, то о возможностях  
нарушителя можно сделать следующие выводы.

1. Атаки внешнего нарушителя, направленные на каналы связи посредством  
   перехвата информации и последующего ее анализа, уничтожения, модификации и  
   блокирования информации, реализация попыток преодоления системы защиты информации,  
   с использованием, в том числе, уязвимостей программной среды, а также утечка информации  
   по техническим каналам нейтрализуются организационными и режимными мероприятиями, а также условиями функционирования ИС.
2. Возможности внутреннего нарушителя существенным образом зависят от  
   действующих в пределах контролируемой зоны ограничительных факторов, из которых  
   основным является реализация комплекса режимных и 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 несанкционированных  
   действий.
3. Ввиду исключительной роли в ИС лиц категории I и II в число этих лиц должны  
   включаться только доверенные лица, к которым применен комплекс особых  
   организационно-режимных мер по их подбору, принятию на работу, назначению на  
   должность и контролю выполнения функциональных обязанностей.
4. Лица категорий III-VII относятся к вероятным нарушителям. Среди лиц категорий  
   III-VII наиболее опасными вероятными нарушителями являются лица категории III  
   (пользователи ИС) и лица категории VII (уполномоченный персонал разработчиков ИС,  
   который на договорной основе имеет право на техническое обслуживание и модификацию  
   компонентов ИС).

Представленная модель угроз с описанием вероятного нарушителя для ИС должна  
использоваться при формировании обоснованных требований безопасности информации  
(профиля защиты ИС) и проектировании СЗ информации не составляющей государственной тайны ИС.

Приложение 5. ПРОЕКТ

|  |
| --- |
| (Оператор) |

Типовая форма

списка лиц, допущенных в защищаемое помещение №\_\_

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Должность** | **Фамилия и инициалы** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| 8 |  |  |
| 9 |  |  |
| 10 |  |  |
| 11 |  |  |
| 12 |  |  |
| 13 |  |  |

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 6. ПРОЕКТ**

Приказ

о назначении ответственного за обеспечение безопасности

персональных данных

|  |
| --- |
| (Оператор) |

**О назначении ответственного за обеспечение безопасности персональных данных**

В целях исполнения Федерального закона №152-ФЗ от 27 июля 2006 года «О  
персональных данных» в *(наименование оператора):*

ПРИКАЗЫВАЮ:

1. Назначить ответственного за организацию обработки персональных данных в (наименование оператора):

Иванова И.И. - занимаемая должность;

1. Ответственному за организацию обработки персональных данных, в срок до

организовать проведение работ по защите персональных данных в соответствие с требованиями действующего законодательства и представить на утверждение организационно-распорядительные документы, регламентирующие защиту персональных данных.

1. Контроль за исполнением настоящего приказа возложить на

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 7. ПРОЕКТ**

|  |
| --- |
| (Оператор) |

Перечень  
информационных систем персональных данных

(ПРИМЕР)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Название  АС(ИСПДн) | Тип обработки ПДн | Описание каналов передачи данных | Структура | Местонахождение  ИСПДн (адрес подразделения) |
| 1 | АС  «Корпоративная сеть Управления» | Многопользовательская, с разграничением прав | ЛВС без подключения к Internet.Передача данных по выделенные каналам связи без шифрования | распределе  нная |  |
| 2 | АИС «Кадры» | Многопользователь ская, с разграничением прав | ЛВС без подключения к Internet. Передача данных по выделенные каналам связи с шифрованием. | распределе  нная |  |
| 3 | Бухгалтерская программа Парус Бюджет "Зарплата" | Многопользователь ская, с разграничением прав | ЛВС без подключения к Internet. | локальная |  |

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 8. ПРОЕКТ**

|  |
| --- |
| (Оператор) |

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в *(наименование оператора)*

(ПРИМЕР)

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование сведений** | **Гриф**  **конфиденциальности** | **Сроки**  **хранения** |
| 1. | Фамилия, имя, отчество | Конфиденциально | 5 лет |
| 2. | Дата рождения | Конфиденциально | 5 лет |
| 3. | Адрес регистрации | Конфиденциально | 5 лет |
| 4. | Контактный телефон | Конфиденциально | 5 лет |
| 5. | Серия и номер документа удостоверяющего личность | Конфиденциально | 5 лет |
| 6. | Номер страхового свидетельства государственного пенсионного страхования | Конфиденциально | 5 лет |
| 7. | Серия, номер полиса обязательного медицинского страхования | Конфиденциально | 5 лет |
| 8. | Гражданство | Конфиденциально | 5 лет |

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

Лист ознакомления

|  |  |  |
| --- | --- | --- |
| Фамилия, Имя, Отчество | Должность | Дата ознакомления, роспись |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Приложение 9. ПРОЕКТ**

Образец уведомления об обработке (о намерении осуществлять обработку) персональных данных, рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных

Руководителю Управления Федеральной

службы по надзору в сфере связи,

информационных технологий и массовых

коммуникаций по Саратовской области

**УВЕДОМЛЕНИЕ**

**Об обработке (о намерении осуществлять обработку) персональных данных**

|  |
| --- |
| (наименование (фамилия, имя, отчество), адрес оператора) |

руководствуясь

(правовое основание обработки персональных данных)

с целью

(цель обработки персональных данных)

осуществляет обработку:

|  |
| --- |
| (категории персональных данных) |

принадлежащих:

|  |
| --- |
| (категории субъектов, персональные данные которых обрабатываются) |

Обработка вышеуказанных персональных данных будет осуществляться путем:

|  |
| --- |
| (перечень действий с персональными данными, общее описание используемых оператором |

способов обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

|  |
| --- |
| (описание мер, предусмотренных ст. 18.1. и 19 Федерального закона от 27.07.2006 |

№ 152-ФЗ

|  |
| --- |
| «О персональных данных», в т.ч. сведения о наличии шифровальных (криптографических) |
| средств и наименования этих средств; фамилия, имя, отчество физического лица или |

наименование

|  |
| --- |
| юридического лица, ответственных за организацию обработки персональных данных, |
| и номера их контактных телефонов, почтовые адреса и адреса электронной почты) |

Сведения о наличии или об отсутствии трансграничной передачи персональных данных

|  |
| --- |
| (при наличии трансграничной передачи персональных данных в процессе их обработки, |

указывается перечень иностранных государств, на территорию которых осуществляется

трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных

|  |
| --- |
| (сведения об обеспечении безопасности персональных данных в соответствии с |

требованиями

|  |
| --- |
| к защите персональных данных, установленными Правительством Российской Федерации) |

Дата начала обработки персональных данных: .

Срок или условие прекращения обработки персональных данных: .

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

*Рекомендации по заполнению образца формы уведомления об обработке (о намерении*

*осуществлять обработку) ПДн:*

1. В поле «наименование (фамилия, имя, отчество), адрес оператора» указывается:
   1. Для юридических лиц (операторов):

* полное наименование с указанием организационно-правовой формы и  
  сокращенное наименование юридического лица (оператора), осуществляющего обработку  
  ПДн;
* наименование филиала(ов) (представительства(в) юридического лица  
  (оператора), осуществляющего обработку ПДн (для юридических лиц с филиальной  
  структурой указывается список субъектов Российской Федерации (с указанием кода  
  субъекта - согласно справочнику «Коды регионов», утвержденному приказом ФНС России  
  от 13.10.2006 года № САЭ-3-04/706@ «Об утверждении формы сведений о доходах  
  физических лиц» зарегистрированным Министерством юстиции Российской Федерации  
  17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы  
  (представительства) юридического лица и (или) где оператором производится обработка  
  ПДн. Уведомление направляется юридическим лицом в соответствующее территориальное  
  управление Роскомнадзора по месту своего нахождения с указанием всех имеющихся  
  филиалов (представительств)[1](#bookmark81));
* место нахождения (указывается место нахождения юридического лица в  
  соответствии с учредительными документами и свидетельством о постановке юридического  
  лица на учет в налоговом органе, а также место нахождения филиала(ов) (представительств)  
  юридического лица, контактная информация[2](#bookmark82));
* индивидуальный номер налогоплательщика (ИНН).
  1. Для государственных, муниципальных органов (операторов):
* полное и сокращенное наименование государственного, муниципального  
  органа;
* наименование территориального(ых) органа(ов), осуществляющего(их)  
  обработку ПДн;
* место нахождения (указывается место нахождения государственного,  
  муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, контактная информация);
* индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилия, имя, отчество), адреса оператора, а также  
направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1Если для каких-либо операторов (с учетом филиалов (представительств) значения пунктов 2-9 отличаются, то для них формируется отдельное уведомление.

2Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический  
адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка  
ПДн (все действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление,  
изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн).  
При этом, необходимо уточнить - обработка ПДн осуществляется только юридическим лицом (формирование центральной  
информационной системы) и (или) филиалами (представительствами).

1. В поле «правовое основание обработки персональных данных» указываются:  
   Федеральный закон, Постановление Правительства Российской Федерации, иной  
   нормативно-правовой акт, закрепляющий основание и порядок обработки ПДн[3](#bookmark83).

Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности,

с указанием лицензионных условий, закрепляющих запрет на передачу ПДн третьим лицам  
без согласия в письменной форме субъекта ПДн[4](#bookmark84).

1. В поле «цель обработки персональных данных» указываются цели обработки ПДн (а также их соответствие полномочиям оператора)[5](#bookmark85).
2. В поле «категории персональных данных» указываются все категории ПДн,  
   подлежащих обработке.
3. В поле «категории субъектов, персональные данные которых обрабатываются»  
   указываются категории субъектов (физических лиц) и виды отношений с субъектами  
   (физическими лицами), ПДн которых обрабатываются. Например: работники (субъекты),  
   состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица  
   (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие  
   в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.
4. В поле «перечень действий с персональными данными, общее описание  
   используемых оператором способов обработки персональных данных» указываются  
   действия, совершаемые оператором с ПДн, а также описание используемых оператором  
   способов обработки ПДн:

неавтоматизированная обработка ПДн;

исключительно автоматизированная обработка ПДн с передачей полученной  
информации по сети или без таковой;

смешанная обработка ПДн[6](#bookmark86).

1. В поле «описание мер, которые оператор обязуется осуществлять при обработке  
   ПДн, по обеспечению безопасности ПДн при их обработке», указываются организационные  
   и технические меры, в том числе использование шифровальных (криптографических)  
   средств, используемых для защиты ПДн от неправомерного или случайного доступа к ним,  
   уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от  
   иных неправомерных действий при их обработке.
2. В поле «дата начала обработки персональных данных» указывается конкретная дата  
   начала совершения действий с ПДн, включая сбор, систематизацию, накопление, хранение,
3. В поле «срок или условие прекращения обработки персональных данных»  
   указывается конкретная дата или основание (условие), наступление которого повлечет  
   прекращение обработки ПДн.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного  
нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки ПДн. (Например:  
ст. 85-90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона «Об актах гражданского  
состояния» и др.).

4Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу ПДн (или информации,  
касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных  
условий.

5Под «целью обработки персональных данных» понимаются, как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по обработке ПДн.

6При автоматизированной обработке ПДн либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки ПДн информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации. уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн (фактическая дата начала обработки ПДн).

**Приложение 10. ПРОЕКТ**

|  |
| --- |
| (Оператор) |

**Перечень**

**должностей служащих государственного или муниципального органа,  
замещение которых предусматривает осуществление обработки  
персональных данных либо осуществление доступа к  
персональным данным**

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 11. ПРОЕКТ**

|  |
| --- |
| (Оператор) |

**Перечень**

должностей, ответственных за проведение мероприятий по обезличиванию

обрабатываемых персональных данных

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 12. ПРОЕКТ**

Приказ

о создании комиссии по определению уровня защищенности ИСПДн

|  |
| --- |
| (Оператор) |

**О создании комиссии по определению уровня защищенности ИСПДн**

В целях исполнения с Постановления Правительства Российской Федерации от 1  
ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их  
обработке в информационных системах персональных данных» в (наименование оператора):

ПРИКАЗЫВАЮ:

1. Создать комиссию по определению уровня защищенности информационных систем  
   персональных данных составе:

председатель комиссии:

Иванов И.И. - занимаемая должность;

члены комиссии:

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность.

1. Членам комиссии в срок до \_\_\_\_\_\_\_\_\_\_\_ произвести анализ исходных данных ИСПДн \_\_\_\_\_\_\_\_\_\_ (название ИСПДн) \_\_\_\_\_\_\_\_\_, определить требования по защищенности для установленного уровня защищенности и составить акт определения уровня защищенности
2. Контроль за исполнением настоящего приказа возложить на

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 13. ПРОЕКТ**

**Акт определения уровня защищенности в**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Комиссия в составе,

председатель комиссии:

Иванов И.И. - занимаемая должность;

члены комиссии:

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность;

Иванова И.И. - занимаемая должность.

