

**Общие меры по защите информации  
в государственных информационных системах Ленинградской области,  
не содержащих информации ограниченного доступа**

## 1 Общие положения

Перечень документов, на основании которых выполняются мероприятия по информационной безопасности в государственных информационных системах Ленинградской области, не содержащих информации ограниченного доступа (ГИС 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 Составы 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 Составы 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**

Средства защиты информации (СЗИ), применяемые в ГИС ЛО, должны иметь сертификаты соответствия требованиям по безопасности информации, подтверждающим возможность их применения в государственных информационных системах не ниже 3 класса защищенности (КЗ).

В составе Системы ЗИ ГИС 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 6 класса («Требования к межсетевым экранам» Утверждены приказом ФСТЭК России от 9 февраля 2016 г. №9, ДСП);

- средства защиты информации от несанкционированного доступа;

- средства криптографической защиты информации не ниже класса КС1.

В качестве средств криптографической защиты информации при удалённом взаимодействии пользователей с ГИС 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 ГИС ЛО необходимо:

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

- обеспечить сохранности носителей информации ограниченного доступа ГИС 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 ГИС 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 ГИС 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 ГИС ЛО.	п.9 [7] <sup>1</sup> , п.7 [4]
2.	Документ об определении лиц, ответственных за выявление инцидентов и реагирование на них	п.18.1 [7]

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

3.	Журнал учета СКЗИ ГИС ЛО, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	п.26, 27 [6]
4.	Перечень пользователей СКЗИ ГИС ЛО	п.19 [6]
5.	Заключение о возможности эксплуатации СКЗИ ГИС ЛО	п.7 [6]
6.	Заключение по обучению пользователей ГИС ЛО правилам работы с СКЗИ	п.21 [6]
7.	Документ об определении лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ ГИС ЛО, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.	п.6 [5], п.63 [6]
8.	Правила доступа в помещения, где размещены используемые СКЗИ ГИС ЛО, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нестандартных ситуациях.	п.6 [5], п.63 [6]
9.	Журнал контроля за соблюдением условий использования СКЗИ	п. 7 [6]