



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
СИБИРСКИЙ КЛИНИЧЕСКИЙ ЦЕНТР
ФЕДЕРАЛЬНОГО МЕДИКО-БИОЛОГИЧЕСКОГО АГЕНТСТВА

УТВЕРЖДАЮ

Генеральный директор
ФГБУЗ СКЦ ФМБА России



В.В. Баранкин

25 Октября 2011 г.
№ 598

ПОЛИТИКА

информационной безопасности персональных данных

Диск № 2-2008-17. Политика

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИСПДн – информационная система персональных данных

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

УБПДн – угрозы безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности персональных данных (далее – Политика) ФГБУЗ СКЦ ФМБА России (далее – Учреждения), разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПД Учреждения и является официальным документом.

1.2. Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также других подзаконных актов регулирующих сферу защиты информации.

1.3. В Политике определены требования к ИСПДн, степень ответственности персонала, требования к системе защиты, статус и обязанности сотрудников учреждения по защите ПДн.

1.4. Политика информационной безопасности ПДн определяет стратегию Учреждения в области ИБ ПДн, а также те меры и средства которые целесообразно применять для их защиты от несанкционированного доступа.

1.5. Целью настоящей Политики является обеспечение безопасности ПДн циркулирующих в информационных системах Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

1.6. Настоящая Политика направлена на:

- соблюдение интересов субъектов ПДн, Учреждения и государства в информационной сфере;
- соответствие процессов сбора, накопления, обработки и предоставления ПДн нормам законодательства Российской Федерации;
- унификацию политики Учреждения в области реализации технических, программных и программно – технических мер по защите информации;
- реализацию персональной ответственности за нарушения информационной безопасности;
- предотвращение и нейтрализацию угроз информационной безопасности Учреждения;
- постоянный, системный подход к контролю состояния информационной безопасности Учреждения.

1.7. Настоящая Политика информационной безопасности утверждается генеральным директором и вводится в действие приказом Учреждения.

2. ОБЛАСТЬ ДЕЙСТВИЯ

2.1. Политика информационной безопасности затрагивает все виды деятельности Учреждения, касающиеся сбора, обработки, накопления, предоставления и распространения ПДн.

2.2. Предметом настоящей Политики являются:

- персональные данные, представленные в виде документированной информации на различного рода носителях, информационных массивов и баз данных, подлежащих защите в соответствии с законодательством Российской Федерации и внутренними организационно-распорядительными документами Учреждения;
- средства и системы информатизации, программные средства, автоматизированные системы управления, информационные и технологические процессы, используемые для обработки ПДн.

2.3. Выполнение положений настоящей Политики информационной безопасности является обязательным для всех сотрудников Учреждения.

2.4. Взаимоотношения по использованию положений настоящего документа применительно к защите информации, находящейся в совместном ведении с другими организациями, регулируются на основании специальных соглашений.

3. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Система защиты ПДн разрабатывается на основании:

- федеральных законов, Указов Президента, Постановлений Правительства РФ, приказов и положениях ФСТЭК России, ФСБ России, Минкомсвязь России и других нормативно – правовых актов регулирующих область защиты информации;
- модели угроз информационной безопасности Учреждения;
- концепции информационной безопасности Учреждения;
- перечня персональных данных, подлежащих защите;
- актов классификации информационной системы персональных данных.

3.2. Система защиты ПДн Учреждения основывается на:

- использовании ПДн только в соответствии с целями их обработки в Учреждении;
- регламентации порядка доступа к информационным ресурсам;
- определении прав доступа к информационным ресурсам их владельцами;
- применении сертифицированных ФСТЭК России и ФСБ России средств защиты информации.

3.3. СЗПДн Учреждения должна обеспечивать:

- защиту внешнего периметра ИСПДн Учреждения от внешних угроз;
- защиту серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам серверов, механизмов мониторинга и аудита безопасности;
- комплексную антивирусную защиту систем, входящих в состав ИСПДн за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по всем узлам системы;
- мониторинг сетевого трафика в реальном масштабе времени с целью выявления злоумышленных действий пользователей ИСПДн Учреждения и попыток осуществления НСД к ресурсам корпоративной сети со стороны внешних злоумышленников;

- защиту прикладных подсистем, функционирующих в составе ИСПДн, обеспечение доступности предоставляемых ими прикладных сервисов;
- защиты межсетевых взаимодействий между узлами ИСПДн входящими в состав сети, включая подразделения Учреждения.

3.4. Для обеспечения безопасности СЗПДн необходимо использовать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства обнаружения вторжений;
- средства анализа защищенности;
- средства идентификации и аутентификации пользователей;
- средства физического разграничения доступа в защищаемые помещения;
- средства видеонаблюдения и охранной сигнализации;
- средства криптографической защиты информации;
- другие средства направленные на обеспечение информационной безопасности.

4. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Комплекс мер по защите информации в Учреждении включает в себя следующие мероприятия:

- назначение ролей и распределение ответственности;
- разработка, реализация, внедрение и контроль исполнения планов мероприятий и других документов по обеспечению информационной безопасности;
- аудит информационной безопасности Учреждения.

4.2. Политика защиты ИСПДн Учреждения реализуется путем сочетания организационных и технических мер направленных на защиту ИСПДн.

4.3. К организационным мерам защиты ИСПДн относятся:

- управление персоналом;
- физическая защита объекта;
- поддержание работоспособности;
- инвентаризация информационных ресурсов Учреждения;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

4.4. Реагирование на нарушения режима безопасности должно предусматривать набор оперативных мероприятий, регламентов и инструкций, направленных на обнаружение и нейтрализацию угрозы.

4.5. Общее руководство информационной безопасностью в Учреждении осуществляет Заместитель генерального директора по информационным и инновационным технологиям.

4.6. Работы по обеспечению информационной безопасности непосредственно осуществляют:

- ответственный за защиту информации в Учреждении;

- администраторы автоматизированных систем, информационных и коммуникационных систем, серверного оборудования, отдельного ПО.

4.7. В качестве основных задач возлагаемых на них следует выделить:

- администрирование встроенных механизмов используемого системного и прикладного программного обеспечения;
- администрирование применяемых дополнительных средств защиты информации;
- установление полномочий работников в отношении защищаемых информационных ресурсов;
- контроль выполнения работниками требований нормативных документов в области информационной безопасности.

5. ОБЯЗАННОСТИ СОТРУДНИКОВ УЧРЕЖДЕНИЯ ПО ЗАЩИТЕ ПДн

5.1. Описание обязанностей всех сотрудников Учреждения по обработке и защите ПДн закреплены в следующих документах:

- инструкция администратора ИСПДн;
- инструкция ответственного за защиту информации в ИСПДн;
- инструкция пользователя ИСПДн;
- инструкция пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.

5.2. Сотрудники Учреждения обязаны информировать о ставших им известными фактах нарушения положений настоящей Политики и инцидентах информационной безопасности своего непосредственного руководителя, ответственного за защиту информации или руководство Учреждения в незамедлительном порядке.

5.3. Ответственное лицо за защиту информации обязано инициировать и проводить служебные расследования по факту нарушений и инцидентов информационной безопасности в соответствии с установленной в Учреждении процедурой, и докладывать о результатах расследований руководству Учреждения.

6. ОТВЕТСТВЕННОСТЬ

6.1. В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6.2 Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).