в ходе своей работы установила следующее:

1. категория персональных данных − \_\_\_\_\_\_\_\_\_\_\_\_\_;
2. обрабатываются персональные данные \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
3. объем обрабатываемых персональных данных − \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ субъектов персональных данных;
4. структура информационной системы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
5. наличие подключений информационной системы к сетям связи общего  
   пользования и (или) сетям международного информационного обмена: \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
6. режим обработки персональных данных: \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
7. режим разграничения прав доступа пользователей информационной системы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
8. местонахождение технических средств: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
9. наличие угроз связанных с недекларированными возможностями программного  
   обеспечения \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

По результатам анализа исходных данных ИСПДн \_\_\_\_\_\_\_\_\_\_ (название ИСПДн) \_\_\_\_\_\_\_\_\_ присваивается \_\_\_ класс защищенности.

Требования по защищенности для \_\_\_\_ уровня (согласно ПП №1119):

|  |
| --- |
|  |
|  |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Председатель комиссии | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| Члены комиссии: | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| (должность) | (подпись) | (Ф.И.О.) |

**Приложение 14. ПРОЕКТ**

Должностная инструкция

ответственного за организацию обработки персональных данных в государственном или муниципальном органе

О**бщие положения**

1. Настоящий документ определяет основные обязанности, права и ответственность  
   пользователя ИСПДн (наименование оператора).
2. Пользователем является каждый сотрудник, участвующий в рамках своих  
   функциональных обязанностей в процессах автоматизированной обработки информации и  
   имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ  
   ИСПДн.
3. Пользователь несет персональную ответственность за свои действия.
4. Пользователь в своей работе руководствуется настоящей инструкцией и  
   (указываются действующие внутренние организационно-распорядительные документы,  
   регламентирующие обработку ПДн у оператора).
5. Ознакомление сотрудников с требованиями настоящей Инструкции проводит  
   ответственный за обеспечение безопасности ПДн под роспись.
6. Методическое руководство работой пользователя осуществляется ответственным  
   за обеспечение безопасности ПДн.
7. **Функции и обязанности пользователя**
   1. Каждый пользователь обязан:
      1. Знать и выполнять требования действующих нормативных и руководящих  
         документов, а также внутренних инструкций и распоряжений, регламентирующих порядок  
         действий по обеспечению безопасности ПДн.
      2. Выполнять свои функциональные обязанности строго в рамках прав доступа к  
         внутренним и внешним информационным ресурсам, техническим средствам, полученным  
         согласно Разрешительной системы доступа к информационным ресурсам, программным и  
         техническим средствам ИСПДн.
      3. Знать и соблюдать установленные требования по режиму обработки ПДн,  
         организации парольной защиты, по проведению антивирусного контроля, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн.
      4. Знать и строго выполнять правила работы со СЗИ.
      5. Соблюдать правила при работе в сетях общего доступа и (или) международного  
         обмена.
      6. Во время работы с защищаемой информацией экран монитора в помещении  
         располагать так, чтобы исключалась возможность несанкционированного ознакомления с  
         отображаемой на нем информацией посторонними лицами, шторы (жалюзи) на оконных  
         проемах должны быть завешаны.
      7. Обо всех выявленных нарушениях, связанных с обработкой ПДн обратиться к  
         ответственному за обеспечение безопасности ПДн.
      8. Заблокировать доступ при отсутствии визуального контроля за рабочей  
         станцией. Для этого необходимо нажать одновременно комбинацию клавиш  
         <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.
   2. Пользователю запрещается:
      1. Разглашать защищаемую информацию по Перечню ПДн, подлежащих защите,  
         третьим лицам.
      2. Копировать защищаемую информацию на неучтенные носители информации.
      3. Использовать компоненты программного и аппаратного обеспечения ИСПДн в  
         неслужебных целях.
      4. Самостоятельно устанавливать, тиражировать, или модифицировать  
         программное и аппаратное обеспечение, изменять установленный алгоритм  
         функционирования технических и программных средств ИСПДн.
      5. Подключать личные внешние носители и мобильные устройства к техническим  
         средствам ИСПДн.
      6. Отключать (блокировать) СЗИ ИСПДн.
      7. Обрабатывать информацию и выполнять работы, не предусмотренные  
         Разрешительной системой доступа к информационным ресурсам, программным и  
         техническим средствам ИСПДн.
      8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты  
         доступа к ресурсам ИСПДн.
      9. Привлекать посторонних лиц для производства ремонта или настройки средств  
         ИСПДн.
8. **Организация парольной защиты**
   1. Личные пароли доступа к средствам ИСПДн выдаются пользователям  
      администратором безопасности, ответственным за обеспечение безопасности ПДн или  
      другим уполномоченным лицом.
   2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3  
      месяца.
   3. Правила ввода пароля:

ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность его подсматривания  
посторонними лицами.

* 1. Правила хранение пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и  
других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль.

* 1. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования организации парольной защиты;

своевременно сообщать администратору безопасности или ответственному за  
обеспечение безопасности ПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

1. **Ответственность пользователя**
2. За ненадлежащее исполнение или неисполнение своих должностных  
   обязанностей, предусмотренных настоящей инструкцией, другими организационно-

распорядительными документами, в соответствии с действующим трудовым  
законодательством Российской Федерации.

1. За правонарушения, совершенные в процессе своей деятельности в пределах,  
   определенных действующим административным, уголовным и гражданским  
   законодательством Российской Федерации.
2. За разглашение сведений конфиденциального характера и другой защищаемой  
   информации в пределах, определенных действующим административным, уголовным и  
   гражданским законодательством Российской Федерации.

**Приложение 15. ПРОЕКТ**

Должностная инструкция

администратора безопасности информационных систем персональных данных *(наименование оператора)*

**Общие положения**

1. Настоящий документ определяет основные обязанности, права и  
   ответственность администратора безопасности ИСПДн (наименование оператора).
2. Администратор безопасности назначается руководителем оператора или  
   начальником подразделения, ответственного за обеспечение безопасности ПДн.
3. Администратор безопасности в своей работе руководствуется настоящей  
   инструкцией и (указываются действующие внутренние организационно-распорядительные  
   документы, регламентирующие обработку ПДн у оператора).
4. Администратор безопасности является ответственным должностным лицом,  
   уполномоченным на проведение работ по поддержанию достигнутого уровня защиты  
   ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
5. Администратор безопасности осуществляет методическое руководство  
   операторов, системных администраторов и других лиц, допущенных к работе в ИСПДн, в  
   вопросах обеспечения защиты ПДн.
6. Требования администратора безопасности, связанные с выполнением им своих  
   должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
7. Администратор безопасности несет персональную ответственность за качество  
   проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.
8. **Должностные обязанности администратора безопасности**
   1. Администратор безопасности обязан:
9. Знать перечень и состав ИСПДн, перечень задач, решаемых их использованием.
10. Знать и выполнять требования действующих нормативных и руководящих  
    документов, а также внутренних инструкций и распоряжений, регламентирующих порядок  
    действий по обеспечению защиты ПДн.
11. Осуществлять установку, настройку и сопровождение СЗИ.
12. Осуществлять учет применяемых СЗИ, эксплуатационной и технической  
    документации к ним.
13. Участвовать в контрольных и тестовых испытаниях и проверках элементов  
    ИСПДн.
14. Участвовать в приемке новых программных средств.
15. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно  
    Разрешительной системы доступа к информационным ресурсам, программным и  
    техническим средствам ИСПДн.
16. Уточнять в установленном порядке обязанности пользователей ИСПДн.
17. Проводить резервирование ПДн.
18. Вести учет носителей ПДн.
19. Выдавать пользователям личные пароли доступа к средствам ИСПДн.
20. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
21. Контролировать неизменность состояния СЗИ их параметров и режимов  
    защиты.
22. Контролировать физическую сохранность средств и оборудования ИСПДн.
23. Контролировать исполнение пользователями ИСПДн введенного режима  
    безопасности, а так же правильность работы с элементами ИСПДн и СЗИ.
24. Контролировать исполнение пользователями парольной защиты.
25. Контролировать работу пользователей в сетях общего пользования и  
    международного обмена.
26. Своевременно анализировать журналы учета событий, с целью выявления  
    возможных нарушений.
27. Не допускать установку, использование, хранение и размножение в ИСПДн  
    программных средств, не связанных с выполнением функциональных задач.
28. Осуществлять периодические контрольные проверки рабочих станций и  
    тестирование правильности функционирования СЗИ ИСПДн.
29. Оказывать помощь пользователям ИСПДн в части применения СЗИ и  
    консультировать по вопросам введенного режима защиты.
30. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о  
    нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях  
    установленных требований по защите информации.
31. В случае отказа работоспособности СЗИ ИСПДн принимать меры по их  
    своевременному восстановлению и выявлению причин, приведших к отказу  
    работоспособности.
32. Принимать меры по реагированию, в случае возникновения нештатных и  
    аварийных ситуаций, с целью ликвидации их последствий, участвовать в расследовании  
    причин их возникновения.
33. **Организация парольной защиты**
    1. Личные пароли доступа к средствам ИСПДн выдаются пользователям  
       администратором безопасности, ответственным за обеспечение безопасности ПДн или  
       другим уполномоченным лицом.
    2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3  
       месяца.
    3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-  
либо его часть;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы трех категорий из числа  
следующих четырех:

б) прописные буквы английского алфавита от A до Z;

в) строчные буквы английского алфавита от а до z;

г) десятичные цифры (от 0 до 9);

д) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

запрещается использовать в качестве пароля имя входа в систему, простые пароли

типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности

и своих родственников, номера автомобилей, телефонов и другие пароли, которые можно  
угадать, основываясь на информации о пользователе;

запрещается выбирать пароли, которые уже использовались ранее.

1. **Права администратора безопасности**
   1. Администратор безопасности имеет право:
      1. Отключать любые элементы СЗПДн при изменении конфигурации,  
         регламентном техническом обслуживании или устранении неисправностей в установленном порядке.
      2. В установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн.
      3. Требовать от сотрудников соблюдения правил работы в ИСПДн, приведенных в  
         должностных инструкциях.
      4. Требовать от пользователей безусловного соблюдения установленной  
         технологии обработки ПДн и выполнения требований локальных документов,  
         регламентирующих вопросы обеспечения защиты ПДн.
      5. Требовать прекращения обработки информации в случае нарушения  
         установленной технологии обработки ПДн или нарушения функционирования СЗИ.
      6. Вносить свои предложения по совершенствованию СЗПДн.
      7. Инициировать проведение служебных расследований по фактам нарушения  
         установленных требований обеспечения защиты ПДн в ИСПДн.
2. **Ответственность администратора безопасности**
   1. Администратор безопасности несет ответственность:
      1. За ненадлежащее исполнение или неисполнение своих должностных  
         обязанностей, предусмотренных настоящей инструкцией, другими локальными  
         организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.
      2. За правонарушения, совершенные в процессе своей деятельности в пределах,  
         определенных действующим административным, уголовным и гражданским  
         законодательством Российской Федерации.
      3. За разглашение сведений конфиденциального характера и другой защищаемой  
         информации в пределах, определенных действующим административным, уголовным и  
         гражданским законодательством Российской Федерации.
      4. На администратора безопасности возлагается персональная ответственность за  
         работоспособность и надлежащее функционирование СЗИ ИСПДН.

**Приложение 16. ПРОЕКТ**

Типовое обязательство

служащего государственного или муниципального органа, непосредственно  
осуществляющего обработку персональных данных, в случае расторжения с  
ним государственного или муниципального контракта прекратить обработку  
персональных данных, ставших известными ему в связи с исполнением

должностных обязанностей

ОБЯЗАТЕЛЬСТВО  
о неразглашении информации, содержащей персональные данные

Я,

(ФИО государственного гражданского служащего)

Исполняющий (ая) должностные обязанности по занимаемой должности

|  |
| --- |
| (должность, наименование структурного подразделения департамента) |

Предупрежден (а), что на период исполнения должностных обязанностей в  
соответствии с должностным регламентом, мне будет предоставлен допуск к  
конфиденциальной информации (персональным данным), не содержащим сведений,  
составляющих государственную тайну. Настоящим добровольно принимаю на себя  
обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены  
   (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения,  
   которые мне доверены (будут доверены) или станут известными в связи с выполнением  
   должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения,  
   сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы  
   защиты конфиденциальных сведений.
6. После прекращения права на допуск к конфиденциальным сведениям (расторжения  
   служебного контракта) прекратить обработку персональных данных, не разглашать и не  
   передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен(а)  
к дисциплинарной ответственности и/или иной ответственности в соответствии с  
законодательством Российской Федерации.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(подпись) расшифровка подписи*

**Приложение 17. ПРОЕКТ**

**Форма  
согласия субъекта персональных данных на обработку персональных  
данных**

Я,

(фамилия, имя, отчество)

|  |
| --- |
| (адрес регистрации) |
| (адрес фактического проживания) |
| (паспорт: серия, номер, дата выдачи, кем выдан) |

В соответствии Федеральным законом от № 152-ФЗ «О персональных данных» даю

согласие \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее Оператор): на обработку (включая сбор,

систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,  
распространение (в том числе, передачу), обезличивание, блокирование, уничтожение) моих  
персональных данных.

