

Приложение № 1  
к приказу Аппарата Губернатора и  
Правительства Камчатского края  
от 30.12.2011 № 797-п

**Политика информационной безопасности  
в информационных системах персональных данных  
Аппарата Губернатора и Правительства Камчатского края «Кадры»  
и «Бухгалтерия»**

## ОПРЕДЕЛЕНИЯ

В настоящем документе в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из сотрудников Аппарата Губернатора и Правительства Камчатского края 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, характеризующееся 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, на основании которых можно установить его личность.

**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, транс-

портные 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 (ИСПДн)** – 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.

**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** – 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.

**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.

**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 субъектом персональных данных (персональные данные, сделанные общедоступными субъектом персональных данных).

**Оператор (персональных данных)** – Аппарат Губернатора и Правительства Камчатского края.

**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.

**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.

**Пользователь информационной системы персональных данных** – сотрудник Apparата Губернатора и Правительства Камчатского края, участвующий в функционировании информационной системы персональных данных или использующий результаты ее функционирования.

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

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

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

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, 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.

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

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

**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 невозможно восстановить содержание персональных данных в информационной системе персональных данных 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.

**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**

АВС – антивирусные средства  
АРМ – автоматизированное рабочее место  
ВТСС – вспомогательные технические средства и системы  
ИСПДн – информационная система персональных данных  
КЗ – контролируемая зона  
ЛВС – локальная вычислительная сеть  
МЭ – межсетевой экран  
НСД – несанкционированный доступ  
ОС – операционная система  
ПДн – персональные данные  
ПМВ – программно-математическое воздействие  
ПО – программное обеспечение  
ПЭМИН – побочные электромагнитные излучения и наводки  
САЗ – система анализа защищенности  
СЗИ – средства защиты информации  
СЗПДн – система (подсистема) защиты персональных данных  
СОВ – система обнаружения вторжений  
ТКУИ – технические каналы утечки информации  
УБПДн – угрозы безопасности персональных данных

## ВВЕДЕНИЕ

Настоящая Политика информационной безопасности Apparата Губернатора и Правительства Камчатского края (далее – Политика) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» определяет политику оператора в отношении обработки персональных данных, правовых актов Apparата Губернатора и Правительства Камчатского края (далее - Appарат) по вопросам обработки персональных данных, а также правовых актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности ИСПДн Apparата, утвержденной приказом Appарата.

Правовой основой Политики являются:

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

2) постановление Правительства Российской Федерации от 11.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

3) «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом директора ФСТЭК России от 05.02.2010 № 58;

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», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-662.

В Политике определены требования и степень ответственности пользователей ИСПДн Apparата «Кадры» и «Бухгалтерия» (далее – ИСПДн Apparата), структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников Apparата, ответственных за обеспечение безопасности персональных.

## **1. Общие положения**

1.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Apparata от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее – УБПДн).

1.2. Безопасность персональных данных в Apparate 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.

1.3. К информации и связанным с ней ресурсам представляется доступ для сотрудников Apparata, уполномоченных на обработку ПДн в ИСПДн Apparata. Ответственными за обеспечение безопасности ПДн в Apparate, являются сотрудники Apparata, которыми осуществляется своевременное обнаружение и реагирование на УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.4. Состав объектов защиты в Apparate определен Перечнем персональных данных, подлежащих защите в ИСПДе Apparata «Бухгалтерия и Перечнем персональных данных, подлежащих защите в ИСПДн Apparata «Кадры».

## **2. Область действия**

Требования настоящей Политики распространяются на всех сотрудников Apparata (штатных, оказывающих услуги по договору и т.п.), а также всех иных лиц (подрядчики, аудиторы и т.п.).

## **3. Система защиты персональных данных**

3.1. СЗПДн Apparata, основана на:

- 1) техническом задании по созданию СЗПДн;
- 2) перечне персональных данных, подлежащих защите;
- 3) классификации информационных систем персональных данных в соответствующих актах;
- 4) модели угроз безопасности персональных данных;
- 5) положении о разграничении прав доступа к обрабатываемым персональным данным;
- 6) руководящих документов ФСТЭК и ФСБ России.

