

Бюджетное учреждение здравоохранения
Удмуртской Республики
**«Республиканская клиническая туберкулезная больница
Министерства здравоохранения Удмуртской Республики»**



ИНСТРУКЦИЯ
Пользователя ИСПДн
БУЗ УР «РКТБ МЗ УР»

Ижевск - 2019

Определения и принятые сокращения

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

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Пользователь ИСПДн (далее – Пользователь) – лицо, осуществляющее обработку персональных данных в информационной системе персональных данных.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированных средств, предназначенный для автоматизации деятельности определенного вида (ПК, ноутбук, терминал).

Общие положения

Настоящая Инструкция разработана для Пользователей Бюджетного учреждения здравоохранения Удмуртской Республики «Республиканская клиническая туберкулезная больница Министерства здравоохранения Удмуртской Республики» (далее – БУЗ УР «РКТБ МЗ УР») с целью обеспечения защиты персональных данных (далее – ПДн) при их обработке.

ПДн не подлежат разглашению (распространению), за исключением общедоступных и обезличенных ПДн.

Пользователем является каждый сотрудник БУЗ УР «РКТБ МЗ УР», в рамках своих должностных обязанностей участвующий в процессах обработки персональных данных, имеющий к ним доступ на законном основании и в соответствии с регламентирующими документами учреждения.

Обработка персональных данных Пользователем осуществляется с применением средств автоматизации и без применения средств автоматизации. Обработка ПДн без применения средств автоматизации включает в себя следующие разрешенные действия Пользователей: создание, добавление (накопление), изменение, чтение, передача сторонним организациям (в госорганы на законном основании и по договорам). Обработка ПДн с использованием средств автоматизации включает в себя следующие разрешенные действия Пользователей: создание, добавление (накопление), изменение, чтение, печать, поиск, формирование отчетов, передача сторонним организациям, администрирование.

Все операции с бумажными и материальными носителями ПДн (выдача, копирование, передача) должны учитываться в соответствующих журналах и карточках и контролироваться ответственным лицом за организацию и координацию работ по обеспечению защиты ПДн.

Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке и защите ПДн, руководящими и нормативными документами Роскомнадзора, ФСТЭК России, ФСБ России и иными регламентирующими документами.

Методическое руководство работой Пользователя осуществляется ответственным лицом за организацию и координацию работ по обеспечению защиты ПДн и Администратором безопасности ПДн.

2. Права Пользователя

2.1 Пользователь имеет право:

2.1.1 Обращаться для получения консультаций к технику автономных систем обработки информации и управления ПДн по вопросам работы и настройки АРМ;

2.1.2 Вносить предложения и замечания по совершенствованию системы защиты ПДн;

2.1.3 Обжаловать решения или действия Администратора безопасности ПДн и ответственного лица за обработку и обеспечение защиты ПДн у главного врача БУЗ УР «РКТБ МЗ УР».

3. Обязанности Пользователя

3.1 Пользователь обязан:

3.1.1 Хранить в тайне конфиденциальные сведения, составляющие ПДн, ставшие ему известными в ходе выполнения своих служебных обязанностей и пресекать действия других Пользователей и третьих лиц, которые могут привести к разглашению такой информации.

Вернуть в полном объеме, в случае оставления занимаемой должности, все бумажные, электронные и материальные носители ПДн, относящиеся к деятельности структурного подразделения, организации и третьих лиц, полученные им в течение всего срока исполнения своих служебных обязанностей. В том числе копии, черновики, переписку и иные материалы, содержащие конфиденциальные сведения.

3.1.2 Выполнять обработку ПДн согласно Перечню действий, утвержденному приказом главного врача БУЗ УР «РКТБ МЗ УР» о допуске и доступе, в соответствии с Матрицами доступа сотрудников к ИСПДн, как с применением средств автоматизации, так и без применения таковых.

3.1.3 Выполнять требования ответственного лица за обработку и обеспечение защиты ПДн и Администратора безопасности ПДн, касающиеся обработки и защиты ПДн.

3.1.4 Знать и строго выполнять требования по режиму обработки ПДн и требования действующих нормативных актов и руководящих документов, а также инструкций и иных документов, регламентирующих порядок действий по защите информации.

3.1.5 Соблюдать правила при работе в сетях общего доступа и (или) международного обмена (раздел 4).

3.1.6 Хранить в тайне свой идентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты ИСПДн.

3.1.7 Использовать в рамках исполнения своих служебных обязанностей, только учтенные съемные носители информации (дискеты, компакт-диски, flash-носители) и выполнять соответствующие требования к учету, хранению и порядку работы с данными носителям, установленные в БУЗ УР «РКТБ МЗ УР».

3.1.8 Разместить монитор персонального АРМ таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией лицами, не имеющими доступа к данным сведениям и третьими лицами.

3.1.9 Заблокировать, покидая рабочее место, доступ к АРМ. Для этого необходимо нажать сочетание клавиш Ctrl+Alt+Del и выбрать опцию «Блокировка компьютера».

3.1.10 Контролировать обновление антивирусных баз и других программных средств, отвечающих за обеспечение безопасности ПДн. В случае необходимости сообщать о необходимости обновления Администратору безопасности ПДн.

