

**КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ**

ПРИКАЗ

18 августа 2021 года

№ 16

**Об утверждении Правил доступа в помещения,
в которых осуществляется обработка информации ограниченного доступа
в государственных информационных системах Ленинградской области,
информационных системах персональных данных, размещены используемые
для ее защиты СКЗИ, хранятся СКЗИ и (или) носители ключевой,
аутентифицирующей и парольной информации СКЗИ,
в рабочее и нерабочее время, а также в нештатных ситуациях
и признании утратившим силу приказа Комитета цифрового развития
Ленинградской области**

В соответствии с п. 2.11, 2.12, 2.13 Положения о Комитете цифрового развития Ленинградской области, утвержденного постановлением Правительства Ленинградской области 05 августа 2019 года № 364, п. 4.2 Порядка взаимодействия органов исполнительной власти Ленинградской области при создании, модернизации и развитии государственных информационных систем Ленинградской области, утвержденного постановлением Правительства Ленинградской области от 20 июня 2019 года № 287, п. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, п. 6 Состав 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, утвержденного Приказом ФСБ России от 10 июля 2014 года №378

п р и к а з ы в а ю

1. Утвердить Правила доступа в помещения, в которых осуществляется обработка информации ограниченного доступа в государственных информационных системах Ленинградской области, информационных системах персональных данных, размещены используемые для ее защиты средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях согласно приложению 1.

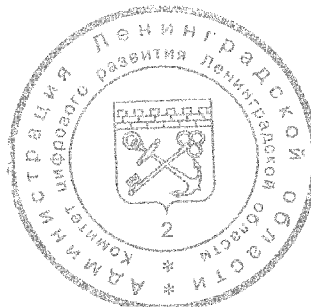
2. Утвердить форму Перечня лиц, имеющих право доступа в помещения, в которых осуществляется обработка информации ограниченного доступа в государственных информационных системах Ленинградской области, информационных системах персональных данных, размещены используемые для ее защиты СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ согласно приложению 2.

3. Признать утратившим силу приказ Комитета цифрового развития от 26 августа 2020 года № 17 «Об утверждении Правил доступа в помещения, где размещены информационные системы персональных данных, размещены и используются средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях».

4. Довести настоящий приказ до работников органов исполнительной власти Ленинградской области.

5. Контроль исполнения настоящего приказа возложить на первого заместителя председателя Комитета – начальника департамента информационной безопасности и инфраструктуры.

Первый заместитель председателя
Комитета цифрового развития
Ленинградской области



А.Ю. Попов

УТВЕРЖДЕНЫ
приказом Комитета цифрового
развития Ленинградской области
от 18 августа 2021 года № 16

(Приложение 1)

ПРАВИЛА

доступа в помещения, в которых осуществляется обработка информации
ограниченного доступа в государственных информационных системах
Ленинградской области, информационных системах персональных данных,
размещены используемые для ее защиты СКЗИ, хранятся СКЗИ
и (или) носители ключевой, аутентифицирующей и парольной информации
СКЗИ, в рабочее и нерабочее время,
а также в нештатных ситуациях

1. Общие положения

1.1 Настоящие правила разработаны в целях обеспечения безопасности защищаемой информации при ее обработке в государственных информационных системах Ленинградской области, информационных системах персональных данных.

1.2. Настоящие правила устанавливают требования к помещениям органов исполнительной власти Ленинградской области, в которых осуществляется обработка информации ограниченного доступа в государственных информационных системах Ленинградской области, информационных системах персональных данных, размещены используемые для ее защиты средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – специальные помещения), и порядок доступа в них.

1.3. Соблюдение настоящих правил обязательно для работников органов исполнительной власти Ленинградской области (далее – ОИВ ЛО) и прочих лиц,

которым для исполнения служебных обязанностей необходим доступ в специальные помещения.

2. Требования к специальным помещениям

2.1. Специальные помещения должны находиться в пределах контролируемой зоны, границами которой являются: периметр охраняемой территории зданий, ограждающие конструкции охраняемых зданий, охраняемых частей зданий или помещений.

2.2. Двери специальных помещений должны быть оборудованы механическими или электронными замками, обеспечивающими их надёжное запираение.

3. Порядок доступа в специальные помещения

3.1. Доступ в помещения в рабочее (служебное) время имеют работники ОИВ ЛО, включенные в Перечень лиц, имеющих право доступа в помещения, в которых осуществляется обработка информации ограниченного доступа в государственных информационных системах Ленинградской области, информационных системах персональных данных, размещены используемые для ее защиты СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

3.2. В нерабочее (неслужебное) время пребывание в помещениях работников, указанных в п. 3.1 Правил, осуществляется в порядке, установленном действующими правовыми актами, регламентирующими пропускной режим в зданиях, занимаемых ОИВ ЛО.

3.3. Нахождение в специальных помещениях прочих работников ОИВ ЛО в рабочее (служебное) и нерабочее (неслужебное) время в отсутствии лиц, обладающих правом доступа в такие помещения, запрещается.

3.4. Работники, обладающие правом доступа в служебные помещения, при оставлении помещений обязаны закрывать двери и запирают их на замки.

3.5. Вскрытие, закрытие (опечатывание) служебных помещений, производится работниками, имеющими право доступа в специальные помещения.

3.6. При вскрытии специальных помещений, работники, имеющие право доступа в такие помещения, обязаны провести предварительный внешний осмотр с целью установления целостности дверей и замков, и, после открытия дверей, внутренний осмотр с целью проверки наличия и целостности оборудования, имеющихся печатей (пломб).

3.7. При обнаружении неисправностей дверей и запирающих устройств работники обязаны:

- не вскрывая помещение доложить о них непосредственному руководителю;
- в присутствии не менее, чем двух других работников вскрыть помещение и осмотреть его;
- составить акт вскрытия помещения, содержащий сведения о дате и времени вскрытия, обстоятельствах, повлекших его, лицах, производивших вскрытие, о выявленных при осмотре нарушениях, и передать его руководителю для организации служебного расследования.

3.8. В нештатных ситуациях, в случае необходимости принятия в рабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещения, иных аналогичных случаях, необходимо руководствоваться установленными правилами пожарной безопасности и иными правилами обеспечения безопасности жизнедеятельности. При этом по возможности работниками, осуществляющими работу в данном помещении, организуется контроль допуска в данные помещения обслуживающего или иного персонала.

3.9. В нештатных ситуациях, в случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещения, иных аналогичных случаях, вскрытие служебного помещения осуществляется сотрудником службы безопасности в соответствии с действующим режимом охраны помещений.

3.10. Работники, обладающие правом доступа в специальное помещение, прибывшие после нейтрализации нештатных ситуаций, обязаны выполнить мероприятия, указанные в пункте 3.7 настоящих правил.

3.11. Ответственность за соблюдение настоящих правил возлагается на руководителей структурных подразделений и работников, обладающих правом доступа в помещения.

УТВЕРЖДЕНА
приказом Комитета
цифрового развития
Ленинградской области
от 18 августа 2021 года № 16

(Приложение 2)

ФОРМА

УТВЕРЖДАЮ
Руководитель ОИВ ЛО

_____ ФИО

«__» _____» 202 г.

ПЕРЕЧЕНЬ

лиц, имеющих право доступа в помещения, в которых осуществляется обработка информации в государственных информационных системах Ленинградской области, информационных системах персональных данных, размещены используемые для ее защиты СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

№ п/п	Должность	Ф.И.О.	Кабинет, адрес помещения

Ответственный за защиту информации
в органе исполнительной власти
Ленинградской области

ФИО