На основании указанных документов определяется необходимый уровень защищенности каждой из ИСПДн Apparata. На основании анализа актуальных угроз безопасности ПДн, описанных в Модели угроз безопасности ИСПДн Apparata, составляется заключение о необходимости использования технических

средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в технических заданиях на создание системы защиты информации в ИСПДн Apparata.

3.2. Для ИСПДн Apparata составляется список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн Apparata:

- 1) АРМ пользователей;
- 2) сервера приложений;
- 3) СУБД;
- 4) границы ЛВС;
- 5) каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

3.3. В зависимости от уровня защищенности ИСПДн Apparata и актуальных угроз, СЗПДн может включать следующие технические средства:

- 1) АВС для АРМ пользователей и серверов;
- 2) средства межсетевого экранирования;
- 3) средства защиты от НСД;
- 4) средства защиты каналов связи;
- 5) средства анализа защищенности;
- 6) средства криптографической защиты информации.

Так же в список включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций средств защиты включает в себя:

- 1) управление и разграничение доступа пользователей;
- 2) регистрация и учет действий с информацией;
- 3) обеспечение целостности данных;
- 4) обнаружение вторжений.

#### **4. Требования к подсистемам СЗПДн**

4.1. СЗПДн Apparata включает в себя следующие подсистемы:

- 1) управления доступом, регистрации и учета;
- 2) обеспечения целостности и доступности;
- 3) антивирусной защиты;
- 4) межсетевого экранирования;
- 5) анализа защищенности;
- 6) обнаружения вторжений;
- 7) криптографической защиты.

Подсистемы СЗПДн имеют различные функциональные возможности в зависимости от класса ИСПДн Apparata, определенного в актах классификации ИСПДн Apparata.

4.1.1. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

1) идентификация и проверка подлинности субъектов доступа при входе в ИСПДн Apparata;

2) идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

3) идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

4) регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;

5) регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

6) регистрация попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

4.1.2. Подсистема управления доступом реализуется с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть использовано 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.

4.1.3. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств в ИСПДн Apparata, а так же средств защиты, при случайной или намеренной модификации. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, и резервированием ключевых элементов ИСПДн Apparata.

4.1.4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Apparata.

Средства антивирусной защиты предназначены для реализации следующих функций:

1) резидентный антивирусный мониторинг;

2) антивирусное сканирование;

3) скрипт-блокирование;

4) централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта;

5) автоматизированное обновление антивирусных баз;

6) ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

7) автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн Apparata.

4.1.5. Подсистема межсетевое экранирования предназначена для реализации следующих функций:

- 1) фильтрация открытого и зашифрованного (закрытого) IP-трафика по заданным параметрам;
- 2) фиксация во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- 3) идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ;
- 4) регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- 5) контроль целостности своей программной и информационной части;
- 6) фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- 7) фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- 8) регистрация и учет запрашиваемых сервисов прикладного уровня;
- 9) блокирование доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- 10) контроль за сетевой активностью приложений и обнаружение сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

4.1.6. Подсистема анализа защищенности, направлена на выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн Аппарата, которые могут быть использованы нарушителем для реализации атаки на систему. Функциональные возможности подсистемы реализуются программными и программно-аппаратными средствами.

4.1.7. Подсистема обнаружения вторжений, направлена на выявление сетевых атак на элементы ИСПДн Аппарата, подключенные к сетям общего пользования и (или) международного обмена. Функциональные возможности подсистемы реализуются программными и программно-аппаратными средствами.

4.1.8. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Аппарата, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена. Подсистема реализуется путем внедрения криптографических программно-аппаратных комплексов.

## 5. Пользователи ИСПДн Apparata

5.1. Основные группы пользователей в Apparate определены в Концепции информационной безопасности. В каждой ИСПДн Apparata выделены следующие группы пользователей, участвующих в обработке и хранении ПДн:

- 1) администраторы безопасности ИСПДн;
- 2) операторы ИСПДн;
- 3) программисты-разработчики ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным Apparata.

