

Приложение  
к приказу КГАУЗ Краевой  
Центр СПИД  
от 14.04. 2021 № 45-орг

Политика информационной безопасности  
информационных систем персональных данных  
КГАУЗ Краевой Центр СПИД

## **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** – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

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

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

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

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

**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 (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 характеристиках 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, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Организация** – КГАУЗ Краевой Центр СПИД[к1].

**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.

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

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

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

**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.

**Программная закладка** – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие (утечка, изменение, блокирование, уничтожение информации или уничтожение и модификация программного обеспечения информационной системы персональных данных и (или) блокирование аппаратных средств). Программная закладка может быть реализована в виде вредоносной программы или программного кода.

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

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

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-

телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

**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 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 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** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

## **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  
ТКУ И – технические каналы утечки информации  
УБПДн – угрозы безопасности персональных данных

## **ВВЕДЕНИЕ**

Настоящая Политика информационной безопасности (далее – Политика) КГАУЗ Краевой Центр СПИД (далее – Организация) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности ИСПД Организации.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

### **Общие положения**

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

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 УБПДн.

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

Состав объектов защиты представлен в Перечне сведений конфиденциального характера Организации.

Состав ИСПДн подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки.

### **1. Область действия**

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

### **2. Система защиты персональных данных**

На основании документов, разработанных в Организации определяется необходимый уровень защищенности ПДн каждой ИСПДн Организации. На основании анализа актуальных угроз безопасности ПДн принимается решение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые

мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

### **3. Требования к подсистемам СЗПДн**

СЗПДн включает в себя следующие подсистемы:  
управления доступом, регистрации и учета;  
обеспечения резервного копирования;  
антивирусной защиты;  
межсетевого экранирования;  
криптографической защиты каналов передачи информации.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

#### **Подсистемы управления доступом, регистрации и учета**

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

идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

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

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

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

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД).

#### **Подсистема обеспечения целостности и доступности**

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Организации, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных.

#### **Подсистема антивирусной защиты**

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

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;  
антивирусное сканирование;  
скрипт-блокирование;  
автоматизированное обновление антивирусных баз;  
ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

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

#### **Подсистема межсетевого экранирования**

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

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

#### **Подсистема криптографической защиты каналов передачи информации.**

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Организации, при ее передаче по каналам связи сетей общего пользования.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

### **4. Пользователи ИСПДн**

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

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

Администратора безопасности ИСПДн;

Оператора АРМ;

Технического специалиста по обслуживанию периферийного оборудования;

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

### **Администратор безопасности ИСПДн**

Администратор безопасности ИСПДн (далее – Администратор), сотрудник Организации, ответственный за настройку, внедрение и сопровождение ИСПДн, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент, ответственный за функционирование телекоммуникационной подсистемы ИСПДн.

Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Уполномочен реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн, осуществляет аудит средств защиты, устанавливает доверительные отношения своей защищенной сети с сетями других Организаций.

Администратор обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

### **Оператор АРМ (пользователь ИСПДн)**

Оператор АРМ, сотрудник Организации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн, корректировку ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн 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.

## **Техник программист, специалист по обслуживанию периферийного оборудования**

Техник программист, специалист по обслуживанию периферийного оборудования (далее Техник программист), сотрудник Организации, осуществляет обслуживание и настройку периферийного оборудования ИСПДн, обеспечивает его сопровождение на защищаемом объекте. Техник программист имеет доступ к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Техник программист обладает следующим уровнем доступа и знаний:  
обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн;

знает, по меньшей мере, одно легальное имя доступа.

### **Инженер программист**

Программисты прикладного программного обеспечения, обеспечивающие его сопровождение, внесение корректировок в ИСПДн на защищаемом объекте. К данной группе могут относиться как сотрудники Организации, так и сотрудники сторонних организаций.

Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

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

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

## **5. Требования к персоналу по обеспечению защиты ПДн**

Все сотрудники Организации, являющиеся пользователями ИСПДн, 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 ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электрон-

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

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

Сотрудники Организации должны обеспечивать надлежащую защиту оборудования, оставленного 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 так же записывать на них защищаемую информацию.

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

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

При завершении работы с ИСПДн 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 Организации 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 ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

## **6. Должностные обязанности пользователей ИСПДн**

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн

## **7. Ответственность сотрудников пользователей ИСПДн Организации**

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 гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает 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 (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн 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 Организации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Организации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Организации.

Необходимо внести в Положения о подразделениях Организации, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

Начальник отдела информационного  
программного обеспечения

Т.А. Косяченко