Обработка моих персональных данных может осуществляться с использованием  
средств автоматизации и без использования таких средств исключительно в целях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок действия согласия \_\_\_\_\_\_\_\_\_\_\_\_

Согласие вступает в силу с момента его подписания.

Согласие может быть отозвано мною после окончания договорных отношений на  
основании моего письменного заявления.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

**Приложение 18. ПРОЕКТ**

**Форма  
согласия субъекта персональных данных на обработку персональных данных**

(для участников конкурса на формирование кадрового резерва, лиц состоящих в кадровом резерве)

Я,

(фамилия, имя, отчество)

|  |
| --- |
| (адрес регистрации) |
| (адрес фактического проживания) |
| (паспорт: серия, номер, дата выдачи, кем выдан) |

В соответствии с Конституцией Российской Федерации, Федеральным законом от №  
152-ФЗ «О персональных данных», Федеральным законом от 27.07.2004 № 79-ФЗ «О  
государственной гражданской службе Российской Федерации», Указом Президента  
Российской Федерации от 01.02.2005 № 112 «О конкурсе на замещение вакантной должности  
государственной гражданской службы Российской федерации», Законом Саратовской  
области от 2 февраля 2005 года № 15-ЗСО «О государственной гражданской службе Саратовской области», даю согласие (далее Оператор):

На обработку моих персональных данных, а именно:

* общие сведения (Ф.И.О., дата и место рождения, пол, гражданство, образование,  
  профессия, стаж работы (службы), семейное положение, паспортные данные); сведения о  
  трудовой деятельности, сведения о судимости; сведения о воинском учете; сведения о  
  повышении квалификации, профессиональной переподготовке; сведения о наградах  
  (поощрениях), почетных званиях; сведения о месте регистрации и фактического проживания,  
  контактных телефонах; сведения о составе семьи; сведения о доходах и имуществе,  
  принадлежащем мне и членам моей семьи на праве собственности; сведения о результатах  
  медицинского обследования; сведения, содержащиеся в свидетельстве о постановке на учет в  
  налоговом органе и страховом свидетельстве государственного пенсионного страхования;  
  сведения о пребывании за границей, сведения о наличии заграничного паспорта, сведения о трудовой деятельности.

На передачу моих персональных данных третьим лицам в целях проверки  
достоверности представленных сведений, формирования общего кадрового резерва  
Саратовской области в налоговые органы, в правоохранительные органы; в управление  
государственной службы и кадров Правительства Саратовской области.

Обработка моих персональных данных может осуществляться с использованием  
средств автоматизации и без использования таких средств исключительно в целях

обеспечения соблюдения законов и иных нормативных правовых актов, содействия в  
трудоустройстве, обучения, продвижении по службе (работе).

Я предоставляю право осуществлять следующие действия (операции) с

моими персональными данными: сбор, систематизацию, накопление, хранение, уточнение  
(обновление, изменение), использование, распространение (в том числе, передачу),  
размещение моей фамилии, имени, отчества, наименование должности на формирование  
кадрового резерва на сайте Правительства Саратовской области, обезличивание,  
блокирование, уничтожение.

Данное согласие действительно в течение трех лет с момента завершения конкурса. Согласие может быть отозвано мною на основании моего письменного заявления.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

**Приложение 19. ПРОЕКТ**

**Форма  
согласия на обработку персональных данных государственных гражданских служащих, иных субъектов персональных данных**

Я,

(фамилия, имя, отчество)

|  |
| --- |
| (должность, структурное подразделение) |
| (адрес регистрации) |
| (адрес фактического проживания) |
| (паспорт: серия, номер, дата выдачи, кем выдан) |

даю свое согласие на обработку (далее - Оператор), моих

персональных данных в целях заключения и реализации Служебного контракта (Трудового  
договора), а также в целях соблюдения требований действующего законодательства.  
Для целей настоящего Служебного контракта (Трудового договора) мои персональные  
данные включают в себя: фамилию, имя, отчество, дату рождения, адрес проживания,  
контактный телефон, паспортные данные, ИНН и СНИЛС.  
Я даю согласие на получения моих персональных данных у третьей стороны, в случае  
возникновения необходимости.

Оператор вправе осуществлять все необходимые действия с моими персональными  
данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление,  
изменение), использование, передачу (УФНС, ПФР, ФСС и т.д.), обезличивание,  
блокирование, уничтожение, внесение в информационную систему, обработку с  
использованием средств автоматизации или без использования таких средств.

Передача моих персональных данных иным лицам или их разглашение может  
осуществляться только с моего письменного согласия.

Оператор может осуществлять обработку моих персональных данных в течение  
действия Служебного контракта (Трудового договора) и в течение 75 (семидесяти пяти) лет после его прекращения.

Я вправе отозвать свое согласие на обработку персональных данных посредством  
соответствующего письменного заявления, что влечет дальнейшее расторжение Служебного контракта (Трудового договора).

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

**Приложение 20. ПРОЕКТ**

|  |
| --- |
| (Оператор) |

**Разрешительная система доступа  
к информационным ресурсам, программным и техническим средствам  
информационных систем персональных данных (наименование оператора)**

1. К работе в информационной системе персональных данных (*наименование ИСПДн)* допущены:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Ф.И.О. | Отдел | Должность | Группа |
| 1. |  |  |  |  |
| 2. |  |  |  |  |

1. Перечень ресурсов, программных и технических средств (объектов доступа)  
   входящих в состав ИСПДн *(наименование ИСПДн):*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование средства (ресурса) | Назначение средства (расположение ресурса) | Носит  ели | Приме  чание |
| Информационные ресурсы | | | | |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| Технические средства | | | | |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| Программные средства (установлены на ЖМД (наимен.), сер. №\_\_\_\_)  \_\_\_) | | | | |
| 5. |  |  |  |  |
| 6. |  |  |  |  |

1. Полномочия доступа пользователей к информационным ресурсам, программным и  
   техническим средствам ИСПДн *(наименование ИСПДн):*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование ресурса, тип средства | Гриф  обрабатываемой  информации | Путь  доступа | Полномочия доступа групп пользователей | | |
| Системные  администра-  торы | Операторы | Другие  группы |
| Информационные ресурсы | | | | | | |
| 1. |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 21. ПРОЕКТ**

Порядок

доступа служащих государственного или муниципального органа в помещения,  
в которых ведется обработка персональных данных

Настоящий Порядок доступа служащих государственного или муниципального  
органа в помещения, в которых ведется обработка персональных данных (далее - Порядок)  
разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О  
персональных данных», Постановлением Правительства Российской Федерации от 15  
сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки  
персональных данных, осуществляемых без использования средств автоматизации»,  
Постановлением Правительства РоссийскойФедерацииот21 марта 2012 г. № 211 «Об  
утверждении перечня мер, направленных на обеспечение выполнения обязанностей,  
предусмотренных Федеральным законом «О персональных данных» и принятыми в  
соответствии с ним нормативными правовыми актами, операторами, являющимися  
государственными или муниципальными органами» и другими нормативными правовыми  
актами.

1. Персональные данные относятся к конфиденциальной информации.  
   Должностные лица, получившие доступ к персональным данным, обязаны не раскрывать  
   третьим лицам и не распространять персональные данные без согласия субъекта  
   персональных данных, если иное не предусмотрено федеральным законом.
2. Обеспечение безопасности персональных данных от уничтожения, изменения,  
   блокирования, копирования, предоставления, распространения персональных данных, а  
   также от иных неправомерных действий в отношении персональных данных достигается, в  
   том числе, установлением правил доступа в помещения, где обрабатываются персональные  
   данные в информационной системе персональных данных и без использования средств  
   автоматизации.
3. Для помещений, в которых обрабатываются персональные данные,  
   организуется режим обеспечения безопасности, при котором обеспечивается сохранность  
   носителей персональных данных и средств защиты информации, а также исключается  
   возможность неконтролируемого проникновения и пребывания в этих помещениях  
   посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться  
условия, обеспечивающие сохранность персональных данных и исключающие  
несанкционированный доступ к ним.

1. В помещения, где размещены технические средства, позволяющие  
   осуществлять обработку персональных данных, а также хранятся носители информации,  
   допускаются только служащие, уполномоченные на обработку персональных данных.
2. Нахождения лиц в помещениях, в которых ведется обработка персональных  
   данных, не являющихся уполномоченными лицами на обработку персональных данных,  
   возможно только в сопровождении уполномоченного сотрудника на время, ограниченное  
   необходимостью решение вопросов, связанных с исполнением государственных функций и  
   (или) осуществлением полномочий в рамках договоров, заключенных с учреждением, в  
   котором ведется обработка персональных данных.
3. Внутренний контроль за соблюдением порядка доступа в помещения, в  
   которых ведется обработка персональных данных, проводится лицом ответственным за  
   организацию обработки персональных данных или комиссией, назначенной распоряжением  
   руководителя учреждения, в котором ведется обработка персональных данных.

**Приложение 22. ПРОЕКТ**

Форма

отзыва согласия субъекта на обработку персональных данных

Отзыв  
согласия на обработку персональных данных

|  |
| --- |
| наименование (Ф.И.О.) оператора |
| Адрес оператора |
| Адрес, где зарегистрирован субъект персональных данных |
| Номер основного документа, удостоверяющего его личность |
| Дата выдачи указанного документа | |

**Заявление**

Прошу Вас прекратить обработку моих персональных данных в связи с их  
неправомерным использованием.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

**Приложение 23. ПРОЕКТ**

Форма

запроса на получение информации, составляющей персональные данные

у субъекта персональных данных

|  |
| --- |
| (Оператор) |

**Запрос**

Уважаемый(ая) (Ф.И.О.), в

связи с у (оператор) возникла необходимость

получения следующей информации, составляющей Ваши персональные данные

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(перечислить информацию)

Просим Вас предоставить указанные сведения в течение рабочих дней с

момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в указанный срок  
дать письменное согласие на получение нами необходимой информации из следующих  
источников , следующими способами

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

По результатам обработки указанной информации нами планируется принятие  
следующих решений, которые будут доведены до Вашего сведения

Против принятого решения Вы имеете право заявить свои письменные возражения в  
 срок.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 24. ПРОЕКТ**

Форма

уведомления об уничтожении персональных данных

субъекта персональных данных

В\_\_\_\_\_\_\_\_\_\_\_\_\_ (оператор)\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от

(Ф.И.О. заявителя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и реквизиты

документа, удостоверяющего

личность заявителя)

Заявление

Прошу уничтожить, обрабатываемые Вами, мои персональные данные:

|  |
| --- |
| (указать уничтожаемые персональные данные) |

в связи с тем, что

(указать причину уничтожения персональных данных)

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

|  |
| --- |
| (Оператор) |

Уведомление об уничтожении

Настоящим уведомлением сообщаем Вам, что в связи с

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

персональные данные уничтожены.

(указать персональные данные)

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 25. ПРОЕКТ**

Форма

уведомления о блокировании персональных данных субъекта

персональных данных

В\_\_\_\_\_\_\_\_\_\_\_\_\_ (оператор)\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от

(Ф.И.О. заявителя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и реквизиты

документа, удостоверяющего

личность заявителя)

Заявление

Прошу заблокировать, обрабатываемые Вами, мои персональные данные:

|  |
| --- |
| (указать блокируемые персональные данные) |

на срок: ; в связи с тем, что

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать причину блокирования персональных данных)

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

|  |
| --- |
| (Оператор) |

Уведомление о блокировании

Уважаем-ый(ая) (Ф.И.О.), в связи с

сообщаем Вам, что Ваши персональные данные

заблокированы на срок .

(указать персональные данные)

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

Приложение 26. ПРОЕКТ

Форма

уведомления об уточнении персональных данных субъекта

персональных данных

В\_\_\_\_\_\_\_\_\_\_\_\_\_ (оператор)\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от

(Ф.И.О. заявителя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и реквизиты

документа, удостоверяющего

личность заявителя)

Заявление

Прошу уточнить, обрабатываемые Вами, мои персональные данные в соответствии со сведениями: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

(указать уточненные персональные данные заявителя)

в связи с тем, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(указать причину уточнения персональных данных)

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

|  |
| --- |
| (Оператор) |

Уведомление об уточнении

Уважаем-ый(ая) (Ф.И.О.), в связи с

сообщаем Вам, что Ваши персональные данные

уточнены в соответствии со сведениями

.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 27. ПРОЕКТ**

Форма

уведомления об обработке персональных данных субъекта

персональных данных

В\_\_\_\_\_\_\_\_\_\_\_\_\_ (оператор)\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от

(Ф.И.О. заявителя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и реквизиты

документа, удостоверяющего

личность заявителя)

Заявление

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию,  
составляющую мои персональные данные, указать цели, способы и сроки ее обработки;  
предоставить сведения о лицах, которые имеют к ней доступ (которым может быть  
предоставлен такой доступ); сведения о том, какие юридические последствия для меня  
может повлечь её обработка. В случае отсутствия такой информации, прошу Вас уведомить  
меня об этом.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.  *(подпись) расшифровка подписи*

|  |
| --- |
| (Оператор) |

Уведомление

Уважаемый(ая) (Ф.И.О.),

(оператор) производится обработка сведений, составляющих Ваши

персональные данные: .

