Приложение № 2
К приказу ГЛПУ ТО «ОСПК»
от 19.07.2010 № 19

Для служебного пользования
Экз. № 1

УТВЕРЖДАЮ
Главный врач
ГЛПУ ТО «ОСПК» А.В. Гаврилей

«19» 07 2010 года
м.п.

ТРЕБОВАНИЯ

по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Информационная система ГЛПУ ТО «Областная станция переливания крови»

1 Общие положения.

1.1 Данные требования по обеспечению безопасности персональных данных (далее ПДн) при их обработке в информационной системе персональных данных «Информационная система ГЛПУ ТО «Областная станция переливания крови» (далее – ИСПДн ГЛПУ ТО «ОСПК») разработаны на основании нормативно правовых актов и методических документов утверждённых ФСБ Российской Федерации и ФСТЭК России в соответствии с пунктом 2 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённого Постановлением Правительства Российской Федерации от 17 ноября 2007 № 781 (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн ГЛПУ ТО «ОСПК». Требования распространяются только на данную ИСПДн ГЛПУ ТО «ОСПК» и её подсистемы.

2 Организационные мероприятия по обеспечению безопасности персональных данных.

2.1 Должна осуществляться охрана помещений, определены границы контролируемой зоны, защищаемые помещения.

2.2 Должны быть определены ответственные за обеспечение безопасности персональных данных.

2.3 Должны быть разработаны инструкции, правила, порядки в части обеспечения безопасности персональных данных.

2.4 Должна осуществляться разрешительная система допуска работников к персональным данным.

2.5 Должен осуществляться выбор технических средств и их расположение в помещениях, обеспечивающий безопасность персональных данных в ИСПДн ГЛПУ ТО «ОСПК».

2.6 К основным вопросам управления обеспечением безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты, поддержания требуемого уровня безопасности персональных данных относятся:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;
- определение порядка изменения правил доступа к защищаемой информации;
- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- определение порядка действия должностных лиц в случае возникновения нештатных ситуаций;
- определение порядка проведения контрольных мероприятий и действий по его результатам.

2.7 Должно быть разграничение допуска к ИСПДн ГЛПУ ТО «ОСПК».

- разграничения допуска к программно-аппаратным ресурсам ИСПДн ГЛПУ ТО «ОСПК»;
- ведение учета ознакомления работников ГЛПУ ТО «ОСПК» с информацией ограниченного распространения;
- включение в функциональные обязанности работников ГЛПУ ТО «ОСПК» обязательства о неразглашении и сохранении сведений ограниченного распространения;
- организация уничтожения сведений ограниченного распространения (на бумажных, магнитных носителях и др.), не используемого в деятельности ГЛПУ ТО «ОСПК»;
- ведение учета отчуждаемых носителей информации;
- организация и осуществление периодического контроля за обеспечением безопасности персональных данных;
- организация учета средств криптографической защиты информации, ключей шифрования и подписи, их хранения, эксплуатации и уничтожения.

3 Мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа (далее – НСД) при их обработке в ИСПДн ГЛПУ ТО «ОСПК».

В комплекс мероприятий по защите персональных данных при их обработке в ИСПДн ГЛПУ ТО «ОСПК» от НСД и неправомерных действий входят следующие направления:

- защита от НСД при многопользовательском режиме обработки персональных данных и разных правах доступа;
- антивирусная защита.

Мероприятия по защите ПДн реализуются в рамках подсистем:

- управления доступом;
- регистрации и учёта;
- обеспечения целостности;
- антивирусной защиты.

3.1 Требования к подсистеме управления доступом.

3.1.1 Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов.

3.1.2 Должна осуществляться идентификация терминалов, компьютеров, узлов сети ИСПДн ГЛПУ ТО «ОСПК», каналов связи, внешних устройств компьютеров по логическим именам и/или адресам.

3.1.3 Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

3.1.4 Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

3.1.5 Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

3.2 Требования к подсистеме регистрации и учёта:

3.2.1 Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн ГЛПУ ТО «ОСПК». 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) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.

3.2.2 Должна осуществляться регистрация выдачи печатных (графических) документов на «твёрдую» копию. В параметрах регистрации указываются дата и время выдачи (обращение к подсистеме вывода), спецификация устройства выдачи – логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ.

3.2.3 Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов (персональных данных). В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный).

3.2.4 Должна осуществляться 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 её результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла.

3.2.5 Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей (защищаемым файлам). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту (файлу) с указанием её результата (успешная, неуспешная –

несанкционированная), идентификатор субъекта доступа (пользователя), спецификация защищаемого (файла) объекта – логическое имя (номер).
3.2.6 Должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку).
3.2.7 Должен осуществляться дублирующий учёт защищаемых носителей информации.
3.2.8 Должна осуществляться регистрация изменений полномочий субъектов доступа и статусов объектов доступа. В параметрах регистрации указываются дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения.
3.2.9 Должен осуществляться автоматический учёт создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистемах управления доступом. Маркировка должна отражать уровень конфиденциальности объекта.
3.2.10 Должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и занесением учётных данных в журнал (учётную карточку), учёт защищаемых носителей должен проводиться в журнале (карточке) с регистрацией их выдачи (приёма).
3.2.11 Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации.
3.2.12 Должна осуществляться сигнализация попыток нарушения защиты.

3.3 Требования к подсистеме обеспечения целостности:

3.3.1 Должна обеспечиваться целостность программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных должна проверяться при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечиваться использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и/или хранения персональных данных.
3.3.2 Должна осуществляться физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надёжных препятствий для несанкционированного проникновения в помещения и хранилища носителей информации.
3.3.3 Должно проводиться 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 Должно быть наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.
3.3.5 Должен быть предусмотрен администратор защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн.
3.3.6 Должны использоваться сертифицированные средства защиты.

3.4 Требования к подсистеме антивирусной защиты:

3.4.1 Должна проводиться автоматическая проверка на наличие вредоносных программ или последствий ПВМ при импорте в ИСПДн ГЛПУ ТО «ОСПК» всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.
3.4.2 Должны быть реализованы механизмы автоматического блокирования обнаруженных ВП путём их удаления из программных модулей или уничтожения.
3.4.3 Должна регулярно выполняться проверка на предмет наличия ВП в средствах защиты от ПВМ (при первом запуске средства защиты от ПВМ и с устанавливаемой периодичностью).
3.4.4 Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП.
3.4.5 Должен быть реализован механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.

4 Мероприятия по обеспечению безопасности персональных данных от побочных электромагнитных излучений и наводок (далее – ПЭМИН) при их обработке в ИСПДн ГЛПУ ТО «ОСПК».

Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации:

использование технических средств в защищенном исполнении;

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

размещение объектов защиты в соответствии с предписанием на эксплуатацию;

размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео - и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.