**МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОСТОВСКОЙ ОБЛАСТИ**

**УТВЕРЖДАЮ**

И.о. министра здравоохранения

Ростовской области

С.Г. Беседовский

«25» декабря 2015 г.

# ПОЛИТИКА

## информационной безопасности информационных систем персональных данных министерства здравоохранения Ростовской области

г. Ростов-на-Дону
2015 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, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

**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 (ИСПДн)** - 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.

**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 докумен-

тации, 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** 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.

**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.

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

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

**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 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 не-

санкционированных 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.

**МЗ РО** - Министерство здравоохранения Ростовской области.

**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 |
| **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 |
| **ТЗКИ** | техническая защита конфиденциальной информации |
| **Ответственный по ТЗКИ** | ответственный за защиту информации на объекте информатизации (сотрудник подразделения назначенный приказом министра здравоохранения Ростовской области) |
| **ТКУ И** | технические каналы утечки информации |
| **УБПДн** | угрозы безопасности |

# I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности информационных систем персональных данных министерства здравоохранения Ростовской области (далее - Политика) разработана в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иных нормативных правовых актов, руководящих и методических документов по информационной безопасности.

Настоящая Политика определяет основные цели и задачи построения системы защиты персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также для минимизации ущерба от возможной реализации угроз безопасности ПДн (далее - УБПДн);

2. Действие Политики распространяется на всех должностных лиц, эксплуатирующих технические и программные средства ИСПДн.

3. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

В ИСПДн обеспечивается доступность авторизованных пользователей к ПДн и связанным с ними ресурсам, осуществляется своевременное обнаружение и реагирование на УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

# II. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. На основании результатов обследования условий обработки ПДн в министерстве, имеющихся ИСПДн, категорий обрабатываемых ПДн, используя руководящие документы ФСТЭК и ФСБ России определяется необходимый уровень защищенности ПДн для каждой ИСПДн министерства.

На основании анализа актуальных угроз безопасности ПДн, описанных в Модели угроз безопасности ПДн при их обработке в ИСПДн и по результатам проверки условий обработки ПДн, делается заключение о необходимости использования технических средств и применения организационных мероприятий для обеспечения безопасности ПДн.

2. Для каждой ИСПДн составляется список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн в ИСПДн.

В список используемых технических средств защиты информации также включаются средства защиты.

Список функций защиты включает:

управление и разграничение доступа пользователей;

регистрацию и учет действий с информацией;

обеспечение целостности данных;

обнаружение вторжений.

3. В зависимости от уровня защищенности ПДн и актуальности угроз, СЗПДн может включать следующие технические средства:

антивирусные средства для рабочих станций пользователей и серверов;

средства межсетевого экранирования;

средства криптографической защиты информации при передаче защищаемой информации по каналам связи;

средства защиты от НСД;

средства обнаружения вторжений;

средства анализа защищенности.

4. Список используемых технических средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн соответствующие изменения вносятся в эксплуатационно-техническую документацию.

Ответственность за поддержание в актуальном состоянии используемых технических средств защиты информации в ИСПДн возлагается на ответственного по ТЗКИ.

# III. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СЗПДн включает в себя следующие подсистемы:
управления доступом, регистрации и учета;
обеспечения целостности и доступности;
антивирусной защиты;
межсетевого экранирования;
анализа защищенности;
обнаружения вторжений;
криптографической защиты.

Подсистемы СЗПДн имеют различные функциональные возможности в зависимости от класса ИСПДн и установленного уровня защищенности ПДн, определенных в Акте классификации ИСПДн и установления уровня защищенности ПДн.

Список соответствия функций подсистем СЗПДн классу защищенности указан в приложении к настоящей Политике.

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

- идентификация и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрация попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом реализуется с использованием технических средств или их комплексов, обеспечивающих меры по аутентификации и контролю.

3. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности защищаемой информации при случайной или намеренной их модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием необходимых элементов ИСПДн.

4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и автоматизированных рабочих мест пользователей ИСПДн.

