Акционерное общество
«Конструкторское бюро специального машиностроения»

Политика информационной безопасности персональных данных при их обработке в информационной системе персональных данных АО «КБСМ»

г. Санкт-Петербург

2016 г.

Содержание

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

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

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

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 и биологические особенности человека и на основе которых можно установить его личность, включая отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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.

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

Информативный сигнал – электрические сигналы, 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 (ИС) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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 – операторы и иные 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.

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.

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 субъ-

ектов, 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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

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

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная за-

кладка может быть реализована в виде вредоносной программы или программного кода.

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 раскрытие персональных данных неопределенному кругу лиц.

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

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья (детальные медицинские данные) 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.

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

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место
ИС	– информационная система персональных данных
КЗ	– контролируемая зона
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
САЗ	– система анализа защищенности
СЗИ	– средства защиты информации
СЗПДн	– система (подсистема) защиты персональных данных
СОВ	– система обнаружения вторжений
ТС	– технические средства

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных АО «КБСМ».

Политика разработана в соответствии со следующими нормативными документами:

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с учетом новых редакций ФЗ);

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утв. Постановлением Правительства РФ от 01.11.2012 г. № 1119;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. Приказом ФСТЭК России от 18.02.2013 г. № 21;

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. Приказом ФСТЭК России 15.02.08 г.

– «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИС, степень ответственности персонала, структура и необходимый уровень защищенности, требования к системе защиты ПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИС.

1 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты предприятия от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных и уровень их защищенности.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожения персональных данных.

Состав объектов защиты представлен в *Перечне персональных данных, подлежащих защите в информационной системе персональных данных*.

Эта Политика информационной безопасности утверждается Генеральным директором предприятия.

2 Область действия

Требования настоящей Политики распространяются на всех сотрудников предприятия (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- Отчёта об обследовании информационной системы персональных данных;
- Перечня персональных данных, подлежащих защите в информационной системе персональных данных;
- Акта определения типа актуальных угроз безопасности персональных данных и требуемого уровня защищенности персональных данных в информационной системе персональных данных;
- Модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным в информационной системе персональных данных;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется тип актуальных угроз для информационной системы персональных данных и необходимый уровень защищённости ПДн в ИС предприятия. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз безопасности персональных данных делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения соответствующего уровня защищенности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИС должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИС:

- АРМ пользователей;
- Сервера приложений;
- СУБД;

- Граница ЛВС;
- Каналов передачи в сети международного обмена (общего пользования), если по ним передаются ПДн.

В зависимости от выбранного уровня защищенности ПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- системы обнаружения вторжений;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче ПДн по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список мер по обеспечению безопасности может включать:

- Идентификацию и аутентификацию субъектов доступа и объектов доступа;
- Управление доступом субъектов доступа к объектам доступа;
- Ограничение программной среды;
- Защиту машинных носителей персональных данных;
- Регистрацию событий безопасности;
- Антивирусную защиту;
- Обнаружение вторжений;
- Контроль (анализ) защищенности персональных данных;
- Обеспечение целостности ИС и персональных данных;
- Обеспечение доступности персональных данных;
- Защиту среды виртуализации;
- Защиту технических средств;
- Защиту ИС, ее средств, систем связи и передачи данных
- Выявление инцидентов и реагирование на них;
- Управление конфигурацией ИС и системы защиты ПДн.

4 Требования к подсистемам системы защиты ПДн

Система защиты персональных данных с учетом актуальных угроз включает в себя следующие подсистемы:

1. Идентификация и аутентификация субъектов доступа и объектов доступа;
2. Управление доступом субъектов доступа к объектам доступа;
3. Регистрация событий безопасности;
4. Ограничение программной среды;
5. Защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;
6. Обеспечение целостности ИС и ПДн;
7. Обеспечение доступности ПДн;
8. Антивирусная защита;
9. Контроль (анализ) защищенности ПДн;
10. Обнаружение (предотвращение) вторжений;
11. Защита среды виртуализации;
12. Защита технических средств;
13. Защита ИС, ее средств, систем связи и передачи данных;
14. Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и к возникновению угроз безопасности ПДн, и реагирование на них;
15. Управление конфигурацией ИС и системы защиты ПДн.

