

**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  
«Бухгалтерский и кадровый учет»  
ГБУЗ ТО «Хоспис»**

**1. Общие положения**

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных «Бухгалтерский и кадровый учет» 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 «Бухгалтерский и кадровый учет» 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 «Бухгалтерский и кадровый учет» входят мероприятия, реализуемые в рамках подсистем:

- идентификация и аутентификация субъектов доступа и объектов доступа,
- управление доступом субъектов доступа к объектам доступа,
- 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.

#### **Подсистема идентификации и аутентификации субъектов доступа и объектов доступа**

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Бухгалтерский и кадровый учет», 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 «Бухгалтерский и кадровый учет», 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 пользователей, администраторам и лицам, обеспечивающим функционирование информационной системы;
6. ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
7. реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
8. регламентация и контроль использования в информационной системе технологий беспроводного доступа;
9. регламентация и контроль использования в информационной системе мобильных технических средств;
10. управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

#### **Подсистема регистрации системы безопасности**

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Бухгалтерский и кадровый учет», должны быть реализованы следующие мероприятия:

1. определение событий безопасности, 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 «Бухгалтерский и кадровый учет», 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 «Бухгалтерский и кадровый учет», должен быть реализован контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

### **Подсистема защиты среды виртуализации**

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Бухгалтерский и кадровый учет», 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.

### **Подсистема защиты технических средств**

Для всех работников ГБУЗ ТО «Хоспис», допущенных к обработке ПДн в ИСПДн «Бухгалтерский и кадровый учет», 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 «Бухгалтерский и кадровый учет», должна быть обеспечена защита 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.

#### **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 «Бухгалтерский и кадровый учет» 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 «Бухгалтерский и кадровый учет».

Фельдшер ГБУЗ ТО «Хоспис»



П.Н. Сафронов