КОМИТЕТ
ПО СВЯЗИ И ИНФОРМАТИЗАЦИИ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

20 апреля 2017 года № 13

Об утверждении типовых организационно-распорядительных документов по защите информации, не содержащей сведения, составляющие государственную тайну

В целях обеспечения выполнения органами исполнительной власти Ленинградской области требований по защите информации, установленных в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 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», приказом 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», устанавливающими требования к защите информации, не содержащей сведения, составляющие государственную тайну, в соответствии с Положением о Комитете по связи и информатизации Ленинградской области, утвержденным постановлением Правительства Ленинградской области от 3 июня 2015 года № 193,

п р и к а з ы в а ю:

Утвердить типовые организационно-распорядительные документы по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну:

1) Перечень должностных лиц, имеющих право доступа к информационным ресурсам в органе исполнительной власти Ленинградской области, согласно Приложению 1.

2) Порядок допуска в служебные помещения и к техническим средствам органа исполнительной власти Ленинградской области, в рабочее и нерабочее время, а также в нештатных ситуациях (далее – Порядок), согласно Приложению 2.

3) Перечень пользователей средств криптографической защиты информации в органе исполнительной власти Ленинградской области, согласно Приложению 3.

4) Порядок учета, хранения и уничтожения машинных носителей информации в органе исполнительной власти Ленинградской области, согласно Приложению 4.

5) Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в органе исполнительной власти Ленинградской области (для обладателя конфиденциальной информации), согласно Приложению 5.

Председатель Комитета
по связи и информатизации
Ленинградской области А. Шорников

Приложение № 1
к приказу Комитета по связи
и информатизации Ленинградской области
от 20 апреля 2017 года № 13

УТВЕРЖДАЮ

Руководитель органа
исполнительной власти
Ленинградской области
«___»_____ _____ г.

_____ _____

Перечень должностных лиц, имеющих право доступа к информационным ресурсам в органе исполнительной власти Ленинградской области

Наименование должности	Перечень информационных ресурсов, к которым необходим доступ
Наименование подразделения	
	* - информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну; - общедоступная информация

* Указывается информационная система или конкретный информационный ресурс, к которому предоставляется доступ.

«___» _____ _____ г.

_____
(подпись исполнителя)

Приложение 2
к приказу Комитета по связи
и информатизации Ленинградской области
от 20 апреля 2017 года № 13

УТВЕРЖДАЮ

Руководитель органа
исполнительной власти
Ленинградской области
«___»_____ _____ г.

_____ _____

Порядок допуска в служебные помещения и к техническим средствам органа исполнительной власти Ленинградской области, в рабочее и нерабочее время, а также в нештатных ситуациях

1. Настоящий порядок, устанавливает требования к допуску должностных лиц и обслуживающего персонала в служебные помещения и к техническим средствам органа исполнительной власти Ленинградской области.

2. Для служебных помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки и защиты информации, препятствующий возможности неконтролируемого проникновения или пребывания посторонних лиц, не имеющих право доступа в такие помещения.

3. При обработке в служебных помещениях, информации ограниченного доступа, содержащейся в государственных информационных системах, обеспечиваются контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования (далее - защищаемые объекты), а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к защищаемым объектам и в помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом предусматривают:

а) определение лиц, допущенных к защищаемым объектам, а также в помещения и сооружения, в которых они установлены (Приложение № 1);

б) санкционирование физического доступа к защищаемым объектам, а также в помещения и сооружения, в которых они установлены;

4. В служебных помещениях, в которых размещаются компоненты информационных систем персональных данных (далее – ИСПДн) и используемые или находящиеся на хранении средства криптографической защиты информации (далее - СКЗИ), документация на СКЗИ, носители ключевой, аутентифицирующей и парольной информации СКЗИ обеспечивается режим безопасности, который достигается путем:

а) оснащения таких помещений входными дверьми с замками, обеспечения постоянного закрытия дверей на замок и их открытия только для санкционированного
прохода;

б) утверждения перечня лиц, имеющих право доступа в такие помещения (Приложение № 1).

5. Лица, не имеющие право доступа в служебные помещения, допускаются в такие помещения в присутствии должностных лиц, имеющих право доступа в служебные помещения.

6. Служебные помещения располагаются в пределах контролируемой зоны, границами которой являются ограждающие конструкции здания, в котором они размещены, с учётом контролируемых территорий.