Подсистемы СЗПДн имеют различный функционал в зависимости от установленного уровня защищенности ПДн, определенного в *Акте определения типа актуальных угроз безопасности ПДн и требуемого уровня защищенности ПДн в информационной системе персональных данных*. Список мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн представлен в Приложении 1.

4.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа должна 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). Она предназначена для реализации следующих функций:

- идентификация и аутентификация пользователей, являющихся работниками оператора;
- идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

Подсистема может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

4.2 Управление доступом субъектов доступа к объектам доступа

Подсистема управлением доступом субъектов доступа к объектам доступа

должна обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности, установленных в ИС правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил. Она предназначена для реализации следующих функций:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- предупреждение пользователя при его входе в ИС о том, что в ИС реализованы меры по обеспечению безопасности ПДн, и о необходимости соблюдения установленных оператором правил обработки ПДн;
- оповещение пользователя после успешного входа в ИС о его предыдущем входе в информационную систему;
- ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ИС;
- блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу;
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

- поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- регламентация и контроль использования в ИС технологий беспроводного доступа;
- регламентация и контроль использования в ИС мобильных технических средств;
- управление взаимодействием с ИС сторонних организаций;
- обеспечение доверенной загрузки средств вычислительной техники.

4.3 Ограничение программной среды

Подсистема ограничения программной среды должна обеспечивать установку и (или) запуск только разрешенного к использованию в ИС программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в ИС программного обеспечения. Она предназначена для реализации следующих функций:

- управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
- управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;
- установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
- управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

4.4 Защита машинных носителей персональных данных

Подсистема защиты машинных носителей ПДн должна исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей ПДн. Она предназначена для реализации следующих функций:

- учет машинных носителей ПДн;
- управление доступом к машинным носителям ПДн;
- контроль перемещения машинных носителей ПДн за пределы контролируемой зоны;
- исключение возможности несанкционированного ознакомления с содержанием ПДн, хранящихся на машинных носителях, и (или) использования носителей ПДн в иных ИС;
- контроль использования интерфейсов ввода (вывода) информации на машинные носители ПДн;
- контроль ввода (вывода) информации на машинные носители ПДн;
- контроль подключения машинных носителей ПДн;
- уничтожение (стирание) или обезличивание ПДн на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

4.5 Регистрация событий безопасности

Подсистема регистрация событий безопасности должна обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в ИС, а также возможность просмотра и анализа информации о таких событиях и реагирование на них. Она предназначена для реализации следующих функций:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;

- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- 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 памяти;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- генерирование временных меток и (или) синхронизация системного времени в ИС;
- защита информации о событиях безопасности.

4.6 Подсистема антивирусной защиты

Подсистема антивирусной защиты должна обеспечивать обнаружение в ИС 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. Она предназначена для реализации следующих функций:

- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов).

4.7 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений должна обеспечивать обнаружение действий в ИС, направленных на несанкционированный доступ к информации, специальные воздействия на ИС и (или) ПДн в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия. Она предназначена для реализации следующих функций:

- обнаружение вторжений;
- обновление базы решающих правил.

4.8 Контроль (анализ) защищенности персональных данных

Подсистема анализа защищенности (САЗ) ПДн должна обеспечивать контроль уровня защищенности ПДн, обрабатываемых в ИС, путем проведения систематических мероприятий по анализу защищенности ИС и тестированию работоспособности системы защиты ПДн. Она предназначена для реализации следующих функций:

- выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- контроль состава технических средств, программного обеспечения и средств защиты информации;
- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС.

4.9 Обеспечение целостности ИС и персональных данных

Подсистема обеспечения целостности ИС и ПДн должна обеспечивать обнаружение фактов несанкционированного нарушения целостности ИС и содержащихся в ней ПДн, а также возможность восстановления ИС и содержащихся в ней ПДн. Она предназначена для реализации следующих функций:

- контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
- контроль целостности ПДн, содержащихся в базах, данных ИС;

- обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;
- обнаружение и реагирование на поступление в ИС незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама);
- контроль содержания информации, передаваемой из ИС (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 ИС;
- ограничение прав пользователей по вводу информации в ИС;
- контроль точности, полноты и правильности данных, вводимых в ИС;
- контроль ошибочных действий пользователей по вводу и (или) передаче ПДн и предупреждение пользователей об ошибочных действиях.