(указать сведения)

Цели обработки: .

Способы обработки: .

Перечень лиц, которые имеют доступ к информации, содержащей Ваши  
персональные данные или могут получить такой доступ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Должность** | **Ф.И.О.** | **Вид доступа** | **Примечания** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

По результатам обработки указанной информации нами планируется принятие  
следующих решений, которые будут доведены до Вашего сведения

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Против принятого решения Вы имеете право заявить свои письменные возражения в  
 срок.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. *(должность) (подпись) расшифровка подписи*

**Приложение 28. ПРОЕКТ**

Форма

журнала регистрации и учета обращений субъектов персональных данных

**Журнал**

учета обращений субъектов персональных данных о выполнении их  
законных прав, при обработке персональных данных в

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **ФИО** | **Дата** | **Цель** |
|  | Иванов И.И. | 01.10.2010 | Информирование |
|  | Сидоров С.С. | 01.10.2010 | Прекращение обработки |
|  | Петров П.П. | 01.10.2010 | Уточнение ПДн |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Приложение 29. ПРОЕКТ**

Модель угроз

безопасности персональных данных при их обработке в информационной  
системе персональных данных (наименование ИСПДн)

**Введение**

Модель УБПДн (далее - Модель) при их обработке в ИСПДн (наименование ИСПДн)  
построена на основании методического документа ФСТЭК России «Базовая модель угроз  
безопасности персональных данных при их обработке в информационных системах  
персональных данных».

В Модели представлено описание структуры ИСПДн, состава и режима обработки  
ПДн, классификация потенциальных нарушителей, оценка исходного уровня защищенности,  
анализ УБПДн.

Анализ УБПДн включает:  
описание угроз;

оценку вероятности возникновения угроз;  
оценку реализуемости угроз;  
оценку опасности угроз;  
определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности  
актуальных угроз.

1. **Информационная система персональных данных**
   1. Структура ИСПДн

Таблица 1. Параметры ИСПДн

|  |  |
| --- | --- |
| Структура ИСПДн | Автоматизированное рабочее место /Локальная ИСПДн / Распределенная ИСПДн |
| Режим обработки ПДн в ИСПДн | Однопользовательская ИСПДн / многопользовательская ИСПДн с равными правами доступа / многопользовательская ИСПДн с разными правами доступа |
| Режим разграничения прав доступа пользователей | С разграничением/без разграничения |
| Подключение ИСПДн к сетям общего пользования и (или) сетям международного информационного обмена | Имеется / не имеется |
| Категория ПДн, обрабатываемых в ИСПДн | Специальная, биометрическая, иная, общедоступная категория ПДн обрабатывающая ПД (не) сотрудников оператора |
| Объем ПДн, обрабатываемых в ИСПДн | Менее 100000/ более 100000 |
| Местонахождение технических средств ИСПДн | Все технические средства ИСПДн находятся в пределах Российской |
|  | Федерации / технические средства ИСПДн частично или целиком находятся за пределами Российской Федерации |
| Заданные характеристики безопасности ПДн | Специальная/типовая |

* 1. Состав и структура персональных данных

Исходя из состава обрабатываемых ПДн, можно сделать вывод, что они относятся к  
 категории ПДн.

Объем обрабатываемых ПДн, составляет записей о субъектах ПДн.

* 1. Конфигурация ИСПДн

Отображается конфигурация ИСПДн - схематичное взаиморасположение элементов  
ИСПДн ([Глава II. раздел 13](#п2_13)).

Отображается территориальное расположение ИСПДн относительно КЗ ([Глава II.  
раздел 13](#п2_13)).

* 1. Структура обработки ПДн

В ИСПДн обработка ПДн происходит следующим образом ([Глава II. раздел 13](#п2_13)):

1) ,

2) ,

3) .

* 1. Режим обработки ПДн

В ИСПДн обработка ПДн осуществляется в

*однопользовательском/многопользовательском* режиме с *разграничением/без  
разграничения* прав доступа.

Режим обработки предусматривает следующие действия с ПДн: сбор,  
систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,  
распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

К работе в ИСПДн допущены сотрудники со следующими полномочиями доступа:

Таблица 2. Матрица доступа

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные  действия | Сотрудник  и |
| Системные  администраторы  ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн.  Обладают полной информацией о технических средствах и | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные  действия | Сотрудник  и |
|  | конфигурации ИСПДн.  Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.  Обладают правами конфигурирования и административной настройки технических средств ИСПДн. |  |  |
| Администраторы  безопасности  ИСПДн | Обладают правами администратора ИСПДн.  Обладают полной информацией об ИСПДн.  Имеют доступ к СЗИ, средствам  протоколирования и к части ключевых элементов ИСПДн.  Не имеют прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Ответственные за обеспечение безопасности ПДн | Обладают полной информацией об ИСПДн.  Не имеют прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | * сбор * систематизация * накопление * хранение * уточнение * использование * уничтожение |  |
| Операторы ИСПДн с правами записи | Обладают всеми необходимыми атрибутами и правами, обеспечивающими | * сбор * систематизация * накопление * хранение |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные  действия | Сотрудник  и |
|  | доступ ко всем ПДн. | * уточнение * использование * уничтожение |  |
| Операторы ИСПДн с правами чтения | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - использование |  |

* 1. Классификация нарушителей

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

внешние нарушители - физические лица, не имеющие права пребывания на  
территории КЗ, в пределах которой размещается оборудование ИСПДн;

внутренние нарушители - физические лица, имеющие право пребывания на  
территории КЗ, в пределах которой размещается оборудование ИСПДн.

* + 1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается  
нарушитель, который не имеет непосредственного доступа к техническим средствам и  
ресурсам системы, находящимся в пределах КЗ.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую  
информацию по ТКУИ, так как объем информации, хранимой и обрабатываемой в ИСПДн,  
является недостаточным для возможной мотивации внешнего нарушителя к осуществлению  
действий, направленных на утечку информации по ТКУИ.

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

* + 1. Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от  
действующих в пределах КЗ 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 КЗ и контролю за порядком проведения работ, направленных на  
предотвращение и пресечение НСД.

Система разграничения доступа ИСПДн (наименование ИСПДн) обеспечивает  
разграничение прав пользователей на доступ к информационным, программным, аппаратным  
и другим ресурсам ИСПДн в соответствии с утвержденной Разрешительной системой доступа  
к информационным ресурсам, программным и техническим средствам ИСПДн (наименование  
ИСПДн). К внутренним нарушителям могут относиться:

администраторы ИСПДн (категория I);

администраторы конкретных подсистем или баз данных ИСПДн (категория II);

пользователи ИСПДн (категория III);

пользователи, являющиеся внешними по отношению к конкретной ИСПДн (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 ИСПДн, но не имеющие права доступа к ним (категория  
VI);

обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.)  
(категория VII);

уполномоченный персонал разработчиков ИСПДн, который на договорной основе  
имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-  
аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия  
различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут  
реализовывать УБПДн, используя возможности по непосредственному доступу к ПДн,  
обрабатываемых и хранимых в ИСПДн, а также к техническим и программным средствам  
ИСПДн, включая СЗИ, в соответствии с установленными для них административными  
полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен  
применяться комплекс особых организационно-режимных мер по их подбору, принятию на  
работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна  
ввиду принятых организационных и контролирующих мер.

1. Предположения об имеющейся у нарушителя информации об объектах  
   реализации УБПДн

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

общая информация - информации о назначения и общих характеристиках ИСПДн;

эксплуатационная информация - информация, полученная из эксплуатационной  
документации;

чувствительная информация - информация, дополняющая эксплуатационную  
информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может знать:

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

Предполагается, что лица категории III и категории IV владеют только  
эксплуатационной информацией, что обеспечивается организационными мерами. При этом  
лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией,  
используемой в ИСПДн, 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  
ИСПДн, что обеспечивается организационными мерами. При этом лица категории V не  
владеют парольной и аутентифицирующей информацией, используемой в ИСПДн.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не  
превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об  
ИСПДн, включая информацию об уязвимостях технических и программных средств ИСПДн.  
Организационными мерами предполагается исключить доступ лиц категории VIII к  
техническим и программным средствам ИСПДн в момент обработки с использованием этих  
средств защищаемой информации.

Таким образом, наиболее информированными об ИСПДн 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 СЗИ. К такой информации, например, относится парольная,  
аутентифицирующая и ключевая информация.

* + 1. Предположения об имеющихся у нарушителя средствах реализации УБПДн

Предполагается, что нарушитель имеет:

* аппаратные компоненты СЗПДн;
* доступные в свободной продаже технические средства и программное обеспечение;
* специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для  
реализации УБПДн, а также возможности по их применению зависят от многих факторов,  
включая реализованные конкретные организационные меры, финансовые возможности и  
компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя  
средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный  
нарушитель имеет все необходимые для реализации угроз средства, возможности которых не

превосходят возможности аналогичных средств реализации угроз на информацию,  
содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

средств перехвата по ТКУИ;

средств воздействия через сигнальные цепи (информационные и управляющие  
интерфейсы СВТ);

средств воздействия на источники и через цепи питания;

средств воздействия через цепи заземления;

средств активного воздействия на технические средства (средств облучения).

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

* 1. Исходный уровень защищенности ИСПДн

*(Уровень исходной защищенности ИСПДн определяется на основании методического  
документа ФСТЭК России «Методика определения актуальных угроз безопасности  
персональных данных при их обработке в информационных системах персональных  
данных».)*

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель,  
зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице 3 представлены характеристики уровня исходной защищенности для  
ИСПДн.

Таблица 3. Показатели исходной защищенности ИСПДн

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные** | **Уровень защищенности** | | |
| **характеристики ИСПДн** | **Высокий** | **Средний** | **Низкий** |
| 1. По территориальному размещению: |  |  |  |
| распределенная ИСПДн, которая | - | - | + |
| охватывает несколько областей, краев, |  |  |  |
| округов или государство в целом; |  |  |  |
| городская ИСПДн, охватывающая не | - | - | + |
| более одного населенного пункта |  |  |  |
| (города, поселка); |  |  |  |
| корпоративная распределенная | - | + | - |
| ИСПДн, охватывающая многие |  |  |  |
| подразделения одной организации; |  |  |  |
| локальная (кампусная) ИСПДн, | - | + | - |
| развернутая в пределах нескольких |  |  |  |
| близко расположенных зданий; |  |  |  |
| локальная ИСПДн, развернутая в | + | - | - |
| пределах одного здания |  |  |  |
| 2. По наличию соединения с сетями |  |  |  |
| общего пользования: |  |  |  |
| ИСПДн, имеющая многоточечный | - | - | + |
| **Технические и эксплуатационные** | **Уровень защищенности** | | |
| **характеристики ИСПДн** | **Высокий** | **Средний** | **Низкий** |
| выход в сеть общего пользования; |  |  |  |
| ИСПДн, имеющая одноточечный | - | + | - |
| выход в сеть общего пользования; |  |  |  |
| ИСПДн, физически отделенная от сети | + | - | - |
| общего пользования |  |  |  |
| 3. По встроенным (легальным) |  |  |  |
| операциям с записями баз |  |  |  |
| персональных данных: | + | - | - |
| чтение, поиск; |  |  |  |
| запись, удаление, сортировка; | - | + | - |
| модификация, передача | - | - | + |
| 4. По разграничению доступа к |  |  |  |
| персональным данным: |  |  |  |
| ИСПДн, к которой имеют доступ | - | + | - |
| определенные перечнем сотрудники |  |  |  |
| организации, являющейся владельцем |  |  |  |
| ИСПДн, либо субъект ПДн; |  |  |  |
| ИСПДн, к которой имеют доступ все | - | - | + |
| сотрудники организации, являющейся |  |  |  |
| владельцем ИСПДн; |  |  |  |
| ИСПДн с открытым доступом | - | - | + |
| 5. По наличию соединений с другими |  |  |  |
| базами ПДн иных ИСПДн: |  |  |  |
| интегрированная ИСПДн (организация | - | - | + |
| использует несколько баз ПДн ИСПДн, |  |  |  |
| при этом организация не является |  |  |  |
| владельцем всех используемых баз |  |  |  |
| ПДн); |  |  |  |
| ИСПДн, в которой используется одна | + | - | - |
| база ПДн, принадлежащая организации |  |  |  |
| - владельцу данной ИСПДн |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные** | **Уровень защищенности** | | |
| **характеристики ИСПДн** | **Высокий** | **Средний** | **Низкий** |
| 6. По уровню обобщения (обезличивания) |  |  |  |
| ПДн: | + | - | - |
| ИСПДн, в которой предоставляемые |  |  |  |
| пользователю данные являются |  |  |  |
| обезличенными (на уровне |  |  |  |
| организации, отрасли, области, региона | - | + | - |
| и т.д.); |  |  |  |
| ИСПДн, в которой данные |  |  |  |
| обезличиваются только при передаче в |  |  |  |
| другие организации и не обезличены | - | - | + |
| при предоставлении пользователю в |  |  |  |
| организации; |  |  |  |
| ИСПДн, в которой предоставляемые |  |  |  |
| пользователю данные не являются |  |  |  |
| обезличенными (т.е. присутствует |  |  |  |
| информация, позволяющая |  |  |  |
| идентифицировать субъекта ПДн) |  |  |  |
| 7. По объему ПДн, которые |  |  |  |
| предоставляются сторонним пользователям |  |  |  |
| ИСПДн без предварительной обработки: |  |  |  |
| ИСПДн, предоставляющая всю базу данных с | - | - | + |
| ПДн; |  |  |  |
| ИСПДн, предоставляющая часть ПДн; | - | + | - |
| ИСПДн, не предоставляющая никакой | + | - | - |
| информации. |  |  |  |