5.2. Администраторами безопасности ИСПДн в Apparate являются уполномоченные сотрудники Apparata, Министерства специальных программ и по делам казачества Камчатского края, Агентства по информатизации и связи Камчатского края, ответственные за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

5.2.1. Администраторы безопасности:

- 1) обладают правами администратора ИСПДн Apparata;
- 2) обладают полной информацией об ИСПДн Apparata;
- 3) имеют доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн Apparata;
- 4) имеют права доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

5.2.2. Администраторы безопасности уполномочены:

- 1) реализовывать политику информационной безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн Apparata;
- 2) осуществлять аудит средств защиты;
- 3) устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

5.3. Операторами ИСПДн являются сотрудники Apparata, осуществляющие обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн Apparata, формирование справок и отчетов по информации, полученной из ИСПДн Apparata. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

5.3.1. Операторы ИСПДн:

- 1) обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн;
- 2) располагают конфиденциальными данными, к которым имеет доступ.

5.4. Программисты-разработчики ИСПДн Apparata (поставщики) прикладного программного обеспечения, обеспечивают его сопровождение на защищаемом объекте. К данной группе относятся сотрудники Агентства по информатизации и связи Камчатского края или привлекаемых в соответствии с законодательством Российской Федерации для разработки программного обеспечения.

5.4.1. Программисты-разработчики:

1) обладают информацией об алгоритмах и программах обработки информации на ИСПДн Apparata;

2) обладают возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн Apparata на стадии ее разработки, внедрения и сопровождения;

3) располагают любыми фрагментами информации о топологии ИСПДн Apparata и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн Apparata.

## **6. Требования к пользователям по обеспечению защиты ПДн**

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

6.2. Должностное лицо, ответственное за организацию и планирование мероприятий по защите информации в Apparate, при оформлении на должность сотрудника обязан организовать его ознакомление с необходимыми документами, регламентирующими требования по защите и обработке ПДн в Apparate, а также обучение его навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн Apparata.

6.3. Сотрудник Apparata знакомится с настоящей Политикой, принятыми процедурами работы с элементами ИСПДн Apparata и СЗПДн.

6.4. Пользователи ИСПДн Apparata обязаны:

1) обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов;

2) следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации);

3) обеспечивать надлежащую защиту оборудования и АРМ, 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 и АРМ, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты;

4) обеспечивать отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов, при работе с ПДн в ИСПДн Apparata;

5) защищать АРМ или терминалы с помощью блокировки ключом или эквивалентным средством контроля, например, доступом по паролю, если не используются иные дополнительные средства защиты, при завершении работы в ИСПДн Apparata.

6.5. Пользователям ИСПДн Apparata запрещается:

1) устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию;

2) разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Apparata, третьим лицам.

6.6. Пользователи ИСПДн Apparata информируются администратором безопасности об угрозах нарушения режима безопасности ПДн и ответственности за его нарушения.

6.7. Пользователи ИСПДн Apparata обязаны без промедления сообщать администратору безопасности или своему непосредственному руководителю обо всех наблюдаемых или подозрительных случаях работы ИСПДн, способных повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн.

## **7. Должностные обязанности пользователей ИСПДн Apparata**

7.1. Должностные обязанности пользователей ИСПДн определены в следующих документах:

1) должностном регламенте государственного гражданского служащего Apparata;

2) инструкции пользователя информационной системы персональных данных в Apparate;

3) инструкции пользователя по обеспечению безопасности при возникновении внештатных ситуаций в Apparate.

## **8. Ответственность пользователей Apparata**

8.1. В соответствии со статьей 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований указанного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

За нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей предусмотрена ответственность в соответствии со статьями 272,273 и 274 УК РФ.

8.2. Администратор безопасности Apparata несет ответственность за все действия, совершенные от имени их учетных записей или системных учет-

ных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях пользователями ИСПДн Apparata правил, связанных с безопасностью ПДн, они несут ответственность, в соответствии с законодательством Российской Федерации.

8.3. Приведенные в настоящем разделе требования нормативных документов по защите информации отражаются в Положениях о структурных подразделениях Apparata, осуществляющих обработку ПДн в ИСПДн Apparata и должностных регламентах государственных гражданских служащих Apparata.

Положениями о структурных подразделениях Apparata, осуществляющих обработку ПДн в ИСПДн Apparata предусматриваются положения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.