4.10 Обеспечение доступности персональных данных

Подсистема обеспечения доступности персональных данных должна обеспечивать авторизованный доступ пользователей, имеющих права по доступу к ПДн, содержащимся в ИС, в штатном режиме функционирования ИС. Она предназначена для реализации следующих функций:

- использование отказоустойчивых технических средств;
- резервирование ТС, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИС;
- контроль безотказного функционирования ТС, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;

- обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного интервала.

4.11 Защита среды виртуализации

Подсистема защиты среды виртуализации должна исключать НСД к ПДн, 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. Она предназначена для реализации следующих функций:

- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- регистрация событий безопасности в виртуальной инфраструктуре;
- управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;
- доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией;
- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- контроль целостности виртуальной инфраструктуры и ее конфигураций;

- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- реализация и управление антивирусной защитой в виртуальной инфраструктуре;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей.

4.12 Защита технических средств

Подсистема защиты технических средств должна исключать НСД к стационарным ТС, обрабатывающим ПДн, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту ТС от внешних воздействий, а также защиту ПДн, представленных в виде информативных электрических сигналов и физических полей. Она предназначена для реализации следующих функций:

- защита информации, обрабатываемой ТС, от ее утечки по техническим каналам (ПЭМИН);
- организация КЗ, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- контроль и управление физическим доступом к ТС, 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;
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

- защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

4.13 Защита информационной системы, ее средств, систем связи и передачи данных

Подсистема защиты ИС, ее средств, систем связи и передачи данных должна обеспечивать защиту ПДн при взаимодействии ИС или ее отдельных сегментов с иными ИС и информационно-телекоммуникационными сетями посредством применения архитектуры ИС и проектных решений, направленных на обеспечение безопасности ПДн. Она предназначена для реализации следующих функций:

- разделение в ИС функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС;
- предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом;
- обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи;
- обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации);
- запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;
- передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с ПДн, при обмене ими с иными ИС;
- 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;

- 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;
- 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;
- подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
- исключение возможности отрицания пользователем факта отправки ПДн другому пользователю;
- исключение возможности отрицания пользователем факта получения ПДн от другого пользователя;
- использование устройств терминального доступа для обработки ПДн;
- защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки ПДн;
- выявление, анализ и блокирование в ИС скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов;
- разбиение ИС на сегменты (сегментирование ИС) и обеспечение защиты периметров сегментов ИС;

- обеспечение загрузки и исполнения программного обеспечения с машинных носителей ПДн, доступных только для чтения, и контроль целостности данного ПО;
- изоляция процессов (выполнение программ) в выделенной области памяти;
- защита беспроводных соединений, применяемых в ИС.

4.14 Выявление инцидентов и реагирование на них

Подсистема по выявлению инцидентов и реагированию на них должна обеспечивать обнаружение, идентификацию, анализ инцидентов в ИС, а также принятие мер по устранению и предупреждению инцидентов. Она предназначена для реализации следующих функций:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификация и регистрация инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- принятие мер по устранению последствий инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

4.15 Управление конфигурацией информационной системы и системы защиты персональных данных

Подсистема по управлению конфигурацией ИС и системы защиты ПДн должна обеспечивать управление изменениями конфигурации ИС и системы защиты ПДн, анализ потенциального воздействия планируемых изменений на обеспечение безопасности ПДн, а также документирование этих изменений. Она предназначена для реализации следующих функций:

- определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и системы защиты ПДн;
- управление изменениями конфигурации ИС и системы защиты ПДн;
- анализ потенциального воздействия планируемых изменений в конфигурации ИС и системы защиты ПДн на обеспечение защиты ПДн и согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности ПДн;
- документирование информации (данных) об изменениях в конфигурации ИС и системы защиты ПДн.