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет **высокий** уровень исходной защищенности, если не менее 70%  
   характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные  
   решения по первому столбцу, соответствующему высокому уровню защищенности), а  
   остальные - среднему уровню защищенности (положительные решения по второму  
   столбцу)( Y1=0).
2. ИСПДн имеет **средний** уровень исходной защищенности, если не выполняются  
   условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже  
   «средний» (берется отношение суммы положительные решений по второму столбцу,  
   соответствующему среднему уровню защищенности, к общему количеству решений), а  
   остальные - низкому уровню защищенности (Y1=5).
3. ИСПДн имеет **низкую** степень исходной защищенности, если не выполняются  
   условия по пунктам 1 и 2 (Y1=10).
   1. Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем  
показатель, характеризующий, насколько вероятным является реализация конкретной  
УБПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы  
определяется по 4 вербальным градациям этого показателя:

**маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы

(Y2 = 0);

**низкая вероятность**- объективные предпосылки для реализации угрозы существуют,  
но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

**средняя вероятность** - объективные предпосылки для реализации угрозы  
существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

**высокая вероятность** - объективные предпосылки для реализации угрозы  
существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

При обработке ПДн в ИСПДн можно выделить следующие угрозы:

* + 1. Угрозы утечки информации по ТКУИ
       1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся  
непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн,  
возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн функции голосового ввода ПДн или функции воспроизведения ПДн  
акустическими средствами отсутствуют.

Вероятность реализации угрозы - .

* + - 1. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с  
помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств  
отображения СВТ, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

В ИСПДн введен контроль доступа в КЗ, АРМ пользователей расположены так, что  
практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы - .

* + - 1. Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных  
электромагнитных излучений у элементов ИСПДн.

*Угрозы данного класса маловероятны, т.к. размер КЗ большой, и элементы ИСПДн  
экранируются несколькими несущими стенами, и паразитный сигнал маскируется со  
множеством других паразитных сигналов элементов, не входящих в ИСПДн.*

Вероятность реализации угрозы - .

* + 1. Угрозы НСД к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения  
ее безопасности:

нарушению конфиденциальности (копирование, неправомерное распространение);

нарушению целостности (уничтожение, изменение);

нарушению доступности (блокирование).

* + - 1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей  
         информации путем физического доступа к элементам ИСПДн
         1. Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в  
помещения, где расположены элементы ИСПДн.

В введен контроль доступа в КЗ, установлена охранная сигнализация, двери  
закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - .

* + - * 1. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к  
носителям информации.

В введен контроль доступа в КЗ, установлена охранная сигнализация, двери  
закрываются на замок, установлены решетки на первых и последних этажах здания, ведется  
учет и хранение носителей в сейфе.

Вероятность реализации угрозы - .

* + - * 1. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в  
помещения, где происходит работа пользователей.

В (наименование оператора) введен контроль доступа в КЗ, установлена охранная  
сигнализация, двери закрываются на замок, установлены решетки на первых и последних  
этажах здания, организовано хранение ключей в сейфе.

Вероятность реализации угрозы - .

* + - * 1. Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в  
помещения, где расположены элементы ИСПДн и СЗИ, а так же происходит работа  
пользователей.

В (наименование оператора) введен контроль доступа в КЗ, установлена охранная  
сигнализация, двери закрываются на замок, установлены решетки на первых и последних  
этажах здания, осуществляется разграничение доступа пользователей к защищаемым  
ресурсам ИСПДн.

Вероятность реализации угрозы - .

* + - * 1. Вывод из строя узлов ИСПДн, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в  
помещения, где расположены элементы ИСПДн и проходят каналы связи.

В (наименование оператора)введен контроль доступа в КЗ, установлена охранная  
сигнализация, двери закрываются на замок, установлены решетки на первых и последних  
этажах здания.

Вероятность реализации угрозы - .

* + - * 1. Несанкционированное отключение СЗИ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в  
помещения, где расположены СЗИ ИСПДн.

В (наименование оператора) введен контроль доступа в КЗ, установлена охранная  
сигнализация, двери закрываются на замок, установлены решетки на первых и последних  
этажах здания, осуществляется разграничение доступа к настройкам СЗИ.

Вероятность реализации угрозы - .

1.8.2.2. Угрозы хищения, несанкционированной модификации или блокирования  
информации за счет НСД с применением программно-аппаратных и программных средств (в том числе ПМВ)

1. Действия вредоносных программ (вирусов)

На всех элементах ИСПДн установлена антивирусная защита.

Вероятность реализации угрозы - .

1. Недекларированные возможности системного программного обеспечения и  
   программного обеспечения для обработки ПДн

В ИСПДн применяется программное обеспечение, разработанное сторонними  
специалистами.

Вероятность реализации угрозы - .

1. Установка программного обеспечения не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки программного  
обеспечения внутренними нарушителями, что может привести к нарушению  
конфиденциальности, целостности и доступности ПДн, обрабатываемых в ИСПДн.

В ИСПДн определен перечень прав пользователей и осуществляется разграничение  
доступа к ресурсам ИСПДн.

Вероятность реализации угрозы - .

1. Угрозы не преднамеренных действий пользователей и нарушений  
   безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном  
   обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности  
   элементов, сбоев электропитания) и стихийного характера
2. Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей  
ИСПДн, которые нарушают положения парольной политике в части их создания (создают  
легкие или пустые пароли, не меняют пароли по истечении срока их жизни или  
компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают  
ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В ИСПДн введена парольная политика, предусматривающая требуемую сложность  
пароля и периодическую его смену, осуществляется контроль за ее выполнением,  
пользователи проинструктированы о парольной политике и о действиях в случаях утраты  
или компрометации паролей.

Вероятность реализации угрозы - .

1. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей  
ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не  
осведомлены о них.

В ИСПДн осуществляется резервное копирование обрабатываемых ПДн.

Вероятность реализации угрозы - .

1. Непреднамеренное отключение СЗИ

Угроза осуществляется за счет действия человеческого фактора пользователей  
ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и СЗИ или не  
осведомлены о них.

В ИСПДн осуществляется разграничение доступа к настройкам СЗИ.

Вероятность реализации угрозы - .

1. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств,  
из-за которых может происходить нарушение целостности и доступности ПДн.

В (наименование оператора)осуществляется резервирование ключевых элементов  
ИСПДн.

Вероятность реализации угрозы - .

1. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за  
чего может происходить нарушение целостности и доступности ПДн.

В ИСПДн ко всем ключевым элементам подключены источники бесперебойного  
питания и осуществляет резервное копирование ПДн.

Вероятность реализации угрозы - .

1. Угрозы преднамеренных действий внутренних нарушителей
2. Доступ к информации, модификация, уничтожение лицами, не  
   допущенными к ее обработке

Угроза осуществляется путем НСД внешних пользователей к элементам ИСПДн.

В ИСПДн осуществляется разграничение доступа к ПДн, проводится резервное  
копирование обрабатываемых ПДн.

Вероятность реализации угрозы - .

1. Разглашение информации, модификация, уничтожение сотрудниками,  
   допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн,  
которые нарушают положения о неразглашении ПДн.

В ИСПДн пользователи осведомлены о порядке работы с ПДн.

Вероятность реализации угрозы - .

1. Угрозы НСД по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных,  
обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям связи общего  
пользования и (или) сетям международного информационного обмена» (п. 6.6.Базовой  
модели угроз безопасности персональных данных при их обработке в информационных

системах персональных данных, ФСТЭК России 2008 г.), для ИСПДн рассматриваются  
следующие угрозы, реализуемые с использованием протоколов межсетевого  
взаимодействия:

угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и  
принимаемой из внешних сетей информации;

угрозы сканирования, направленные на выявление типа или типов используемых  
операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых  
портов и служб, открытых соединений и др.;

угрозы выявления паролей по сети;

угрозы навязывание ложного маршрута сети;

угрозы подмены доверенного объекта в сети;

угрозы внедрения ложного объекта в сети;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и  
   принимаемой из внешних сетей информации

Эта угроза реализуется с помощью специальной программы-анализатора пакетов,  
перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в  
которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы  
нарушитель:

изучает логику работы ИСПДн - то есть стремится получить однозначное  
соответствие событий, происходящих в системе, и команд, пересылаемых при этом рабочей  
станцией, в момент появления данных событий. В дальнейшем это позволяет  
злоумышленнику на основе задания соответствующих команд получить, например,  
привилегированные права на действия в системе или расширить свои полномочия в ней;

перехватывает поток передаваемых данных, которыми обмениваются компоненты  
сетевой операционной системы, для извлечения конфиденциальной или идентификационной  
информации (например, статических паролей пользователей для доступа к удаленным  
рабочим станциям по протоколам FTP и TEL№ET, не предусматривающих шифрование), ее  
подмены, модификации и т.п.

1. Перехват за переделами КЗ  
   Вероятность реализации угрозы - .
2. Перехват в пределах КЗ внешними нарушителями

В (наименование оператора) введен контроль доступа в КЗ, установлена охранная  
сигнализация, двери закрываются на замок, установлены решетки на первых и последних  
этажах здания.

Вероятность реализации угрозы - .

1. Перехват в пределах КЗ внутренними нарушителями

В ИСПДн осуществляется разграничение доступа к ресурсам ИСПДн.

Вероятность реализации угрозы - .

1. Угрозы сканирования сети, направленные на выявление типа или типов  
   используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии  
   сети, открытых портов и служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым  
службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых  
протоколов, доступных портов сетевых служб, законов формирования идентификаторов  
соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей  
пользователей.

Вероятность реализации угрозы - .

1. Угрозы выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной  
защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов,  
таких как простой перебор, перебор с использованием специальных словарей, установка  
вредоносной программы для перехвата пароля, подмена доверенного объекта сети и перехват  
пакетов. В основном для реализации угрозы используются специальные программы, которые  
пытаются получить доступ к рабочей станции путем последовательного подбора паролей. В  
случае успеха, злоумышленник может создать для себя «проход» для будущего доступа,  
который будет действовать, даже если на рабочей станции изменить пароль доступа.

Вероятность реализации угрозы - .

1. Угрозы навязывание ложного маршрута в сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или  
межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена  
недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы  
идентификации сетевых управляющих устройств), в результате чего можно попасть,  
например, на хост или в сеть злоумышленника, где можно войти в операционную среду  
технического средства в составе ИСПДн. Реализации угрозы основывается на  
несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и  
управления сетью (ICMP, S№MP) для внесения изменений в маршрутно-адресные таблицы.  
При этом нарушителю необходимо послать от имени сетевого управляющего устройства  
(например, маршрутизатора) управляющее сообщение.

Вероятность реализации угрозы - .

1. Угрозы подмены доверенного объекта в сети

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие  
алгоритмы идентификации и аутентификации объектов, пользователей и т.д. Под  
доверенным объектом понимается объект сети (СВТ, межсетевой экран, сетевой коммутатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с  
установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении  
прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с  
объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует  
преодоления системы идентификации и аутентификации сообщений.

Процесс реализации угрозы без установления виртуального соединения может иметь  
место в сетях, осуществляющих идентификацию передаваемых сообщений только по  
сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от  
имени сетевых управляющих устройств (например, от имени маршрутизаторов) об  
изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому  
средству ИСПДн - цели угроз.

Вероятность реализации угрозы - .

1. Угрозы внедрения ложного объекта в сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В  
случае если объекты сети изначально не имеют адресной информации друг о друге,  
используются различные протоколы удаленного поиска (например, ARP, D№S, WI№S в  
сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных  
запросов и получении на них ответов с искомой информацией. При этом существует  
возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа,  
использование которого приведет к требуемому изменению маршрутно-адресных данных. В  
дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет  
проходить через ложный объект сети.

Вероятность реализации угрозы - .

1. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его  
уязвимостях, позволяющих нарушителю создавать условия, когда ОС оказывается не в  
состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на  
обработку пакетов, передаваемых злоумышленником со снижением пропускной способности  
каналов связи, производительности сетевых устройств, нарушением требований к времени  
обработки запросов. Примерами реализации угроз подобного рода могут служить:  
направленный шторм запросов на установление TCP-соединений, шторм запросов к FTP-  
серверу;

явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при  
обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания  
каналов связи, переполнение очередей запросов на обслуживание), при котором легальные  
запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо  
получают отказ в обслуживании ввиду переполнения очередей запросов, дискового  
пространства памяти и т.д. Примерами угроз данного типа могут служить шторм сообщений почтовому серверу;

явный отказ в обслуживании, вызванный нарушением логической связности между  
техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от  
имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или  
идентификационной и аутентификационной информации;

явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с  
нестандартными атрибутами или имеющих длину, превышающую максимально допустимый

размер, что может привести к сбою сетевых устройств, участвующих в обработке запросов,  
при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности  
соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с  
одного адреса такого количества запросов на подключение к техническому средству в составе  
ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»),  
что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или  
полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме  
обработки запросов.

Вероятность реализации угрозы - .

1. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на рабочей станции ИСПДн различные  
предварительно внедренные вредоносные программы: программы-закладки, вирусы,  
«сетевые шпионы», основная цель которых - нарушение конфиденциальности,  
целостности, доступности информации и полный контроль за рабочей станцией. Кроме  
того, возможен несанкционированный запуск прикладных программ пользователей для  
несанкционированного получения необходимых нарушителю данных, для запуска  
управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

распространение файлов, содержащих несанкционированный исполняемый код;

удаленный запуск приложения путем переполнения буфера приложений-серверов;

удаленный запуск приложения путем использования возможностей удаленного  
управления системой, предоставляемых скрытыми программными и аппаратными  
закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации  
распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут  
служить: файлы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов,  
интерпретируемых скриптов; файлы, содержащие исполняемые коды программ. Для  
распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые  
сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных  
регистров иногда удается переключить процессор после прерывания, вызванного переполнением  
буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами), либо штатными средствами управления и администрирования компьютерных сетей. В результате их использования удается добиться удаленного контроля над станцией в сети.

Вероятность реализации угрозы - .

1. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для  
своего распространения активно используют протоколы и возможности локальных и

глобальных сетей. Основным принципом работы сетевого вируса является возможность  
самостоятельно передать свой код на удаленный сервер или рабочую станцию.  
«Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на  
выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть»  
пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:  
программы подбора и вскрытия паролей;  
программы, реализующие угрозы;

программы, демонстрирующие использование не декларированные возможности  
программного и программно-аппаратного обеспечения ИСПДн;  
программы-генераторы компьютерных вирусов;  
программы, демонстрирующие уязвимости СЗИ и др.

Вероятность реализации угрозы - .

* 1. Реализуемость угроз

По итогам оценки уровня защищенности (y1) и вероятности реализации угрозы (Y2),  
рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность  
реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться  
соотношением Y = (Y1+ Y2)/20

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

если 0 < Y < 0,3, то возможность реализации угрозы признается низкой;  
если 0,3 < Y < 0,6, то возможность реализации угрозы признается средней;  
если 0,6 < Y < 0,8, то возможность реализации угрозы признается высокой;  
если Y > 0,8, то возможность реализации угрозы признается очень высокой.

Оценка реализуемости УБПДн представлена в таблице 4.

Таблица 4. Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность  реализации |
| 1. Угрозы от утечки по техническим каналам | | |
| 1.1. Угрозы утечки акустической информации |  |  |
| 1.2. Угрозы утечки видовой информации |  |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |  |
| 2. Угрозы НСД к информации | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн | | |
| 2.1.1. Кража ПЭВМ |  |  |
| 2.1.2. Кража носителей информации |  |  |
| 2.1.3. Кража ключей и атрибутов доступа |  |  |
| 2.1.4. Кражи, модификации, уничтожения информации |  |  |
|  |  |  |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи |  |  |
| 2.1.6. Несанкционированное отключение СЗИ |  |  |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе ПМВ) | | |
| 2.2.1. Действия вредоносных программ (вирусов) |  |  |
| 2.2.2. Не декларированные возможности системного программного обеспечения и программного обеспечения для обработки ПДн |  |  |
| 2.2.3. Установка программного обеспечения не связанного с исполнением служебных обязанностей |  |  |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) | | |
| 2.3.1. Утрата ключей и атрибутов доступа |  |  |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками |  |  |
| 2.3.3. Непреднамеренное отключение СЗИ |  |  |
| 2.3.4. Выход из строя аппаратно-программных средств |  |  |
| 2.3.5. Сбой системы электроснабжения |  |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке |  |  |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке |  |  |
| 2.5.Угрозы НСД по каналам связи | | |
| 2.5.1.Угроза «Анализ сетевого трафика» |  |  |
| 2.5.1.1. Перехват за переделами КЗ |  |  |
| 2.5.1.2. Перехват в пределах КЗ внешними нарушителями |  |  |
| 2.5.1.3.Перехват в пределах КЗ внутренними нарушителями |  |  |
| 2.5.2.Угрозы сканирования сети |  |  |
| 2.5.3.Угрозы выявления паролей по сети |  |  |
| 2.5.4.Угрозы навязывание ложного маршрута в сети |  |  |
| 2.5.5.Угрозы подмены доверенного объекта в сети |  |  |
| 2.5.6.Угрозы внедрения ложного объекта в сети |  |  |
| 2.5.7.Угрозы типа «Отказ в обслуживании» |  |  |
| 2.5.8.Угрозы удаленного запуска приложений |  |  |
| 2.5.9.Угрозы внедрения по сети вредоносных программ |  |  |

* 1. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите  
информации и определяется вербальным показателем опасности, который имеет три  
значения:

**низкая опасность** - если реализация угрозы может привести к незначительным  
негативным последствиям для субъектов ПДн;

**средняя опасность** - если реализация угрозы может привести к негативным  
последствиям для субъектов ПДн;

**высокая опасность** - если реализация угрозы может привести к значительным  
негативным последствиям для субъектов ПДн.

Оценка опасности УБПДн представлена в таблице 5.

Таблица 5. Опасность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам | |
| 1.1. Угрозы утечки акустической информации |  |
| 1.2. Угрозы утечки видовой информации |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |
| 2. Угрозы НСД к информации | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ |  |
| 2.1.2. Кража носителей информации |  |
| 2.1.3. Кража ключей и атрибутов доступа |  |
| 2.1.4. Кражи, модификации, уничтожения информации |  |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи |  |
| 2.1.6. Несанкционированное отключение СЗИ |  |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе ПМВ) | |
| 2.2.1. Действия вредоносных программ (вирусов) |  |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 2.2.2. Не декларированные возможности системного программного обеспечения и программного обеспечения для обработки ПДн |  |
| 2.2.3. Установка программного обеспечения не связанного с исполнением служебных обязанностей |  |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) | |
| 2.3.1. Утрата ключей и атрибутов доступа |  |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками |  |
| 2.3.3. Непреднамеренное отключение СЗИ |  |
| 2.3.4. Выход из строя аппаратно-программных средств |  |
| 2.3.5. Сбой системы электроснабжения |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке |  |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке |  |
| 2.5.Угрозы НСД по каналам связи | |
| 2.5.1.Угроза «Анализ сетевого трафика» |  |
| 2.5.1.1. Перехват за переделами с КЗ |  |
| 2.5.1.2. Перехват в пределах КЗ внешними нарушителями |  |
| 2.5.1.3.Перехват в пределах КЗ внутренними нарушителями |  |
| 2.5.2.Угрозы сканирования сети |  |
| 2.5.3.Угрозы выявления паролей по сети |  |
| 2.5.4.Угрозы навязывание ложного маршрута в сети |  |
| 2.5.5.Угрозы подмены доверенного объекта в сети |  |
| 2.5.6.Угрозы внедрения ложного объекта в сети |  |
| 2.5.7.Угрозы типа «Отказ в обслуживании» |  |
| 2.5.8.Угрозы удаленного запуска приложений |  |
| 2.5.9.Угрозы внедрения по сети вредоносных программ |  |

* 1. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для  
ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6. Правила определения актуальности УБПДн

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

Оценка актуальности угроз безопасности представлена в таблице 7.

Таблица 7. Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам | |
| 1.1. Угрозы утечки акустической информации |  |
| 1.2. Угрозы утечки видовой информации |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |
| 2. Угрозы НСД к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ |  |
| 2.1.2. Кража носителей информации |  |
| 2.1.3. Кража ключей и атрибутов доступа |  |
| 2.1.4. Кражи, модификации, уничтожения информации |  |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи |  |
| 2.1.6. Несанкционированное отключение СЗИ |  |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе ПМВ) | |
| 2.2.1. Действия вредоносных программ (вирусов) |  |
| 2.2.2. Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки ПДн |  |
| 2.2.3. Установка программного обеспечения не связанного с исполнением служебных обязанностей |  |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) | |
| 2.3.1. Утрата ключей и атрибутов доступа |  |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками |  |
| 2.3.3. Непреднамеренное отключение СЗИ |  |
| 2.3.4. Выход из строя аппаратно-программных средств |  |
| 2.3.5. Сбой системы электроснабжения |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке |  |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке |  |
| 2.5.Угрозы НСД по каналам связи. | |
| 2.5.1.Угроза «Анализ сетевого трафика» |  |
| 2.5.1.1. Перехват за переделами КЗ |  |
| 2.5.1.2. Перехват в пределах КЗ внешними нарушителями |  |
| 2.5.1.3.Перехват в пределах КЗ внутренними нарушителями. |  |
| 2.5.2.Угрозы сканирования сети |  |
| 2.5.3.Угрозы выявления паролей по сети |  |
| 2.5.4.Угрозы навязывание ложного маршрута в сети |  |
| 2.5.5.Угрозы подмены доверенного объекта в сети |  |
| 2.5.6.Угрозы внедрения ложного объекта как в сети |  |
| 2.5.7.Угрозы типа «Отказ в обслуживании» |  |
| 2.5.8.Угрозы удаленного запуска приложений |  |
| 2.5.9.Угрозы внедрения по сети вредоносных программ |  |

Были выявлены следующие актуальные угрозы:

1) ,

2) ,

3) .

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить  
следующие мероприятия:

1) ,

2) ,

3) .

* 1. Модель угроз безопасности ПДн при их обработке в ИСПДн (наименование ИСПДн) (сводная таблица)

Исходный уровень защищенности -\_\_\_\_\_\_\_\_\_\_\_.

