Меры по защите информации
в региональном сегменте
единой государственной информационной системы здравоохранения
Ленинградской области

1 Общие положения

Перечень документов, на основании которых выполняются мероприятия по информационной безопасности в региональном сегменте единой государственной информационной системы здравоохранения Ленинградской области (ЕГИСЗ ЛО) приведён в таблице 1.

Таблица 1

№ п\п	Наименование документа	Условное обозначение
1.	Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»	[1]
2.	Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»	[2]
3.	Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	[3]
4.	Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»	[4]
5.	Приказ ФСБ России от 10 июля 2014 года № 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»	[5]
6.	Приказ ФАПСИ от 13 июня 2001 г.№152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	[6]
7.	Приказ ФСТЭК России от 11 февраля 2013 № 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах	[7]
8.	Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России) от 18 февраля 2014 г. № 21 об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	[8]

2. Требования к применяемым средствам защиты информации

Автоматизированные рабочие места, подключаемые к ЕГИСЗ ЛО, должны быть аттестованы в соответствии с требованиями по защите информации по 2 классу защищённости (К2), в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Средства защиты информации (СЗИ), применяемые в ЕГИСЗ ЛО, должны иметь сертификаты соответствия требованиям по безопасности информации, подтверждающим возможность их применения в государственных информационных системах не ниже 2 класса защищенности (К2).

В составе Системы ЗИ ЕГИСЗ ЛО должны применяться средства защиты информации, удовлетворяющие требованиям:

- средства антивирусной защиты не ниже 4 класса («Требования к средствам антивирусной защиты» Утверждены приказом ФСТЭК России от 20 марта 2012 №28ДСП);
- межсетевые экраны не ниже 5 класса («Требования к межсетевым экранам» Утверждены приказом ФСТЭК России от 9 февраля 2016 г. №9, ДСП);
- средства криптографической защиты информации не ниже класса КС2;
- средства защиты от несанкционированного доступа.

В качестве средств криптографической защиты информации при удалённом взаимодействии пользователей с ЕГИСЗ ЛО для подписания с помощью электронной подписи документов в электронном виде должны использоваться средства криптографической защиты информации.

3. Организационные мероприятия по защите информации

В качестве организационных мер для управления защитой и обеспечения безопасности ЕГИСЗ ЛО необходимо:

- обеспечить режим безопасности помещений, в которых размещена ЕГИСЗ ЛО, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечить сохранности носителей информации ограниченного доступа ЕГИСЗ ЛО;

- распределить функции управления доступом к данным и их обработкой между должностными лицами;

- определить порядок изменения правил доступа к защищаемой информации;

- определить порядок действий должностных лиц в случае возникновения нештатных ситуаций;

- определить порядок проведения контрольных мероприятий и действий по его результатам.

В качестве технических мер для управления защитой и обеспечения безопасности ЕГИСЗ ЛО необходимо:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защиту машинных носителей информации;

- регистрацию событий безопасности;

- антивирусную защиту;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности информации;

- целостность информационной системы и информации;

- доступность информации;

- защиту среды виртуализации;

- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных.

Для реализации организационных и технических мер необходимо разработать организационно-распорядительные документы, приведённые в Таблице 2, а также предусмотреть организационные мероприятия, проводимые должностными лицами, при работе в ЕГИСЗ ЛО.

Таблица 2. Перечень организационно-распорядительных документов

№ п\п	Наименование документа	Правовые акты, на основании которых ведется разработка документов
1.	Документ об определении ответственного за защиту информации в ЕГИСЗ ЛО.	п.9 [7][1], п.7 [4]
2.	Правила разграничения доступа субъектов доступа к объектам доступа информационной системы ЕГИСЗ ЛО.	п.15.1, 16.3 [7]
3.	Документ об определении лиц, ответственных за выявление инцидентов и реагирование на них	п.18.1 [7]
4.	Документ об определении лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ЕГИСЗ ЛО и ее системы защиты информации.	п.18.4 [7]
5.	Журнал учета СКЗИ ЕГИСЗ ЛО, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	п.26, 27 [6]
6.	Перечень пользователей СКЗИ ЕГИСЗ ЛО	п.19 [6]
7.	Заключение о возможности эксплуатации СКЗИ ЕГИСЗ ЛО	п.7 [6]
8.	Заключение по обучению пользователей ЕГИСЗ ЛО правилам работы с СКЗИ	п.21 [6]
9.	Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	п.13 [3]
10.	Документ об определении лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ ЕГИСЗ ЛО, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.	п.6 [5], п.63 [6]
11.	Правила доступа в помещения, где размещены используемые СКЗИ ЕГИСЗ ЛО, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях.	п.6 [5], п.63 [6]
12.	Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров	п. 7.б [5]
13.	Журнал осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных	ст. 18.1, п. 1.4 [2]
14.	Журнал контроля за соблюдением условий использования СКЗИ	п. 7 [6]

[1] []- обозначение нормативного документа, указанного в Таблице 1, на основании которого разрабатывается организационно-распорядительный документ.