Государственное автономное учреждение здравоохранения Тюменской области «Тобольская городская стоматологическая поликлиника»
ГАУЗ ТО «ТГСП»

УТВЕРЖДАЮ
Главный врач
ГАУЗ ТО «ТГСП»
_____ В.В. Аполонов
«30» июля 2018 г.

м.п.

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Ultramed» ГАУЗ ТО «ТГСП»

1. Общие положения

1.1. Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (далее – ИСПДн) «Ultramed» ГАУЗ ТО «ТГСП» (далее – Учреждение) разработаны на основании приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и частной модели угроз ИСПДн «Ultramed».

1.2. Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн «Ultramed» Учреждения.

2. Организационные мероприятия по обеспечению безопасности персональных данных

2.1. Задаются требования по: охране помещений, допуску лиц, выбору технических средств, их расположению в помещениях. Кроме того, задаются дополнительные требования по обеспечению конфиденциальности и целостности ПДн.

2.2. К числу мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора могут относиться:

2.2.1. Назначение оператором, ответственного за организацию обработки персональных данных;

2.2.2. Издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов,

устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

2.2.3. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

2.2.4. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных»;

2.2.5. Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

2.2.6. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2.2.7. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

2.2.8. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

2.2.9. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

2.2.10. Учет машинных носителей персональных данных;

2.2.11. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

2.2.12. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

2.2.13. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

2.2.14. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.3. При этом должна обеспечиваться комплексность защиты персональных данных, в том числе посредством применения некриптографических средств защиты.

2.4. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе осуществляется:

2.4.1. Разработка для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

2.4.2. Разработка на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

2.4.3. Определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

2.4.4. Установка и ввод в эксплуатацию средств защиты информации (в том числе криптографических) в соответствии с эксплуатационной и технической документацией к этим средствам;

2.4.5. Проверка готовности средств защиты информации (в том числе криптографических) к использованию с составлением заключений о возможности их эксплуатации;

2.4.6. Поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

2.4.7. Контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

2.4.8. Разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

2.4.9. Описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

- индекса, условного наименования и регистрационных номеров используемых криптосредств;
- соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;
- соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты.

2.5. Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2.6. Пользователи информационных систем персональных данных обязаны:

2.6.1. Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

2.6.2. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

2.6.3. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

2.6.4. Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;

2.6.5. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.7. Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2.8. Обеспечение функционирования и безопасности информационной системы персональных данных возлагается на ответственного за выполнение работ по обеспечению безопасности персональных данных, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь).

2.9. Ответственный за выполнение работ по обеспечению безопасности персональных данных должен иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

2.10. При определении обязанностей ответственного за выполнение работ по обеспечению безопасности персональных данных необходимо учитывать, что безопасность обработки с использованием криптосредств персональных данных обеспечивается:

2.10.1. Соблюдением пользователями криптосредств, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения

безопасности применяемых криптосредств и ключевых документах к ним;

2.10.2. Точным выполнением пользователями криптосредств, требований к обеспечению безопасности персональных данных;

2.10.3. Надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

2.10.4. Обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных мер;

2.10.5. Своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

2.10.6. Немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.11. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей), должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.12. Текущий контроль за организацией и обеспечением функционирования средств защиты информации (в том числе криптографических) возлагается на оператора и ответственного пользователя в пределах их служебных полномочий.

2.13. Контроль за организацией, обеспечением функционирования и безопасности средств защиты информации (в том числе криптографических), предназначенных для защиты персональных данных, при их обработке в информационных системах персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

3. Мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа при их обработке в информационной системе персональных данных

В комплекс мероприятий по защите персональных данных (далее – ПДн) при их обработке в ИСПДн «Ultramed» от несанкционированного доступа (далее – НСД) и неправомерных действий входят мероприятия, реализуемые в рамках подсистем:

- управления доступом,
- регистрации и учета,
- обеспечения целостности,
- обеспечения межсетевой безопасности.

Подсистема управления доступом

3.1. Для всех сотрудников Учреждения, допущенных к обработке ПДн, в подсистеме управления доступом должна быть реализована:

- идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета

3.2. Для всех сотрудников Учреждения, допущенных к обработке ПДн, в подсистеме регистрации и учета должны быть реализованы следующие мероприятия:

3.2.1. Регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются:

- дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;
- результат попытки входа (успешная или неуспешная);
- идентификатор (код или фамилия) пользователя;
- предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.

3.2.2. Регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание документа (наименование, вид, шифр, код);
- идентификатор пользователя, запросившего документ.

3.2.3. Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются:

- дата и время запуска, имя (идентификатор) программы (процесса, задания);
- идентификатор пользователя;
- запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный).

3.2.4. Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);
- идентификатор пользователя;
- спецификация защищаемого файла.

3.2.5. Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная);
- идентификатор пользователя;
- спецификация защищаемого объекта (логическое имя (номер)).

3.2.6. Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

3.2.7. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей.

Подсистема обеспечения целостности

3.3. В подсистеме обеспечения целостности должны быть реализованы следующие мероприятия:

3.3.1. Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;

3.3.2. Физическая охрана технических средств ИСПДн «Ultramed» (устройств и носителей информации), предусматривающая:

- контроль доступа в помещения посторонних лиц;
- наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;

3.3.3. Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

3.3.4. Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Подсистема обеспечения целостности

3.4. В подсистеме обеспечения безопасного межсетевого взаимодействия при подключении ИСПДн к сетям международного информационного обмена

безопасность ПДн достигается путем применения средств межсетевого экранирования, которые обеспечивают:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
- фильтрацию с учетом даты и времени;
- аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
- контроль целостности своей программной и информационной части;

- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Дополнительные требования.

3.5. Наряду с методами и способами, указанными выше, основными методами и способами защиты информации от несанкционированного доступа являются:
- анализ защищенности ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);
- использование средств антивирусной защиты;
- применение программного обеспечения средств защиты информации, соответствующего 4 уровню контроля отсутствия не декларированных возможностей.

4. Методы и способы защиты информации от утечки по техническим каналам.

4.1. При обработке ПДн в ИСПДн «Ultramed» за счет реализации технических каналов утечки информации являются:
- утечки акустической (речевой) информации;
- утечки видовой информации;
- утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Утечки акустической (речевой) информации.

4.2. В ИСПДн «Ultramed» не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн «Ultramed» не предусмотрены.

4.3. Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

Утечки видовой информации.

4.4. Для исключения просмотра текстовой и графической видовой информации отображаемой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн «Ultramed» рекомендуется

оборудовать помещения в которых они установлены шторами (жалюзи), если таковые отсутствуют.

Утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

4.5. Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн «Ultramed», неактуально, так как для ИСПДн «Ultramed» возникновение угроз утечки информации по каналу ПЭМИН имеет малую вероятность, так как технические (аппаратные) средства ИСПДн размещаются в помещениях в пределах контролируемой зоны (далее – КЗ), что приводит к ослаблению побочных электромагнитных излучений (в том числе информативных сигналов) на границе КЗ до величин, обеспечивающих значительную сложность их выделения средством перехвата на фоне естественных шумов в условиях высокой энергонасыщенности.

Главный врач _____ В.В. Аполонов