Таблица 8. Угрозы безопасности

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность  угрозы | Актуальность  угрозы | Меры по противодействию угрозе | |
| Технические | Организационные |
| 1. Угрозы от утечки по техническим каналам | | | | | | |
| 1.1. Угрозы утечки акустической информации |  |  |  |  |  |  |
| 1.2. Угрозы утечки видовой информации |  |  |  |  |  |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |  |  |  |  |  |
| 2. Угрозы НСД к информации | | | | | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн | | | | | | |
| 2.1.1. Кража ПЭВМ |  |  |  |  |  |  |
| 2.1.2. Кража носителей информации |  |  |  |  |  |  |
| 2.1.3. Кража ключей и атрибутов доступа |  |  |  |  |  |  |
| 2.1.4. Кражи, модификации, уничтожения информации |  |  |  |  |  |  |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи |  |  |  |  |  |  |
| 2.1.6. Несанкционированное отключение СЗИ |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно- аппаратных и программных средств (в том числе ПМВ) | | | | | | | | | | |
| 2.2.1. Действия вредоносных программ (вирусов) |  | |  | |  | |  | |  |  |
| 2.2.2. Недекларированные возможности системного программного обеспечения и программного обеспечения для обработки ПДн |  | |  | |  | |  | |  |  |
| 2.2.3. Установка программного обеспечения не связанного с исполнением служебных обязанностей |  | |  | |  | |  | |  |  |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПД н в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) | | | | | | | | | | |
| 2.3.1. Утрата ключей и атрибутов доступа |  | |  | |  | | |  |  |  |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками |  | |  | |  | | |  |  |  |
| 2.3.3. Непреднамеренное отключение СЗИ |  | |  | |  | | |  |  |  |
| 2.3.4. Выход из строя аппаратно- программных средств |  | |  | |  | | |  |  |  |
| 2.3.5. Сбой системы электроснабжения |  | |  | |  | | |  |  |  |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | | | | | | | | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | |  | |  | |  | |  |  |  |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | |  | |  | |  | |  |  |  |
| 2.5. Угрозы НСД по каналам связи | |  | |  | |  | |  |  |  |
| 2.5.1. Угроза «Анализ сетевого трафика» | |  | |  | |  | |  |  |  |
| 2.5.1.1. Перехват за переделами КЗ | |  | |  | |  | |  |  |  |
| 2.5.1.2. Перехват в пределах КЗ внешними нарушителями | |  | |  | |  | |  |  |  |
| 2.5.1.3. Перехват в пределах КЗ внутренними нарушителями | |  | |  | |  | |  |  |  |
| 2.5.2.Угрозы сканирование сети | |  | |  | |  | |  |  |  |
| 2.5.3. Угрозы выявления паролей по сети | |  | |  | |  | |  |  |  |
| 2.5.4. Угрозы навязывание ложного маршрута в сети | |  | |  | |  | |  |  |  |
| 2.5.5. Угрозы подмены доверенного объекта в сети | |  | |  | |  | |  |  |  |
| 2.5.6. Угрозы внедрения ложного объекта в сети | |  | |  | |  | |  |  |  |
| 2.5.7. Угрозы типа «Отказ в обслуживании» | |  | |  | |  | |  |  |  |
| 2.5.8. Угрозы удаленного запуска приложений | |  | |  | |  | |  |  |  |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | |  | |  | |  | |  |  |  |

**Заключение**

В соответствии с Постановлением Правительства Российской Федерации от 1 ноября  
2012 г. № 1119 «Об утверждении требований к защите персональных данных при их  
обработке в информационных системах персональных данных», Приказа ФСТЭК России от  
18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и  
технических мер по обеспечению безопасности персональных данных при их обработке в  
информационных системах персональных данных» и в соответствии с моделью угроз  
безопасности персональных данных информационная система персональных данных  
(указывается наименование ИСПДн) присваивается уровень защищенности.

**Приложение 30. ПРОЕКТ**

Регламент

учета средств защиты информации, эксплуатационной и технической  
документации к ним, электронных носителей персональных данных

**Общие положения**

Регламент учета СЗИ, эксплуатационной и технической документации к ним,  
электронных носителей персональных данных устанавливает:

* порядок учета, ввода в эксплуатацию и изъятия из употребления средств,  
  используемых для обеспечения безопасности ПДн при их обработке в ИСПДн;
* порядок учета и хранения электронных носителей информации, содержащих

ПДн.

Требования настоящего Регламента распространяются на всех должностных лиц,  
допущенных к обработке ПДн.

1. **Порядок учета и хранения средств защиты информации**

Используемые или хранимые оператором СЗИ, эксплуатационная и техническая  
документация к ним подлежат поэкземплярному учету в журнале поэкземплярного учета  
СЗИ, эксплуатационной и технической документации к ним (Таблица 1).

Учет СЗИ, эксплуатационной и технической документации к ним осуществляется  
ответственным за обеспечение безопасности ПДн, администратором безопасности или иным уполномоченным лицом.

Программные средства учитываются совместно с аппаратными средствами, с  
которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-  
программные СЗИ подключаются к системной шине или к одному из внутренних  
интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с  
соответствующими аппаратными средствами.

Все экземпляры СЗИ, эксплуатационная и техническая документация к ним должны  
выдаваться пользователям СЗИ, несущим персональную ответственность за их сохранность  
под роспись в соответствующем журнале.

Эксплуатационная и техническая документация, а также электронные носители с  
инсталляционными файлами СЗИ должны содержаться в хранилищах (шкафах, ящиках,  
сейфах и др.), исключающих бесконтрольный доступ к ним, а также их непреднамеренное  
уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование СЗИ,  
должны быть оборудованы средствами контроля за их вскрытием (опечатаны,  
опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его  
можно было визуально контролировать.

СЗИ изымаются из употребления по решению ответственного за обеспечение  
безопасности ПДн, при этом вносятся необходимые изменения в журнал поэкземплярного  
учета средств защиты информации, эксплуатационной и технической документации к ним.

СЗИ считаются изъятыми из употребления, если исполнена предусмотренная  
эксплуатационной и технической документацией процедура удаления программного  
обеспечения СЗИ, и они полностью отключены от аппаратных средств.

1. **Порядок учета электронных носителей персональных данных**

В структурных подразделениях оператора, работающих с ИСПДн, учет носителей  
ПДн осуществляется специально уполномоченными из числа сотрудников лицами (далее -  
делопроизводителями).

При смене делопроизводителя, составляется акт приема-сдачи носителей ПДн и всех  
журналов учета, который утверждается руководителем или начальником подразделения,  
ответственного за обеспечение безопасности ПДн.

Делопроизводитель выдает носители ПДн только сотрудникам, имеющим допуск к ПДн.

Перед записью ПДн на носитель, сотрудник передает его делопроизводителю для

учета.

При получении носителей ПДн из сторонних организаций они передаются  
делопроизводителю для учета, после чего могут быть выданы исполнителям для работы.

На носителях ПДн проставляются следующие реквизиты:

* регистрационный номер;
* дата и роспись делопроизводителя.

Учет носителей ПДн производится в «Журнале учета электронных носителей  
персональные данные».

Движение (выдача и возврат) носителей с ПДн должно отражаться в  
соответствующем «Журнале учета выдачи и возврата электронных носителей персональных  
данных». Выдача носителей ПДн сотруднику производится под его личную роспись.

Передача носителей с ПДн другим сотрудникам, имеющим допуск к ПДн,  
производится только через делопроизводителя с обязательной записью в «Журнале учета  
выдачи и возврата электронных носителей персональных данных».

Листы журналов нумеруются, прошиваются и опечатываются.

1. **Порядок хранения электронных носителей персональных данных**

Носители информации с ПДн должны храниться в служебных помещениях, в надежно  
запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить носители с ПДн из служебных помещений без согласования с  
делопроизводителем.

Сотрудники должны после окончания работы запирать полученные носители ПДн в  
личный сейф, в случае его отсутствия сдавать делопроизводителю.

Проверка наличия носителей ПДн проводится один раз в год комиссией. В ходе  
ревизии комиссия определяет перечень носителей ПДн, которые (информацию на которых)  
можно уничтожить.

Проверка наличия носителей ПДн при необходимости может проводиться  
ответственным за обеспечение безопасности ПДн или специально уполномоченным лицом.

Уничтожение носителей ПДн (информации на них), утративших свое практическое  
значение и не имеющих исторической ценности, производится по акту. В учетных журналах  
об этом делается отметка со ссылкой на соответствующий акт.

1. **Ответственность за выполнение регламента**

На пользователей ИСПДн, ответственных за обеспечение безопасности ПДн,  
администраторов безопасности, делопроизводителей возлагается персональная  
ответственность за выполнение всех обязанностей, возложенных на них в настоящем  
Регламенте.

За правонарушения, совершенные в процессе своей деятельности должностные лица  
несут ответственность в пределах, определенных действующим административным,  
уголовным и гражданским законодательством Российской Федерации.

Таблица1. Форма журнала поэкземплярного учета средств защиты информации,  
эксплуатационной и технической документации к ним

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование средства защиты информации/ эксплуатационной, технической документации | Регистрационные номера средства защиты информации/ эксплуатационной, технической документации | Отметка о подключении (установке) средства защиты информации | | Отметка об изъятии средства защиты информации из аппаратных средств | | Примечание |
| Ф.И.О. лица, производившего подключение (установку) средства защиты информации, дата, подпись | Номера аппаратных средств, в которые установлены или к которым подключены средства защиты информации | Ф.И.О. лица, производившего изъятие средства защиты информации, дата, подпись | Номер акта или расписка об  уничтожении |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Приложение 31. ПРОЕКТ**

Положение

по обеспечению безопасности персональных данных при их обработке в  
информационных системах персональных данных (наименование оператора)

**Назначение документа**

Настоящий документ определяет порядок организации и проведения работ по  
обеспечению безопасности ПДн при их обработке в ИСПДн (наименование оператора) и  
содержит общие принципы защиты ПДн.

Данный документ направлен на достижение следующих целей:

* выполнение требований законодательства в области обеспечения безопасности

ПДн;

* защита прав и свобод граждан РФ при обработке их ПДн в ИСПДн оператора;
* защита ПДн, обрабатываемых оператором, от НСД и от других  
  несанкционированных действий.

1. **Область действия**

Требования настоящего Положения распространяются на все подразделения  
оператора, которые участвуют в обработке ПДн, либо в организации обработки ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение  
функционирования ИСПДн.

Настоящий документ обязаны знать и использовать в работе все сотрудники  
оператора, а также другие лица, допущенные к работе в ИСПДн.

1. **Общие положения**

Настоящее Положение устанавливает требования по защите ПДн, принципы  
обработки ПДн в ИСПДн оператора.

Настоящее Положение разработано в соответствии со следующими нормативными  
актами:

* Федеральным законом Российской Федерации от 27 июля 2006 г. №152-ФЗ «О  
  персональных данных»;
* Федеральным законом Российской Федерации от 27 июля 2006 г. №149-ФЗ  
  «Об информации, информационных технологиях и о защите информации»;
* Постановлением Правительства Российской Федерации от 15 сентября 2008 г.  
  №687 «Об утверждении Положения об особенностях обработки персональных данных,  
  осуществляемой без использования средств автоматизации»;
* Постановления Правительства Российской Федерации от 1 ноября 2012 г. №  
  1119 «Об утверждении требований к защите персональных данных при их обработке в  
  информационных системах персональных данных»;
* Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава  
  и содержания организационных и технических мер по обеспечению безопасности  
  персональных данных при их обработке в информационных системах персональных  
  данных»
* методическими документами ФСБ России, ФСТЭК России, Роскомнадзора.

Настоящее Положение является методологической основой для:

* формирования и проведения единой политики в области обеспечения  
  безопасности ПДн;
* принятия управленческих решений и разработки практических мер по  
  воплощению политики безопасности ПДн и выработки комплекса согласованных мер  
  нормативно-правового, технического и организационно-технического характера,  
  направленных на выявление, отражение и уменьшение УБПДн;
* координации деятельности при проведении работ по созданию, развитию и  
  эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;
* разработки предложений по совершенствованию правового, нормативного,  
  методического, технического и организационного обеспечения безопасности ПДн в ИСПДн.

Принципы и требования по обеспечению безопасности ПДн распространяются:

* на все возможные формы существования информации, такие как:

физические поля (электрические, акустические, электромагнитные, оптические и т.п.);

носители на бумажной, магнитной, оптической и иной основе.

* на все возможные форматы представления ПДн, такие как:
* документы;
* голос;
* изображения;
* файлы;
* почтовые сообщения;
* базы данных;
* записи базы данных;
* другие информационные массивы.

Предотвращение несанкционированного и нелегитимного доступа к ИСПДн,  
технологиям и информационным ресурсам результатом которого может стать уничтожение,  
модификация, искажение, копирование, распространение, блокирование ПДн требует  
применения комплекса правовых, организационных, организационно-технических мер  
защиты с использованием сертифицированных СЗИ.

Настоящее Положение определяет:

* роли, полномочия, ответственность за обеспечение безопасности ПДн,  
  подразделений оператора;
* порядок организации и проведения работ по обеспечению безопасности ПДн  
  при их обработке в ИСПДн;
* мероприятия по обеспечению безопасности ПДн;
* требования по управлению процессом обеспечения безопасности ПДн;
* требования к составу и содержанию документов оператора, регламентирующих  
  защиту и работу с ПДн.

Целью создания СЗПДн является исключение неправомерного или случайного  
доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения  
ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это  
обеспечение:

* конфиденциальности ПДн;
* целостности ПДн;
* доступности ПДн;
* неотказуемости.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется  
по результатам разработки модели угроз и нарушителя безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

* определение новых ИСПДн;
* инвентаризация и управление изменениями в составе и структуре ИСПДн;
* сбор согласий на обработку ПДн с субъектов ПДн;
* разработка и актуализация Перечня сведений конфиденциального характера;
* уничтожение ПДн;
* управление взаимодействиями с внешними контрагентами по вопросам  
  обработки ПДн;
* взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
* определение уровня защищенности ИСПДн;
* разработка (актуализация) документации на СЗПДн;
* выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
* эксплуатация СЗПДн в соответствии с документацией на нее;
* контроль уровня защищенности ПДн;
* обучение персонала по вопросам защиты ПДн;
* учет применяемых СЗИ, эксплуатационной и технической документации к ним,  
  носителей ПДн;
* учет лиц, допущенных к обработке ПДн;
* взаимодействие с регуляторными органами по вопросам защиты ПДн;
* актуализация и подача уведомлений в уполномоченный орган по защите прав  
  субъектов ПДн;
* аттестация (декларирование соответствия) по требованиям безопасности  
  информации;
* получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн.