5 Пользователи ИС

В ИС можно выделить основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИС, определен их уровень доступа и возможности.

В ИС можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор ИС (системный);
- Администратор безопасности ИС;
- Оператор (пользователь) АРМ;
- Администратор сети;
- Технического специалиста по обслуживанию периферийного оборудования;
- Программист-разработчик ИС.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в *Положение о разграничении прав доступа к обрабатываемым персональным данным ИС*.

5.1 Администратор ИС

Администратор ИС, сотрудник предприятия, ответственный за настройку, внедрение и сопровождение ИС. Обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИС обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;

- обладает правами конфигурирования и административной настройки технических средств ИС.

5.2 Администратор безопасности

Администратор безопасности, сотрудник предприятия, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИС;
- обладает полной информацией об ИС;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИС;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов (МЭ) и систем обнаружения вторжений (СОВ), в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИС;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

5.3 Оператор АРМ

Оператор АРМ, сотрудник предприятия, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИС, формирование справок и отчетов по информации, полученной из ИС. Оператор не имеет полномочий для управления подсистемами обработки данных и системы защиты ПДн.

Оператор ИС обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

5.4 Администратор сети

Администратор сети, сотрудник предприятия, ответственный за функционирование телекоммуникационной подсистемы ИС. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИС;
- обладает частью информации о технических средствах и конфигурации ИС;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

5.5 Технический специалист по периферийному оборудованию

Технический специалист по обслуживанию, сотрудник предприятия, осуществляет обслуживание и настройку периферийного оборудования ИС. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИС;
- обладает частью информации о технических средствах и конфигурации ИС;

- знает, по меньшей мере, одно легальное имя доступа.

5.6 Программист-разработчик ИС

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники предприятия, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИС;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИС на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты ПДн, обрабатываемых в ИС.

6 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники предприятия, являющиеся пользователями ИС, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИС.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИС и средствами защиты ПДн.

Сотрудники предприятия, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники предприятия должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники предприятия должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами предприятия, третьим лицам.

При работе с ПДн в ИС сотрудники предприятия обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИС сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники предприятия должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИС, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и администратору информационной безопасности для принятия мер по устранению угрозы безопасности ПДн.

7 Должностные обязанности пользователей ИС

Должностные обязанности пользователей ИС описаны в следующих документах:

- Инструкция администратора ИС;
- Инструкция администратора безопасности ИС;
- Инструкция пользователя ИС.

8 Ответственность

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством РФ ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование информации и неправомерный доступ к охраняемой законом компьютерной информации (статьи 272 и 274 УК РФ).

Администратор ИС и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками предприятия – пользователей ИС правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Руководители и сотрудники предприятия несут ответственность за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

9 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика являются:

1 Федеральный Закон от 27.07.2006 г. № 152 «О персональных данных», устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн (с учетом новых редакций ФЗ).

2 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утв. Постановлением Правительства РФ от 01.11.2012 г. № 1119.

3 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18.02.2013 № 21.

4 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. приказом ФСТЭК России 15.02.08 г.

5 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. приказом ФСТЭК России 15.02.08 г.

6 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

7 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

10 Содержание мер по обеспечению безопасности ПДн

Условное обозначение	Содержание мер по обеспечению безопасности ПДн	Уровни защищенности ПДн			
		4	3	2	1
Подсистема 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)	+	+	+	+
Подсистема 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			+	+

Подсистема 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				
Подсистема 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		+	+	+

Подсистема 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	+	+	+	+
Подсистема VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
Подсистема VII. Обнаружение вторжений (СОВ)					
СОВ.l	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
Подсистема 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.3	Контроль работоспособности, параметров настройки и правильности функцио-		+	+	+

	нирования 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			+	+
Подсистема 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				
Подсистема 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			+	+
Подсистема 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		+	+	+
Подсистема 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)				
Подсистема 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 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.3	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, пользова-				

	телем 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		+	+	+
Подсистема XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
Подсистема 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		+	+	+