Средства антивирусной защиты выполняют следующие функции:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованная установка (деинсталляция) антивирусного программного обеспечения, настройка, администрирование, просмотр отчетов и статистической информации по работе средств антивирусной защиты;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменение настроек антивирусного программного обеспечения;
- автоматический запуск средств антивирусной защиты после загрузки операционной системы.

Подсистема реализуется путем внедрения антивирусного программного обеспечения в ИСПДн.

5. Подсистема межсетевого экранирования выполняет следующие функции:

фильтрация открытого и зашифрованного (закрытого) IP-трафика по заданным параметрам;

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

идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ;

регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузка и инициализация системы и ее программного останова;

контроль целостности своей программной и информационной части;

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

фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

регистрация и учет запрашиваемых сервисов прикладного уровня;

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

контроль сетевой активности приложений и обнаружение сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальных вычислительных сетей.

6. Подсистема анализа защищенности предназначена для выявления уязвимостей, связанных с ошибками в конфигурации программного

обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функциональные возможности подсистемы реализуется программными и программно-аппаратными средствами.

7. Подсистема обнаружения вторжений обеспечивает выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

Функциональные возможности подсистемы реализуются программными и программно-аппаратными средствами.

8. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения в ИСПДн криптографических программно-аппаратных комплексов.

# IV. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. В Политике определены основные категории пользователей ИСПДн:

- администратор;
- оператор.

На основании этих категорий устанавливаются группы пользователей ИСПДн и определяется их уровень доступа и полномочий.

2. Группы пользователей ИСПДн.

В ИСПДн министерства выделяются следующие группы пользователей, участвующих в обработке ПДн:

администратор ИСПДн;

администратор безопасности;

оператор автоматизированного рабочего места (далее – АРМ).

2. Администратор ИСПДн – государственный гражданский служащий (служащий) министерства, сотрудник другой организации, ответственный за настройку, внедрение и сопровождение ИСПДн. Администратор ИСПДн обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим ПДн.

Администратор ИСПДн 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.

3. Администратор безопасности - государственный гражданский служащий (служащий) министерства, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской части программ.

Администратор безопасности обладает следующим уровнем доступа и знаний:

обладает правами Администратора ИСПДн;

обладает полной информацией об ИСПДн;

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

не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

реализовывать политики безопасности в части настройки системы криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;

осуществлять настройки системы разграничения доступа к ПДн;

осуществлять аудит средств защиты;

устанавливать доверительные отношения своей защищенной сети с сетями других организаций, системой межведомственного электронного взаимодействия, взаимодействующими информационными системами.

4. Оператор АРМ - государственный гражданский служащий (служащий) министерства, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, вводи и редактирования ПДн в ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий на управление 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.

5. Администратор сети - государственный гражданский служащий (служащий) министерства, сотрудник другой организации, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий на управление подсистемами обработки данных и безопасности.

Администратор сети 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;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

6. Технический специалист по обслуживанию - сотрудник другой организации, который осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий на управление подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию 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.

7. Программист- р азработчик (поставщик) прикладного программного обеспечения – сотрудник другой организации, обеспечивающий сопровождение прикладного программного обеспечения на защищаемом объекте.

Программист-разработчик (поставщик) прикладного программного обеспечения:

- 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.

8. На основании результатов проведения ежегодной проверки условий обработки ПДн администратором безопасности ИСПДн определяются и настраиваются права доступа к элементам ИСПДн для всех групп пользователей (настройка системы разграничения доступа к ПДн).

# V. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Все государственные гражданские служащие (служащие) министерства, являющиеся пользователями ИСПДн, должны знать и выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении нового государственного гражданского служащего (служащего) министерства в должность начальник структурного подразделения обязан организовать его ознакомление с документами, регламентирующими требования по защите ПДн, а ответственный по ТЗКИ обязан провести инструктаж по выполнению процедур, необходимых для санкционированного использования ИСПДн.

2. Государственные гражданские служащие (служащие) министерства, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможности их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

3. Государственные гражданские служащие (служащие) министерства должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

4. Государственные гражданские служащие (служащие) министерства должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать порядок доступа служащих министерства в помещения, в которых ведётся обработка ПДн.