7. Вскрытие и закрытие (опечатывание) служебных помещений, производится должностными лицами, имеющими право доступа в данные помещения.

8. В рабочее время, должностным лицам, имеющим право доступа в служебные помещения, запрещено:

оставлять в свое отсутствие незапертым служебное помещение;

оставлять в служебном помещении посторонних лиц, не имеющих право доступа в такое помещение, без присмотра.

9. По окончании работы все технические средства выключаются.

10. Перед открытием помещений, работник, имеющий право доступа в помещения, обязан: провести внешний осмотр с целью установления целостности печатей (пломб), дверей и замков.

При обнаружении нарушения целостности печатей (пломб), дверей или запирающих устройств служебного помещения, работник обязан:

не вскрывая помещение, доложить о ситуации непосредственному руководителю;

в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

составить акт о выявленных нарушениях и передать его руководителю для организации служебного расследования.

11. Обслуживание и сопровождение технических и программных средств, уборка, проведение иных аналогичных работ в служебных помещениях осуществляются в присутствии должностного лица, имеющего право доступа в данное помещение.

12. 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 действия работников осуществляются в соответствии с установленными правилами пожарной безопасности и иными правилами обеспечения безопасности жизнедеятельности. При этом работниками, находящимися в данном помещении, по возможности осуществляется контроль допуска в данные помещения обслуживающего или иного персонала.

13. 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 помещение, иных аналогичных случаях, вскрытие служебного помещения осуществляется сотрудником службы безопасности.

14. По прибытии работников в служебное помещение после нейтрализации нештатных ситуаций, необходимо выполнить мероприятия, указанные в пункте 10 настоящего регламента.

15. Ответственность за соблюдение настоящего порядка возлагается на должностных лиц имеющих право доступа в служебные помещения, в которых ведется обработка информации.

Приложение № 1
к Порядку

УТВЕРЖДАЮ
Руководитель органа
исполнительной власти
Ленинградской области
«___»_____ _____ г.

_____ _____

Перечень лиц, имеющих право доступа в служебные помещения органа исполнительной власти Ленинградской области

№	Должность	Ф.И.О.	№ помещения

«___» _____ _____ г.

_____
(подпись исполнителя)

Приложение 3
к приказу Комитета по связи
и информатизации Ленинградской области
от 20 апреля 2017 года № 13

УТВЕРЖДАЮ

Руководитель органа
исполнительной власти
Ленинградской области

«___»_____ _____ г.

_____ _____

Перечень пользователей средств криптографической защиты информации
в органе исполнительной власти Ленинградской области

п/п	ФИО пользователя

«___» _____ _____ г.

_____

(подпись исполнителя)

Приложение № 4
к приказу Комитета по связи
и информатизации Ленинградской области
от 20 апреля 2017 года № 13

УТВЕРЖДАЮ

Руководитель органа
исполнительной власти
Ленинградской области
«___»_____ _____ г.

_____ _____

Порядок учета, хранения и уничтожения машинных носителей информации в органе исполнительной власти Ленинградской области

1. Общие положения

1.1. Настоящий порядок, определяет правила учёта, маркировки, хранения, передачи другим лицам, осуществления ремонта, технического обслуживания и уничтожения машинных носителей информации в органе исполнительной власти Ленинградской области.

2. Машинные носители информации

2.1. Машинные носители информации – изделия и устройства, предназначенные для записи и обработки информации, входящие в состав средств вычислительной техники (СВТ), а также для хранения и перемещения записанной информации на машинные носители информации.

2.2. Виды МНИ:

- жесткие магнитные диски;
- гибкие магнитные диски;
- оптические и магнитооптические диски;
- устройства долговременной электронной памяти «Flash Memory»;

2.3. Типы МНИ:

– отчуждаемые носители информации, – устанавливаются и/или подключаются к СВТ на время сеанса работы, а по его окончанию отключаются и хранятся в специальном хранилище;

– не отчуждаемые носители информации, – в процессе работы не снимаются и не изымаются из состава СВТ и находится там постоянно.

3. Правила обращения с машинными носителями информации

3.1. Действия с МНИ подлежат учету в «Журнале учета машинных носителей информации» (Приложение № 1).

3.2. Ответственность за ведение журнала возлагается на ответственного за защиту информации.

3.3. Выдача МНИ фиксируется в «Журнале учета машинных носителей защищаемой информации» и подтверждается подписью пользователя.