3.1.11 Информировать ответственное лицо за обработку и обеспечение защиты ПДн, Администратора безопасности ПДн БУЗ УР «РКТБ МЗ УР» о следующих событиях:

- факты утечки, а также другие причины, условия и предпосылки возможной утечки ПДн;
- потеря носителя с ПДн или подозрение компрометации идентификаторов доступа (личных ключей и паролей);
- нарушение целостности пломб корпусов АРМ или иных фактов совершения в отсутствие Пользователя попыток несанкционированного доступа к программно-аппаратным средствам обработки ПДн;
- несанкционированные (произведенные с нарушением установленного порядка) изменения в конфигурации программно-аппаратных средств.
- отклонения от нормальной работы программно-аппаратных средств, выходе из строя или неустойчивого функционирования узлов АРМ, некорректного функционирования установленных в ИСПДн технических средств защиты, а также перебоев в системе электроснабжения.

3.1.12 Сообщить ответственному лицу за обработку и обеспечение защиты ПДн или Администратору безопасности ПДн об обнаруженных уязвимостях и не декларированных возможностях программно-аппаратных средств обработки и защиты ПДн.

3.2 Пользователю запрещается:

- 3.2.1 Передавать другим сотрудникам и третьим лицам (в том числе родственникам) ПДн в любой форме их представления.
- 3.2.2 Использовать ПДн, за исключением ПДн признанных общедоступными, при подготовке публикаций, докладов, и т.д., а так же рекламной деятельности без соответствующего решения ПДЭК, утвержденной главным врачом БУЗ УР «РКТБ МЗ УР».
- 3.2.3 Обрабатывать ПДн за пределами защищаемой ИСПДн: выполнять работу на других АРМ, выносить из служебных помещений, уносить домой.
- 3.2.4 Снимать копии или делать выписки из конфиденциальных документов без разрешения ответственного лица за обработку и обеспечение защиты ПДн или главного врача БУЗ УР «РКТБ МЗ УР».
- 3.2.5 Принимать и передавать документы и материальные носители ПДн без распорядка и участия установленного в БУЗ УР «РКТБ МЗ УР».
- 3.2.6 Оставлять конфиденциальные документы на рабочих столах, в не запираемых ящиках и стеллажах, а так же оставлять незапертыми сейфы, хранилища и помещения, где хранятся конфиденциальные документы.
- 3.2.7 Использовать программно-аппаратные компоненты АРМ в неслужебных целях.
- 3.2.8 Вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ и средств защиты или устанавливать вспомогательное программное обеспечение и аппаратные средства без разрешения Администратора безопасности ПДн.
- 3.2.9 Обрабатывать ПДн в присутствии сотрудников, не имеющих к ним доступ или третьих лиц.
- 3.2.10 Подключать к АРМ неучтенные (личные) внешние носители, мобильные модемные и иные устройства без разрешения Администратора безопасности ПДн.
- 3.2.11 Записывать и хранить ПДн на неучтенных носителях информации (дискеты, компакт-диски, flash-носители).
- 3.2.12 Оставлять включенным без присмотра АРМ, временно не заблокировав доступ (см. п. 3.1.10).
- 3.2.13 Открывать общий сетевой доступ к папкам на своем АРМ.
- 3.2.14 Отключать (блокировать) используемые программно-аппаратные средства защиты.

3.2.15 Привлекать других сотрудников и третьих лиц для ремонта и настройки АРМ, без согласования с ответственным за обработку и обеспечение защиты ПДн и Администратором безопасности ПДн.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1 Работа Пользователя в сетях общего доступа и (или) международного обмена (далее Сеть) должна проводиться строго в рамках исполнения своих служебных обязанностей.

4.2 Работа Пользователя в Сети должна осуществляться только при включенных средствах защиты (антивирус, межсетевой экран и другие программные средства защиты от несанкционированного доступа при межсетевом взаимодействии).

4.3 Передача конфиденциальной информации по Сети должна проводиться при использовании программно-аппаратных криптографических средств и (или) по защищенным каналам связи.

4.4 Пользователю запрещается посещать Интернет-ресурсы сомнительного содержания, которые могут угрожать безопасности программной среды АРМ. В случае обнаружения подобных Интернет-ресурсов Пользователь обязан сообщить о них Администратору безопасности ПДн для блокировки доступа всех Пользователей ИСПДн к данному ресурсу.

4.5 В случае возникновения сбоев, ошибок или других внештатных ситуаций при работе в Сети, Пользователь обязан сообщить об этом Администратору безопасности ПДн.

4.6. Пользователю запрещается использовать личные мобильные или модемные устройства для выхода в Сеть.

Ответственность

Пользователь несет персональную ответственность за соблюдение требований настоящей Инструкции, требований Закона, а так же нормативных документов организаций в области защиты информации. За разглашение конфиденциальной информации и нарушение порядка обработки ПДн вне зависимости от формы их представления, Пользователь может быть привлечен к дисциплинарной, административной, гражданской, уголовной и иной, предусмотренной законодательством ответственности. Пользователь несет персональную ответственность за сохранность доверенных ему носителей ПДн

(бумажных, электронных, материальных) в соответствии с порядком учета выдачи и хранения носителей, определенным в БУЗ УР «РКТБ МЗ УР».

Заместитель главного врача

по общим вопросам

Начальник юридического отдела

Начальник отдела кадров

Администратор безопасности

Э.Я. Исаакова

В.Ф. Хужин

И.Г. Маурин

Ю.С. Смољин

С Инструкцией ознакомлены: