

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационной системе персональных данных
«Прием пациента»

1. Общие положения

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (далее – ИСПДн) «Прием пациента» (далее – Требования) разработаны на основании приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», частной модели угроз безопасности ПДн при их обработке в ИСПДн.

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных (далее – ПДн) при их обработке в ИСПДн.

2. Организационные мероприятия по обеспечению безопасности ПДн

2.1 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 ПДн.

2.2 К числу мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора относятся:

- Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;

- Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников;

- Определение угроз безопасности ПДн при их обработке в ИСПДн;

- Применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

- Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- Учет машинных носителей ПДн;
- Обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- Установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

2.3 При разработке и реализации мероприятий по организации и обеспечению безопасности ПДн при их обработке в информационной системе осуществляется:

- разработка для каждой ИСПДн модели угроз безопасности ПДн при их обработке;
- разработка на основе модели угроз системы безопасности ПДн, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

2.4 В соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и установленным уровнем защищенности ПДн, обрабатываемых в ИСПДн необходимо выполнение следующих требований:

- контроль за выполнением настоящих Требований организуется и проводится не реже 1 раза в 3 года;
- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей ПДн;
- утверждение документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- назначено должностное лицо (работник), ответственный за обеспечение безопасности ПДн в информационной системе;
- необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;
- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника по доступу к ПДн, содержащимся в информационной системе;

– создание структурного подразделения, ответственного за обеспечение безопасности ПДн в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

2.5 При использовании в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации для обеспечения установленного уровня защищенности ПДн применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты;
- межсетевые экраны не ниже 3 класса.

3. Мероприятия по обеспечению безопасности ПДн от несанкционированного доступа при их обработке в ИСПДн

В состав мер по обеспечению безопасности ПДн, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты ПДн.

В таблице 1 приведено содержание требуемых мер по обеспечению безопасности ПДн:

Таблица 1. Содержание требуемых мер по обеспечению безопасности ПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Подразделение, ответственное за выполнение меры по обеспечению безопасности ПДн
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Отдел АСУ, взрослая поликлиника
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Отдел АСУ
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Отдел АСУ
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Отдел АСУ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Подразделение, ответственное за выполнение меры по обеспечению безопасности ПДн
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Отдел АСУ
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Отдел АСУ
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Отдел АСУ
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Отдел АСУ
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Отдел АСУ
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Отдел АСУ
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Отдел АСУ
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Отдел АСУ
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности ПДн, и о необходимости соблюдения установленных оператором правил обработки ПДн	Отдел АСУ
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	Отдел АСУ
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	Отдел АСУ
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Отдел АСУ
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Отдел АСУ
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	Отдел АСУ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Подразделение, ответственное за выполнение меры по обеспечению безопасности ПДн
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Отдел АСУ
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Отдел АСУ
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Отдел АСУ
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Отдел АСУ
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	Отдел АСУ
III. Ограничение программной среды (ОПС)		
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	Отдел АСУ
IV. Защита машинных носителей ПДн (ЗНИ)		
ЗНИ.1	Учет машинных носителей ПДн	Отдел АСУ
ЗНИ.2	Управление доступом к машинным носителям ПДн	Отдел АСУ
ЗНИ.8	Уничтожение (стирание) или обезличивание ПДн на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Отдел АСУ
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Отдел АСУ
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Отдел АСУ
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Отдел АСУ
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Отдел АСУ
РСБ.7	Защита информации о событиях безопасности	Отдел АСУ
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Отдел АСУ
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Отдел АСУ
VII. Обнаружение вторжений (СОВ)		
СОВ.1	Обнаружение вторжений	Отдел АСУ, взрослая

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Подразделение, ответственное за выполнение меры по обеспечению безопасности ПДн
СОВ.2	Обновление базы решающих правил	поликлиника
VIII. Контроль (анализ) защищенности ПДн (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Отдел АСУ
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Отдел АСУ
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Отдел АСУ
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Отдел АСУ
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	Отдел АСУ
IX. Обеспечение целостности информационной системы и ПДн (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Отдел АСУ
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	Отдел АСУ
X. Обеспечение доступности ПДн (ОДТ)		
ОДТ.4	Периодическое резервное копирование ПДн на резервные машинные носители ПДн	Отдел АСУ, при наличии технической возможности
ОДТ.5	Обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного интервала	Отдел АСУ, при наличии технической возможности
XII. Защита технических средств (ЗТС)		
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключая несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Отдел АСУ, взрослая поликлиника

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Подразделение, ответственное за выполнение меры по обеспечению безопасности ПДн
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Взрослая поликлиника
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.3	Обеспечение защиты ПДн 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	Отдел АСУ
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	Отдел АСУ
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки ПДн	Отдел АСУ
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Отдел АСУ
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Отдел АСУ
XIV. Выявление инцидентов и реагирование на них (ИНЦ)		
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Отдел АСУ, взрослая поликлиника
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Отдел АСУ, взрослая поликлиника
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Отдел АСУ, взрослая поликлиника
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Отдел АСУ, взрослая поликлиника
ИНЦ.5	Принятие мер по устранению последствий инцидентов	Отдел АСУ, взрослая поликлиника
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Отдел АСУ, взрослая поликлиника
XV. Управление конфигурацией информационной системы и системы защиты ПДн (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты ПДн	Отдел АСУ
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты ПДн	Отдел АСУ