3.4. МНИ должны маркироваться этикетками, содержащими учетный номер, дату ввода в эксплуатацию, наименование органа исполнительной власти Ленинградской области - владельца МНИ.

3.5. МНИ содержащие биометрические персональные данные должны обеспечивать возможность идентифицировать информационную систему персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись.

3.6. Отчуждаемые носители информации маркируются этикеткой, закрепленной на лицевой стороне носителя.

3.7. Не отчуждаемые носители информации учитываются отдельно и (или) в составе СВТ. При этом соответственно маркируется сам носитель или корпус СВТ, в состав которого входит носитель.

3.8. СВТ в состав которого входит МНИ, вскрывается только в присутствии ответственного за защиту информации и должностного лица эксплуатирующего данное СВТ.

4. Правила хранения машинных носителей информации

4.1. При хранении МНИ должны соблюдаться условия, обеспечивающие сохранность информации, и исключающие несанкционированный доступ к ним, хищение, подмену и уничтожение.

4.2. Хранение и использование МНИ должно осуществляться в соответствии с техническими условиями изготовителя. Не допускается превышение срока эксплуатации, установленного изготовителем МНИ.

4.3. Необходимо обеспечивать раздельное хранение материальных носителей персональных данных, обработка которых осуществляется в различных целях, а также носителей персональных данных от носителей, содержащих иную защищаемую информацию.

4.4. Для хранения МНИ используются хранилища (сейфы, металлические шкафы, и т.п.), оборудованные внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съемном МНИ хранятся данные в зашифрованном с использованием средств криптографической защиты информации (СКЗИ) виде, допускается хранение таких носителей в служебных помещениях вне сейфов (металлических шкафов).

4.5. МНИ с резервными копиями информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного МНИ.

МНИ с резервными копиями рекомендуется хранить в отдельном хранилище.

4.6. В случае если на основании договора хранение носителей поручено другому лицу, существенным условием такого договора является обязанность обеспечения таким лицом безопасности переданной ему информации.

5. Порядок уничтожения носителей защищаемой информации

5.1. МНИ подлежат уничтожению в следующих случаях:

– достижения целей обработки информации или утраты необходимости в их достижении, для носителей, уничтожение информации на которых невозможно без уничтожения самого носителя;

– выхода из строя, повреждение МНИ, в результате которого невозможно осуществлять корректную обработку информации с использованием данного носителя;

– возникновения иных обстоятельств, в результате которых необходимо уничтожить носители, содержащие информацию.

5.2. Уничтожение осуществляется ответственным за защиту информации, с составлением акта об уничтожении МНИ, который подлежит хранению в течение пяти лет.

5.3. Вышедшие из строя МНИ ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.

5.4. Уничтожение МНИ должно обеспечивать полное физическое и невосстановимое уничтожение содержащейся на них информации.

6. Права и обязанности работников при обращении с носителями защищаемой информации

6.1. Запрещается выносить носители из служебных помещений (за пределы контролируемой зоны) для работы с ними на дому, в гостиницах, общественном транспорте и т.д.

6.2. Право на перемещение МНИ за пределы контролируемой зоны предоставлено только тем лицам, которым оно необходимо для выполнения должностных обязанностей (функции).

6.3. Лицам, осуществляющим работу с МНИ, разрешено работать только с МНИ, переданным им в соответствии с настоящим порядком. Запрещается принимать
и передавать другим лицам МНИ без соответствующего разрешения и учета в установленном порядке.

6.4. Руководители подразделений, в которых осуществляется работа с МНИ, должны пресекать действия, которые могут привести к хищению или разрушению носителей.

6.5. О факте утраты МНИ немедленно должен быть поставлен в известность ответственный за защиту информации.

Приложение № 1
к Порядку учета, хранения
и уничтожения машинных
носителей информации

Журнал учета машинных носителей информации

Учетный номер или регистрационный номер	Вид (съемный/несъемный)	Тип (оптический /магнитный /flash) и его емкость	Дата поступления	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения (№ помещения)	Дата и номер акта об уничтожении	Примечание
1	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*

Приложение № 5
к приказу Комитета по связи
и информатизации Ленинградской области
от 20 апреля 2017 года № 13

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной

и технической документации к ним, ключевых документов

в органе исполнительной власти Ленинградской области

(для обладателя конфиденциальной информации)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15