Государственное бюджетное учреждение здравоохранения
Тюменской области
Областная больница №7 (с. Армизонское)

УТВЕРЖДАЮ
Главный врач ГБУЗ ТО
«Областная больница №7»
_____ Д.А. Бойко
«____» _____ 2013г.

м.п.

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационной системе персональных данных
«База пациентов ЛПУ»
ГБУЗ ТО «Областная больница №7»

1. Общие положения

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «База пациентов ЛПУ» ГБУЗ ТО «Областная больница №7» (далее – ИСПДн) 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.

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн «База пациентов ЛПУ» ГБУЗ ТО «Областная больница №7»

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, целостности и доступности персональных данных (далее – 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 Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2.13 Установление 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 Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.2.14.1.

2.3 Оператор персональных данных несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки персональных данных.

2.4 При этом должна обеспечиваться комплексность защиты персональных данных.

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

- разработка для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработка на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, 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;

2.6 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».

2.7 Сведения предусмотренные пунктами 5, 7^1, 10 и 11 части 3 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» должны быть предоставленны в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

2.8 Пользователи информационных систем персональных данных обязаны:

- не разглашать информацию, к которой они допущены, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности персональных данных;
- немедленно уведомлять оператора о фактах утраты или недостачи ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2.9 Обеспечение функционирования и безопасности информационной системы персональных данных возлагается на ответственного пользователя, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь).

2.10 Ответственные пользователи должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

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 ПДн при их обработке в ИСПДн «База пациентов ЛПУ» 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

Для всех сотрудников ГБУЗ ТО «Областная больница №7», допущенных к обработке ПДн в ИСПДн «База пациентов ЛПУ», в подсистеме управления доступом должны быть реализованы следующие мероприятия:

1. идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
2. идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам)
3. идентификация программ, томов, каталогов, файлов, записей, полей записей по именам
4. контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета

Для всех сотрудников ГБУЗ ТО «Областная больница №7», допущенных к обработке ПДн в ИСПДн «База пациентов ЛПУ», в подсистеме регистрации и учета должны быть реализованы следующие мероприятия:

1. регистрация входа (выхода) субъектов доступа 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 АРМ. В параметрах регистрации указываются:

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

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. 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);
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;
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));
6. учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);
7. дублирующий учет защищаемых носителей информации;
8. очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей.

Подсистема обеспечения целостности

В подсистеме обеспечения целостности должны быть реализованы следующие мероприятия:

1. обеспечение целостности программных средств СЗПДн, 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;
2. физическая охрана компонентов ИСПДн «База пациентов ЛПУ» (устройств и носителей информации), предусматривающая:

- контроль доступа в помещения расположения АРМ ИСПДн «База пациентов ЛПУ» посторонних лиц;
- наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн «База пациентов ЛПУ» и хранилище носителей информации, особенно в нерабочее время;

3. периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн «База пациентов ЛПУ» с помощью тест-программ, имитирующих попытки НСД;
4. наличие средств восстановления СЗПДн, предусматривающих ведение двух копий программных средств защиты информации и их периодическое обновление и контроль работоспособности.

Подсистема обеспечения безопасного межсетевого взаимодействия

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.

Наряду с методами и способами, указанными выше, основными методами и способами защиты информации от несанкционированного доступа являются:

- обнаружение вторжений в операционную систему ИСПДн, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);
- использование средств антивирусной защиты;
- централизованное управление средствами защиты информации ИСПДн.
- применение программного обеспечения средств защиты информации, соответствующего 4 уровню контроля отсутствия недекларированных возможностей.

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

При обработке ПДн в ИСПДн техническими каналами утечки информации являются:

- утечки акустической (речевой) информации;
- утечки видовой информации;
- утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Утечки акустической (речевой) информации.

В ИСПДн «База пациентов ЛПУ» не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн «База пациентов ЛПУ» не предусмотрены.

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

Утечки видовой информации.

Утечка видовой информации исключается вследствие невозможности неконтролируемого пребывания на территории КЗ. Нет наличия прямой видимости между возможным средством наблюдения и носителем ПДн.

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

Учитывая класс ИСПДн, категорию обрабатываемых данных, а также имея в виду отсутствие возможности увеличения расстояния от основных технических средств и систем (ОТСС) до границы контролируемой зоны (КЗ) до минимально допустимого, в служебных помещениях, в которых ведется обработка ПДн с использованием ОТСС, необходимо использовать средства активной защиты, предотвращающие утечку информации по каналам ПЭМИН. Однако в соответствии с требованиями санитарных правил и норм (СанПиН) в части электромагнитных излучений радиочастотного диапазона (ЭМИ РЧ), для лечебно-профилактических учреждений недопустима установка средств активной защиты от утечек информации по каналу ПЭМИН. Поэтому в ГБУЗ ТО «Областная больница №7» предусматривается обеспечение защиты от утечек по каналу ПЭМИН посредством ужесточения регламентных мер режима охраны и удаления источников излучения на максимальное расстояние от границ контролируемой зоны в пределах доступных помещений.

Защита утечки ПДн по каналам побочных электромагнитных излучений и наводок производится для ИСПДн 1 класса.

Комплекс мероприятий от утечки конфиденциальной информации по каналу ПЭМИН определяется после проведения и анализа замеров в ИСПДн «База пациентов ЛПУ».

Заместитель главного врача по
организационно-методической работе
с населением
ГБУЗ ТО «Областная больница №7» _____ Л.А. Новосильцева