ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных
государственного бюджетного учреждения здравоохранения
«Самарская областная клиническая психиатрическая больница»

Самара 2022

Содержание

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящее Положение об обеспечении безопасности персональных данных в ГБУЗ «СОКПБ» (далее – Положение) устанавливает требования к порядку обеспечения безопасности персональных данных в ГБУЗ «СОКПБ» (далее – Учреждение).

1.2 Цель принятия документа

1.2.1 Настоящее Положение принято в целях приведения процессов обеспечения безопасности персональных данных Учреждения в соответствие требованиям законодательства.

1.3 Область применения документа

1.4.1 Настоящий документ обязаны знать и использовать в работе ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ИСПДн	информационная система персональных данных
ПДн	персональные данные
СЗПДн	система защиты персональных данных

Таблица 2 — Перечень терминов

Термин	Определение термина
автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
доступ к информации	возможность получения информации и ее использования
информационная система персональных данных	совокупность содержащихся в базах данных персональныхданных и обеспечивающих их обработку информационных технологий и технических средств
обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
уровень защищенности персональных данных	комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

1.5 Внешние нормативные и распорядительные документы

Таблица 4 — Внешние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2	Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 24.07.2014) «О персональных данных»
4	Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4	Постановление Правительства РФ от 16 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
6	Приказ ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
6	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК России 16.02.2008)
7	«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14.02.2008)
8	Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
9	«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ России 21.02.2008 № 149/6/6-622)
10	«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ России 21.02.2008 № 149-64-144)

1.6 Внутренние нормативные и распорядительные документы

Таблица 4 — Внутренние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Положение о порядке организации обработки и обеспечении безопасности персональных данных работников в информационных системах государственного бюджетного учреждения здравоохранения «СОКПБ»
2	Положение о порядке организации обработки и обеспечении безопасности персональных данных пациентов в информационных системах государственного бюджетного учреждения здравоохранения «СОКПБ»
3	Положение об обеспечении безопасности персональных данных государственного бюджетного учреждения здравоохранения «СОКПБ»
4	Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных государственного бюджетного учреждения здравоохранения «СОКПБ»

1.7 Пересмотр документа

1.7.1 Пересмотр настоящего Положения должен осуществляться в следующих случаях, но не реже одного раза в три года:

– при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;

– при существенном изменении процессов обработки персональных данных Учреждения.

2 Основные мероприятия по обеспечению безопасности персональных данных

2.1 Учреждение при обработке персональных данных обязано принимать все необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

2.2 В Учреждении защите подлежат:

– информационные системы персональных данных;

– помещения, в которых осуществляется обработка персональных данных;

– материальные носители персональных данных.

2.4 При автоматизированной обработке ПДн защита информационных систем персональных данных осуществляется с учетом требований документа «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 1 ноября 2012 г. №1119).

2.4 При обработке ПДн без использования средств автоматизации (на бумажных носителях) защита персональных данных осуществляется с учетом требований документа «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (утв. Постановлением Правительства РФ от 16 сентября 2008 г. №687).

2.6 Обеспечение безопасности персональных данных в Учреждении достигается за счет выполнения следующих мероприятий:

а) назначения лица, ответственного за обеспечение безопасности персональных данных;

б) создания системы защиты персональных данных;

в) организации режима обеспечения безопасности помещений, в которых ведется обработка персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

г) определения порядка предоставления допуска к обработке персональных данных и предоставления доступа к информационным системам персональных данных;

д) организации учета машинных носителей персональных данных;

е) обеспечения сохранности материальных (бумажных) носителей персональных данных;

ж) проведения оценки вреда, который может быть причинен субъекту персональных данных в случае нарушения требований Федерального закона «О персональных данных»;

з) обнаружения фактов несанкционированного доступа к персональным данным и принятия мер по таким фактам;

и) восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

к) проведения периодических проверок соблюдения порядка обработки и обеспечения безопасности персональных данных в Учреждении.