5. Государственным гражданским служащим (служащим) министерства запрещается:

- устанавливать постороннее программное обеспечение;
- подключать личные мобильные устройства и носители информации для записи на них защищаемой информации;
- хранить защищаемую информацию и ПДн на внешних ресурсах, идентифицировать физическое размещение которых не представляется возможным.

6. Установка, удаление, обновление программного обеспечения в министерстве осуществляется только государственными гражданскими служащими (служащими) министерства или сотрудниками сторонних организаций, с которыми заключено Соглашение (договор) о конфиденциальности, либо Соглашение (договор) о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн.

7. При работе с ПДн в ИСПДн, государственные гражданские служащие (служащие) министерства обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест или терминалов.

При завершении работы с ИСПДн государственные гражданские служащие (служащие) министерства обязаны произвести выход из системы.

8. Государственные гражданские служащие (служащие) министерства обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, ответственному по ТЗКИ.

# VI. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ

1. В соответствии с Федеральным законом от 27.07.2006 № 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.

Приложение
к Политике информационной безопасности информационных систем персональных данных Министерства здравоохранения Ростовской области

# СПИСОК СООТВЕТСТВИЯ
## Мер защиты ПДн установленным уровням защищенности информационной системы персональных данных

| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Уровни защищенности персональных данных | | | |
|---|---|---|---|---|---|
| | | 4 | 3 | 2 | 1 |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | | | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных | | | | |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему | | | | |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы | | | | |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | | + | + | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | | + | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки | | | | |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | | | + | + |
| | III. Ограничение программной среды (ОПС) | | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения | | | | |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | | | + | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | | | | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов | | | | |
| | IV. Защита машинных носителей персональных данных (ЗНИ) | | | | |
| ЗНИ.1 | Учет машинных носителей персональных данных | | | + | + |
| ЗНИ. 2 | Управление доступом к машинным носителям персональных данных | | | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны | | | | |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах | | | | |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | | | | |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных | | | | |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных | | | | |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | | + | + | + |
| | V. Регистрация событий безопасности (РСБ) | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | | | | |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | | | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | | | | |
| РСБ. 7 | Защита информации о событиях безопасности | | + | + | + | + |
| VI. Антивирусная защита (АВЗ) | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | | + | + | + | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | | + | + | + | + |
| VII. Обнаружение вторжений (СОВ) | | | | | |
| СОВ.1 | Обнаружение вторжений | | | | + | + |
| СОВ.2 | Обновление базы решающих правил | | | | + | + |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | | | + | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | | + | + | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | | | + | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | | | + | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей | | | | + | + |

| | | | | | |
|---|---|---|---|---|---|
| | в информационной системе | | | | |
| IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ) | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | | | + | + |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы | | | | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | | | | |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | | | + | + |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы | | | | |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему | | | | |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему | | | | |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях | | | | |
| X. Обеспечение доступности персональных данных (ОДТ) | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств | | | | |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | | | | |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | | | | + |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | | | + | + |
| ОДТ. 5 | Обеспечение возможности восстановления персональных данных с резервных машинных но- | | | + | + |

| | | | | | |
|---|---|---|---|---|---|
| | сителей персональных данных (резервных копий) в течение установленного временного интервала | | | | |
| XI. Защита среды виртуализации (ЗСВ) | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | | + | + | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | | | | |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией | | | | |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | | | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | | | + | + |
| ЗСВ. 8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | | | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | | + | + | + |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | | + | + | + |
| XII. Защита технических средств (ЗТС) | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | | | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | | | | |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в | + | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| | которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | | | | |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | | | | |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (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, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | | | | |
| ЗИС. 5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | | | | |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами | | | | |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода | | | | |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи | | | | |

| | | | | | |
|---|---|---|---|---|---|
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации | | | | |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | | | | |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | | | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю | | | | |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя | | | | |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных | | | | |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | | | + | + |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов | | | | |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | | | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения | | | | |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти | | | | |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | | + | + | + |
| XIV. Выявление инцидентов и реагирование на них (ИНЦ) | | | | | |
| 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 | | | + | + |
| | XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | | | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | | + | + | + |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | | + | + | + |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | | + | + | + |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | | + | + | + |

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

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