КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

«__» марта 2022 года 15.03.2022 № 22-ОРД-22/2022

Об утверждении мер защиты информации в государственной информационной системе Ленинградской области «Единая информационная система учёта граждан, проживающих в Ленинградской области, нуждающихся в улучшении жилищных условий»

В соответствии с пунктом 3.12 Положения о Комитете цифрового развития Ленинградской области, утвержденного постановлением Правительства Ленинградской области от 5 августа 2019 года № 364 «Об утверждении Положения о Комитете цифрового развития Ленинградской области и о признании утратившими силу полностью или частично отдельных постановлений Правительства Ленинградской области»:

1. Утвердить перечень мер защиты информации в государственной информационной системе Ленинградской области «Единая информационная система учёта граждан, проживающих в Ленинградской области, нуждающихся в улучшении жилищных условий» согласно приложению к настоящему распоряжению.

2. Контроль исполнения настоящего распоряжения возложить на первого заместителя председателя Комитета цифрового развития Ленинградской области - начальника департамента информационной безопасности и инфраструктуры.

Председатель Комитета цифрового развития Ленинградской области

Подлинник электронного документа, подписанного ЭП, хранится в Межведомственной системе электронного документооборота Правительства Ленинградской области

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 7993F4FEBA48D4AF3E375CDF3F8C8EE6D09A
Владелец: Сытник Андрей Сергеевич
Действителен с 15-12-2021 до 15-03-2023

А.С.Сытник

Утверждены
Распоряжением Комитета
цифрового развития
Ленинградской области
от __.__.__ № _____

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ
в государственной информационной системе Ленинградской области «Единая информационная система учёта граждан, проживающих в Ленинградской области, нуждающихся в улучшении жилищных условий»

Санкт-Петербург
2022

1. Общие положения

Государственная информационная система Ленинградской области «Единая информационная система учёта граждан, проживающих в Ленинградской области, нуждающихся в улучшении жилищных условий» (далее – ГИС ЛО «Жилье») является государственной информационной системой, обрабатывающей персональные данные.

ГИС ЛО «Жилье» имеет 3 класс защищенности, 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», и 4 уровень защищенности персональных данных в соответствии с п.п.б, п.12 Постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Перечень документов, на основании которых выполняются мероприятия по информационной безопасности в ГИС ЛО «Жилье» приведён в таблице 1.

Таблица 1

Наименование документа
Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»
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»
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»
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»
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»
Приказ ФСТЭК России от 11 февраля 2013 № 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах
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

2. Организационные мероприятия по защите информации

Организационными мерами по обеспечению безопасности ГИС ЛО «Жилье» являются:

- определение лиц, ответственных за информационную безопасность, администраторов информационной безопасности, администраторов;
- регламентация правил доступа к техническим средствам и средствам информационной безопасности;
- обеспечение режима безопасности помещений, в которых размещена система;
- обеспечение сохранности носителей информации;
- разграничение доступа к данным;
- определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;
- учет средств защиты информации;
- обучение специалистов, ответственных за информационную безопасность и пользователей;
- информирование пользователей об актуальных угрозах безопасности;
- определение порядка проведения внутренних контрольных мероприятий.

3. Требования к применяемым средствам защиты информации

В качестве технических мер для управления защитой и обеспечения безопасности ГИС ЛО «Жилье» необходимо реализовать:

- 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;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

4. Требования к типовым автоматизированным рабочим местам, подключаемым к ГИС ЛО «Жилье»

Автоматизированные рабочие места, подключаемые к ГИС ЛО «Жилье», должны быть аттестованы в соответствии с требованиями к защите информации.

Организационные меры при работе с ГИС ЛО «Жилье» определяются организационно-распорядительными документами, приведенными в Таблице 2.

Таблица 2

Приказ о назначении должностного лица (структурного подразделения), ответственного за защиту информации в информационной системе	п. 14. Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" п. 16 Приказа ФСБ России от 10.07.2014 N 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" п. 9 Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	п. 13 Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" п. 8 Приказа ФСБ России от 10.07.2014 N 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" п.16.3, раздел II Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Документ определение лиц, ответственных за выявление инцидентов и реагирование на них	п.п.6, п. 2, ст.19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Документ определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации	п.18.3, Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Правила доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях	п. 13 Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" п. 6 Приказа ФСБ России от 10.07.2014 N 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"
Перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ	п. 6 Приказа ФСБ России от 10.07.2014 N 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"
Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных	пп.8, п.2, ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" п. 8.2 Приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
Определение границ контролируемой зоны	п. 10 Приказа ФСБ России от 10.07.2014 N 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" ЗИС.3 Приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров	п. 7 Приказа ФСБ России от 10.07.2014 N 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" ЗНИ.1 Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" ст.19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Инструкция по порядку учета и хранению и уничтожения носителей конфиденциальной информации (персональных данных)	ст.19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152 «О персональных данных»	п. 2 ст 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" п. 17 Постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
Правила разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения	п. 15.1 Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" п. 16.3 Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Правила генерации и смены паролей пользователей	АНЗ.5 Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Журнал учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	п. 26 Приказа ФАПСИ от 13.06.2001 N 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"
Перечень пользователей СКЗИ	п. 19 Приказа ФАПСИ от 13.06.2001 N 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"
Заключение о возможности эксплуатации СКЗИ	п. 7 Приказа ФАПСИ от 13.06.2001 N 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"
Заключение об обучении пользователей правилам работы с СКЗИ	п. 21 Приказа ФАПСИ от 13.06.2001 N 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"
Инструкция о порядке резервирования и восстановления	п.п.7, п. 2, ст.19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
План мероприятий по защите информации в Системе	п.18.1, раздел II Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Приказ о назначении ответственного за организацию обработки персональных данных в ИС	Ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Должностная инструкция ответственного за организацию обработки персональных данных в ИС	с т.22.1 ФЗ-152 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Правила рассмотрения запросов субъектов персональных данных или их представителей	ст.20 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"

Порядок доступа в помещения, в которых ведется обработка конфиденциальной информации ИС	п.20.12, раздел II Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Приказ об организации режима обеспечения безопасности помещений, в которых размещена ИС	п.20.12, раздел II Приказа ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Политика оператора в отношении обработки персональных данных	ст.18.1 ФЗ-152 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"

Средства защиты информации, применяемые в ГИС ЛО «Жилье», должны иметь сертификаты соответствия требованиям по безопасности информации, подтверждающим возможность их применения в государственных информационных системах не ниже 3 класса защищенности (К3).

На типовых рабочих местах, подключаемых к ГИС ЛО «Жилье», должны применяться:

- средства вычислительной техники не ниже 5 класса, средства защиты информации не ниже 6 класса и 6 уровня доверия;
- средства антивирусной защиты не ниже 4 класса («Требования к средствам антивирусной защиты» Утверждены приказом ФСТЭК России от 20 марта 2012 № 28 ДСП);
- средства защиты информации от несанкционированного доступа;
- межсетевые экраны не ниже 6 класса, соответствующие 6 или более высокому уровню доверия («Требования к межсетевым экранам», утверждены приказом ФСТЭК России от 9 февраля 2016 г. №9, ДСП);
- средства криптографической защиты информации не ниже класса КС1.