Обработка ПДн должна осуществляться в соответствии со следующими принципами:

* законности целей и способов обработки ПДн и добросовестности;
* соответствия целей обработки ПДн целям, заранее определенным и  
  заявленным при сборе ПДн, а также полномочиям оператора;
* соответствия объема и характера обрабатываемых ПДн, способов обработки  
  ПДн целям обработки ПДн;
* достоверности ПДн, их достаточности для целей обработки, недопустимости  
  обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
* недопустимости объединения созданных для несовместимых между собой  
  целей баз данных ИСПДн.

Оператор должен проводить регулярный анализ соответствия процессов обработки  
ПДн указанным принципам. Данный анализ проводится в случае:

* создания новых ИСПДн;
* внесения изменений в технологические процессы существующие в ИСПДн;
* изменения нормативной базы затрагивающей принципы и (или) процессы  
  обработки ПДн в ИСПДн оператора;
* проведения контрольных и проверочных мероприятий на предмет оценки  
  соответствия процессов обработки ПДн заявленным принципам.

Отнесение сведений оператором к ПДн, безопасность которых должна обеспечиваться  
СЗПДн представляет собой процесс обоснованного установления (документального  
оформления и утверждения) критериев их выделения из всей совокупности сведений,  
находящихся в обращении.

В качестве такого критерия у оператора разрабатывается и утверждается Перечень  
персональных данных, подлежащих защите в (указывается наименование оператора).

1. **Организационная структура системы защиты персональных данных**

СЗПДн является частью общей системы обеспечения информационной безопасности  
оператора.

Основу организационной структуры СЗПДн как правило составляют следующие  
организационные структуры:

* руководство;
* ответственные за обеспечение безопасности ПДн;
* администраторы безопасности ИСПДн;
* ответственные за техническое сопровождение ИСПДн;
* структурные подразделения, участвующие в процессах обработки ПДн;
* сотрудники оператора.

Руководство осуществляет следующие основные функции в области обеспечения  
безопасности ПДн:

* обеспечивает общую организацию работ по защите ПДн;
* издает приказы по вопросам организации СЗПДн;
* утверждает Перечень сведений конфиденциального характера;
* назначает ответственных за обеспечение безопасности ПДн;
* утверждает список лиц, допущенных к обработке ПДн;
* рассматривает и утверждает нормативные документы оператора,  
  регламентирующие обработку и защиту ПДн;
* заслушивает при необходимости ответственных за обеспечение  
  безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Ответственные за обеспечение безопасности ПДн осуществляют следующие  
основные функции:

* разрабатывают Перечень сведений конфиденциального характера;
* участвуют в проведении определении уровня защищенности ИСПДн;
* распределяют ответственность по вопросам обработки и защиты ПДн;
* определяют допустимые сроки хранения ПДн по каждой категории ПДн;
* организуют подачу уведомлений в уполномоченный орган по защите прав  
  субъектов ПДн;
* заслушивают руководителей структурных подразделений о принимаемых  
  мерах по состоянию и совершенствованию СЗПДн;
* организуют работы по разработке, изменению и уточнению политик,  
  регламентов, стандартов в части защиты ПДн;
* осуществляют организацию плановых и внеплановых проверочных  
  мероприятий;
* организуют выполнение требований по защите ПДн у оператора;
* проводят разработку и актуализацию локальных нормативных документов,  
  регламентирующих защиту ПДн у оператора;
* проводит ознакомление сотрудников с нормативными документами в области  
  защиты ПДн;
* проводят оценку эффективности принятых мер и применяемых средств защиты

ПДн;

* проводят занятия с сотрудниками по изучению организационно-  
  распорядительных документов по всему комплексу вопросов защиты ПДн;
* разрабатывают и актуализируют частные модели угроз безопасности ПДн и  
  технические задания на СЗПДн;
* определяют необходимость обучения сотрудников по вопросам обеспечения  
  безопасности ПДн, а также определяют формы и программы обучения сотрудников  
  оператора в области защиты ПДн;
* контролируют выполнение сотрудниками требований по защите ПДн;
* организуют работы по сбору сведений об изменениях в составе и структуре  
  ИСПДн;
* осуществляют контроль соответствия изменений в составе и архитектуре  
  ИСПДн требованиям нормативных документов по защите ПДн, а также внутренних  
  организационно-распорядительных документов оператора;
* контролируют исполнение требований по уничтожению ПДн;
* разрабатывают рекомендации по оптимизации существующих и новых  
  информационных процессов обработки ПДн по критериям соответствия требованиям по  
  защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;
* контролируют исполнение требований нормативных документов оператора в  
  области обеспечения безопасности ПДн, структурными подразделениями и сотрудниками;
* организуют и осуществляют взаимодействие с регуляторами по вопросам  
  защиты ПДн;
* участвуют в аттестации (декларировании соответствия) ИСПДн оператора по  
  требованиям безопасности информации;
* управляют проектами по внедрению систем и средств защиты ПДн;
* контролируют ввод в действие, эксплуатацию СЗПДн;
* проводят расследования инцидентов, связанных с нарушением безопасности  
  ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных  
  ситуаций.

Администраторы безопасности ИСПДн осуществляют следующие основные функции:

* осуществляют сопровождение средств и систем защиты ПДн;
* проводят оперативный контроль функционирования средств и систем защиты

ПДн;

* проводят резервирование ПДн;
* ведут учет носителей ПДн;
* осуществляют выявление и регистрацию попыток НСД к компонентам ИСПДн,  
  информационным ресурсам;
* контролируют соответствие технических, программных и программно-  
  аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и СЗПДн;
* осуществляют учет применяемых СЗИ, эксплуатационной и технической  
  документации к ним;
* контролируют выполнение сотрудниками подразделения требований по защите ПДн;
* участвуют в расследованиях причин возникновения нештатных ситуаций;
* готовят предложения по совершенствованию СЗПДн;
* выполняют комплекс мероприятий по защите информации при проведении  
  ремонтных и регламентных работ;
* обеспечивают защиту ПДн при выводе из эксплуатации компонентов ИСПДн.  
  Ответственные за техническое сопровождение ИСПДн осуществляют следующие

основные функции:

* осуществляют сопровождение технических средств и систем ИСПДн.  
  Структурные подразделения, участвующие в процессах обработки ПДн выполняют

следующие основные функции:

* осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
* осуществляют уведомление субъектов ПДн в случаях определенных  
  нормативными актами;
* эксплуатируют СЗПДн в соответствии с документацией на нее.

Сотрудники оператора выполняют следующие основные функции:

* соблюдают требования нормативных документов по защите ПДн;
* осуществляют обработку ПДн в соответствии с заданием и предоставленными  
  полномочиями.

Конкретное распределение функций администраторов безопасности, ответственных за  
техническое сопровождение ИСПДн, сотрудников должно быть приведено в должностных  
инструкциях.

Распределение ролей, полномочий осуществляется в соответствии с Разрешительной  
системой доступа к информационным ресурсам, программным и техническим средствам  
информационных систем персональных данных.

1. **Порядок организации и проведения работ по обеспечению безопасности персональных данных**

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются  
неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн, на следующих  
этапах:

* инициация проекта ИСПДн;
* планирование проекта ИСПДн;
* реализация проекта ИСПДн, в составе:
* выбор технического решения - концепция реализации;
* проектирование ИСПДн;
* производство ИСПДн;
* приемка ИСПДн;
* внедрение ИСПДн;
* передача системы в эксплуатацию;
* документирование проекта.
* эксплуатация ИСПДн;
* модернизация ИСПДн;
* вывод из эксплуатации.

1. **Допуск персонала к обработке персональных данных**

При допуске к ПДн оператор руководствуется утвержденным списком лиц,  
допущенных к обработке ПДн.

Перечень лиц, допущенных к обработке ПДн, составляется и корректируется  
ответственными за обеспечение безопасности ПДн, на основании данных подаваемых  
руководителями структурных подразделений оператора.

1. **Контроль изменений в составе и структуре информационных систем персональных данных**

Все изменения в составе и структуре ИСПДн должны контролироваться и  
регламентироваться ответственными за обеспечение безопасности ПДн.

Контролю подлежат следующие изменения:

* внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и  
  телекоммуникационного оборудования и т.п.);
* изменение мест включения существующих компонент ИСПДн;
* удаление устройства из состава ИСПДн;
* изменение мест установки устройства из состава ИСПДн;
* прокладка новых кабельных линий связи и внешних линий связи или удаление  
  старых кабельных линий связи;
* существенное изменение состава и конфигурации системного и прикладного  
  программного обеспечения, участвующего в обработке ПДн;
* создание новых и изменение существующих технологических процессов  
  связанных с обработкой ПДн.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн  
должно отслеживаться и анализироваться на предмет соответствия требованиям по защите  
ИСПДн. При необходимости должна производиться модернизация СЗПДн.

1. **Защита от несанкционируемого доступа к элементам информационных систем персональных**

Мероприятия по физическому контролю доступа включают:

* мероприятия по контролю доступа на территорию;
* мероприятия по контролю доступа в помещения с оборудованием ИСПДн;
* мероприятия по контролю доступа к техническим средствам ИСПДн;
* мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории оператора.

Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн  
должны иметь прочные входные двери с надежными кодовыми замками или  
приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и  
открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны  
быть оборудованы замками, либо в этих помещениях должны обеспечиваться  
мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах  
обработки ПДн (обслуживающий персонал, другие сотрудники), должно производиться  
только в присутствии сотрудников, участвующих в соответствующих технологических  
процессах.

Расположение мониторов рабочих станций должно препятствовать их  
несанкционированному просмотру со стороны других лиц, не допущенными к обработке  
ПДн.

При выносе устройств, хранящих ПДн, за пределы КЗ для ремонта, замены и т.п.  
должно быть обеспечено гарантированное уничтожение информации хранимой на этих  
устройствах.

1. **Резервирование персональных данных**

Резервирование ПДн должно обеспечить возможность восстановления информации  
при нарушении целостности основных хранилищ данных.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на различные носители информации с  
соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах  
(металлических шкафах). Хранение (по возможности) должно осуществляться в месте,  
территориально удаленном от основного хранилища информации.

Доступ к резервным копиям должен быть строго регламентирован.

1. **Контроль за обеспечением необходимого уровня защищенности персональных данных**

Для обеспечения эффективности процесса обеспечения безопасности ПДн  
проводится:

* контроль за соблюдением требований по обработке и защите ПДн;
* контроль за соблюдением условий использования средств защиты ПДн,  
  предусмотренных эксплуатационной и технической документацией;
* контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

* текущими;
* внезапными;
* плановыми внешними;
* плановыми внутренними.

Ответственность за текущий контроль эффективности обеспечения безопасности ПДн возлагается на администраторов безопасности ИСПДн.

Ответственность за плановый контроль эффективности обеспечения безопасности  
ПДн возлагается на ответственных за обеспечение безопасности ПДн. Данные проверки  
должны включаться в план аудитов информационной безопасности на год.

Для планового контроля эффективности СЗПДн должны использоваться средства  
выявления уязвимостей информационной безопасности.

Внезапные проверки эффективности при необходимости могут проводиться  
специальными группами по решению ответственных за обеспечение безопасности ПДн.

При проведении контроля эффективности в общем случае должно проверяться:

* наличие установленных СЗИ;
* корректность настроек СЗИ;
* выполнение пользователями и администраторами требований инструктивных  
  материалов по защите ПДн;
* исполнение требований к процедурам обработки ПДн (уничтожению ПДн,  
  сбору согласий, допуску персонала к ПДн и т.п.);
* правильность организации работы с носителями ПДн;
* правильность обращения ключевой информации;
* соответствие СЗПДн реальному положению дел у оператора.

1. **Реагирование на нештатные ситуации**

Оператор должен проводить расследования инцидентов, связанных с НСД и другими  
несанкционированными действиями затрагивающими безопасность ПДн.

В рамках данного процесса должны решаться следующие задачи:

* расследование инцидентов, связанных с безопасностью ПДн;
* ликвидация последствий инцидентов связанных с безопасностью ПДн;
* принятие мер по недопущению возникновения подобных инцидентов в  
  дальнейшем.

**Приложение 32. ПРОЕКТ**

**Протокол**

**проведения внутренней проверки условий обработки персональных данных в**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Настоящий Протокол составлен в том, что \_\_.\_\_.20\_\_\_ ответственным за

организацию обработки персональных данных/ комиссией по внутреннему контролю

проведена проверка .

(тема проверки)

Проверка осуществлялась в соответствии с требованиями

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

название документа

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| (должность) |  | (подпись) |  | (Ф.И.О.) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Председатель комиссии | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| Члены комиссии: | | | | |
| (должность) |  | (подпись) |  | (Ф.И.О.) |
| (должность) | (подпись) | (Ф.И.О.) |
| (должность) | (подпись) | (Ф.И.О.) |