

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ ТЮМЕНСКОЙ ОБЛАСТИ
«ХОСПИС»**

УТВЕРЖДАЮ

Главный врач ГБУЗ ТО «Хоспис»

А.А. Филимонов

« 18 » _____ 2014 г.



**ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационной системе персональных данных
«Медстатистик»
ГБУЗ ТО «Хоспис»**

1. Общие положения

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных «Медстатистик» ГБУЗ ТО «Хоспис» (далее – ИСПДн) разработаны на основании приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке 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 «Медстатистик» ГБУЗ ТО «Хоспис».

2. Организационные мероприятия по обеспечению безопасности персональных данных

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).

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 «Медстатистик» входят мероприятия, реализуемые в рамках подсистем:

- идентификация и аутентификация субъектов доступа и объектов доступа,
- управление доступом субъектов доступа к объектам доступа,
- защита машинных носителей персональных данных,
- регистрация событий безопасности,
- антивирусная защита,
- контроль (анализ) защищенности персональных данных,
- защита среды виртуализации,
- защита технических средств,
- защита информационной системы, ее средств, систем связи и передачи данных,
- управление конфигурацией информационной системы и системы защиты персональных данных.

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. идентификация и аутентификация пользователей, являющихся работниками оператора;
2. управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
3. управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
4. защита обратной связи при вводе аутентификационной информации;
5. идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

Подсистема управления доступом субъектов доступа к объектам доступа

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

2. реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
3. управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
4. разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
5. назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
6. ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
7. блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
8. разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
9. реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
10. регламентация и контроль использования в информационной системе технологий беспроводного доступа;
11. регламентация и контроль использования в информационной системе мобильных технических средств;
12. управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

Подсистема защиты машинных носителей персональных данных

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», должно быть реализовано 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.

Подсистема регистрации системы безопасности

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. определение событий, подлежащих регистрации, и сроков их хранения;
2. определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
3. сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
4. защита информации о событиях безопасности.

Подсистема антивирусной защиты

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. реализация антивирусной защиты;
2. обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Подсистема контроля (анализа) защищенности персональных данных

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
2. контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
3. контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
4. контроль состава технических средств, программного обеспечения и средств защиты информации.

Подсистема защиты среды виртуализации

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
2. управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
3. регистрация событий безопасности в виртуальной инфраструктуре;

4. реализация и управление антивирусной защитой в виртуальной инфраструктуре;
5. разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей.

Подсистема защиты технических средств

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. 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;
2. размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Подсистема защиты информационной системы, ее средств, систем связи и передачи данных

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. 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;
2. защита беспроводных соединений, применяемых в информационной системе.

Управление конфигурацией информационной системы и системы защиты персональных данных

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Медстатистик», в подсистеме должны быть реализованы следующие мероприятия:

1. определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;
2. управление изменениями конфигурации информационной системы и системы защиты персональных данных;

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;
4. документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.

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 «Медстатистик» не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн не предусмотрены.

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

Утечки видовой информации

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 рекомендуется оборудовать помещения в которых они установлены шторами (жалюзи), а также повернуть мониторы в сторону стены.

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

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

Фельдшер ГБУЗ ТО «Хоспис»



П.Н. Сафронов