3 Система защиты персональных данных

4.1 Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения обеспечивается построением системы защиты персональных данных (далее – СЗПДн).

4.2 Функционирование СЗПДн обеспечивается комплексом организационных мероприятий, а также применением технических средств защиты информации с целью обеспечения конфиденциальности, целостности и доступности ПДн в процессе их обработки.

4.4 Объектом защиты СЗПДн являются:

– персональные данные, содержащиеся в ИСПДн;

– технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации);

– общесистемное, прикладное, специальное программное обеспечение;

– информационные технологии;

– средства защиты информации.

4.4 Создание СЗПДн включает следующие этапы:

а) выявление информационных систем, в которых осуществляется обработка персональных данных;

б) выделение информационных систем персональных данных (в одну ИСПДн может быть объединено несколько информационных систем);

в) разработка модели угроз и нарушителя безопасности для каждой из ИСПДн;

г) определение необходимого уровня защищенности ПДн для каждой из ИСПДн;

д) выбор мер обеспечения безопасности персональных данных;

е) разработка технического задания на создание (модернизацию) СЗПДн;

ж) разработка технического проекта (технического решения) СЗПДн;

з) внедрение СЗПДн;

и) проведение приемо-сдаточных испытаний СЗПДн (при необходимости, проведение аттестационных испытаний);

к) осуществление периодического контроля эффективности СЗПДн и, в случае необходимости, принятие решения о модернизации СЗПДн.

4.6 В состав СЗПДн, входят следующие технические подсистемы защиты:

– Подсистема идентификации и аутентификации субъектов доступа
– Подсистема управления доступом субъектов доступа к объектам доступа
– Подсистема регистрации событий безопасности
– Подсистема антивирусной защиты
– Подсистема анализа защищенности
– Подсистема технических средств

4.6 Все средства защиты информации, применяемые в составе СЗПДн, должны пройти оценку соответствия в порядке, установленном законодательством РФ.

4.7 Для выполнения работ по созданию СЗПДн в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридические лица, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

4 Ответственный за обеспечение безопасности персональных данных

4.1 В целях эффективной организации мероприятий по обеспечению безопасности персональных данных в Учреждении назначается лицо, ответственное за обеспечение безопасности персональных данных.

4.2 Роль ответственного за обеспечение безопасности персональных данных назначается одному или нескольким работникам Учреждения приказом исполнительного органа Учреждения.

4.4 Функции ответственного за обеспечение безопасности персональных данных определяются в соответствующем регламенте.

5 Комиссия по обеспечению безопасности персональных данных

6.1 В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в Учреждении создается постоянно действующая комиссия пообеспечению безопасности персональных данных.

6.2 В состав Комиссии должны входить как минимум:

– ответственный за организацию обработки персональных данных;
– ответственный за обеспечение безопасности персональных данных;
– руководители или работники подразделений, ответственных за сопровождение информационных систем персональных данных.

6.4 Состав Комиссии утверждается приказом исполнительного органа Учреждения.

6.4 Комиссия по обеспечению безопасности персональных данных выполняет следующие функции:

а) оценка вреда, который может быть причинен субъекту персональных данных в случае нарушения требований Федерального закона «О персональных данных»;

б) выделение информационных систем персональных данных;

в) разработка модели угроз и нарушителя безопасности персональных данных для каждой информационной системы персональных данных;

г) определение необходимого уровня защищенности персональных данных при их обработке в информационных системах персональных данных;

д) выбор мер по обеспечению безопасности персональных данных;

е) контроль уничтожения (обезличивания) персональных данных;

ж) реализация мер по обнаружению и реагированию на инциденты информационной безопасности, способные привести к нарушению;

з) разработка и утверждение плана внутренних проверок порядка обработки персональных данных;

и) осуществление внутреннего контроля за соблюдением Учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных в соответствии с утвержденным планом проверок.