**государственное бюджетное учреждение здравоохранения Ставропольского края**
**“Пятигорский межрайонный противотуберкулезный диспансер”**

# Положение
# по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных

**№ _____ «_____»_____2018г**

**<u>Ответственный за применение нормативного документа:</u>**

**государственное бюджетное учреждение здравоохранения Ставропольского края**
**“Пятигорский межрайонный противотуберкулезный диспансер”**

# СОДЕРЖАНИЕ

Оглавление

**ИНФОРМАЦИЯ О ДОКУМЕНТЕ** ..... 3

Настоящий документ определяет порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных государственного бюджетного учреждения здравоохранения Ставропольского края «Пятигорского межрайонного противотуберкулезного диспансера» (далее - Организация) и содержит общие принципы защиты персональных данных. ..... 3

Данный документ направлен на достижение следующих целей: ..... 3

Настоящий документ обязаны знать и использовать в работе следующие должностные лица: ..... 6

**ОБЩИЕ ПОЛОЖЕНИЯ** ..... 8

**ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПДН** ..... 8

**государственное бюджетное учреждение здравоохранения Ставропольского края**
**“Пятигорский межрайонный противотуберкулезный диспансер”**

## ИНФОРМАЦИЯ О ДОКУМЕНТЕ

**Назначение документа**
Настоящий документ определяет порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных государственного бюджетного учреждения здравоохранения Ставропольского края «Пятигорского межрайонного противотуберкулезного диспансера» (далее - Организация) и содержит общие принципы защиты персональных данных.

**Цели документа**
Данный документ направлен на достижение следующих целей:

- выполнение требований нормативных документов Российской Федерации, связанных с персональными данными;
- защита прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных Организации;
- защита персональных данных, обрабатываемых в Организации, от несанкционированного доступа и от других несанкционированных действий;
- снижение уровня регуляторных рисков в отношении Организации.

**Ответственность и область применения**
Настоящий документ обязаны знать и использовать в работе следующие должностные лица:

- администратор информационной безопасности ИСПДн;
- администратор ИСПДн.

**Вводимые определения терминов и сокращений**

**Таблица 1. Перечень сокращений**

| Сокращение | Расшифровка сокращения |
|---|---|
| **АРМ** | Автоматизированное рабочее место |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ИСПДн** | Информационная система персональных данных |
| **ЛВС** | Локальная вычислительная сеть |
| **ПДн** | Персональные данные |
| **СЗПДн** | Система защиты персональных данных |
| **СКС** | Структурированная кабельная система |
| **СОИБ** | Система обеспечения информационной безопасности |
| **СТЗ** | Специальное техническое задание |
| **ТЗ** | Техническое задание |

**Таблица 2. Перечень терминов**

| Наименование термина | Определение термина |
|---|---|
| **Безопасность информации [данных]** | Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность. |
| **Блокирование персональных данных** | Временное прекращение 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) воздействии 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 к информации** | Возможность получения информации и ее использования. |
| **Защита информации** | Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. |
| **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. |
| **Информационная система персональных данных** | Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств |
| **Информационные технологии** | Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. |
| **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. |
| **Контролируемая зона** | Пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств. |
| **Межсетевой экран** | Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы. |
| **Модель угроз (безопасности информации)** | Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. |
| **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 защищаемой 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. |

**государственное бюджетное учреждение здравоохранения Ставропольского края**
**“Пятигорский межрайонный противотуберкулезный диспансер”**

| Наименование термина | Определение термина |
|---|---|
| **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. |
| **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 |
| **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. |
| **Оператор** | Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. |
| **Ответственный за применение нормативного документа** | Должностное лицо, ответственное за внедрение и применение нормативного документа. Термин применим к нормативным документам, кроме регламента процесса, для регламента процесса используется термин «Владелец процесса». «Ответственный за применение НД» и «Ответственный за разработку НД» могут совпадать. |
| **Ответственный за разработку нормативного документа** | Должностное лицо или структурное подразделение, ответственное за создание и поддержание нормативного документа в актуальном состоянии. Ответственный за разработку НД отвечает за плановый пересмотр документа и за внесение внеочередных изменений в соответствии с данным положением. |
| **Структурное подразделение** | Официально выделенная в организационной структуре Организации группа работников, выполняющая определенные функции и задачи, предусмотренные Положением о структурном подразделении. |
| **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. |
| **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. |
| **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. |
| **Ресурс информационной системы** | Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы. |
| **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. |

| Наименование термина | Определение термина |
|---|---|
| **Технический канал утечки информации** | совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. |
| **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. |
| **Уполномоченное оператором лицо** | Лицо, которому на основании договора оператор поручает обработку персональных данных. |
| **Целостность информации** | Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения). |
| **Цель защиты информации** | Заранее намеченный результат защиты информации. |

## ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение устанавливает требования по защите персональных данных, принципы обработки персональных данных в информационных системах персональных данных, направленные на защиту интересов Организации в области его экономической деятельности, обеспечение непрерывности бизнес процессов Организации.

Требования Положения распространяются на все структурные подразделения Организации, в которых осуществляется автоматизированная и неавтоматизированная обработка персональных данных, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационных систем персональных данных.

Настоящее Положение разработано в соответствии со следующими нормативными актами:

- Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г № 687;
- постановление правительства РФ от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

Персональные данные являются сведениями, отнесенными к информации ограниченного доступа Организации.

Настоящее Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности персональных данных;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности ПДн;
- координации деятельности структурных подразделений Организации при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности персональных данных;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных в ИСПДн.

Принципы и требования по обеспечению безопасности персональных данных распространяются:

- на все возможные формы существования информации (физические поля (электрические, акустические, электромагнитные, оптические и т.п.), носители на бумажной, магнитной, оптической и иной основе);
- на все возможные форматы представления персональных данных (документы, голос, изображения, файлы, почтовые сообщения, базы данных, записи базы данных, другие информационные массивы).

Предотвращение несанкционированного и нелегитимного доступа к информационным системам, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации.

Настоящее Положение определяет:

- роли, полномочия, ответственность за обеспечение безопасности ПДн, подразделений Организации;
- порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- мероприятия по обеспечению безопасности ПДн;
- требования по управлению процессом обеспечения безопасности ПДн;
- требования к составу и содержанию документов Организации, регламентирующих защиту и работу с ПДн.

При работе с персональными данными, во всех случаях, не урегулированных нормативными документами Организации, необходимо руководствоваться действующим законодательством Российской Федерации.

**государственное бюджетное учреждение здравоохранения Ставропольского края “Пятигорский межрайонный противотуберкулезный диспансер”**

## ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПДН

Целью создания системы защиты ПДн является исключение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

- конфиденциальности ПДн;
- целостности ПДн;
- доступности ПДн;
- неотказуемости;
- учетности[1];
- аутентичности[2];

**Главный врач**
**ГБУЗ СК «ПМПТД»** **Л. В. Романенко**

---

[1] **Учетность**

– свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта (ИСО 7498–2:99);
– обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту.

[2] **Аутентичность**

– свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004);
– идентичность объекта тому, что заявлено.