ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
« ЛИПЕЦКФАРМАЦИЯ»

П Р И К А З

г.Липецк

«17» марта 2017 г. № 131

Об обеспечении безопасности помещений, в которых ведется обработка персональных данных, располагаются средства криптографической защиты информации, и сохранности материальных носителей информации ограниченного доступа, в том числе с машинных носителей информации в ОГУП «Липецкфармация»

С целью организации работ по обеспечению безопасности помещений, в которых ведется обработка персональных данных, располагаются средства криптографической защиты информации, и сохранности материальных носителей информации ограниченного доступа, в том числе машинных носителей информации в ОГУП «Липецкфармация» для выполнения требований постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа ФСБ России от 10 июля 2014 г. № 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»

ПРИКАЗЫВАЮ:

1. Заведующим аптечными организациями и заведующей аптечным складом:

1.1. Утвердить список лиц, допущенных к работе в помещения, где обрабатываются персональные данные и (или) размещены средства криптографической защиты по прилагаемой форме (Приложение № 1).

1.2. Утвердить перечень мест хранения материальных носителей информации ограниченного доступа, не составляющей государственную тайну по прилагаемой форме (Приложение №2).

1.3. Утвердить Инструкцию по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации (Приложение №3).

2. Утвердить Положение об организации режима безопасности помещений, в которых ведется обработка персональных данных и (или) расположены средства криптографической защиты информации в структурных подразделениях ОГУП «Липецкфармация» (Приложение № 4).

3. Назначить ответственными за порядок и организацию режима безопасности помещений, в которых ведется обработка персональных данных и (или) размещаются средства криптографической защиты информации:

- в управлении ОГУП «Липецфармация» - заместителя генерального директора по общим вопросам – Мочалова В.В.,
- в аптеках – заведующих аптеками,
- на областном аптечном складе – заведующую аптечным складом Гарчеву Е.А.

4. Ответственным за порядок и организацию режима безопасности помещений, в которых ведется обработка персональных данных и (или) размещаются средства криптографической защиты информации:

4.1. Осуществлять поэкземплярный учет материальных носителей информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, путем ведения соответствующего журнала.

4.2. Довести до сотрудников, допущенных к обработке информации ограниченного доступа не составляющей государственную тайну, положения утвержденных организационно-распорядительных документов под роспись.

5. Информацию о выполнении приказа предоставить заместителю генерального директора по общим вопросам Мочалову В.В. в письменной форме к 1 сентября 2017 г.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор В.В. Железняк

Приложение №1
к приказу ОГУП «Липецкфармация»
от «17» марта 2017 г. № 131

СПИСОК
лиц, допущенных к работе, в помещения, где обрабатываются персональные данные и (или) размещены средства криптографической защиты

№ п/п	Кабинет (помещение)	ФИО	Должность

Приложение № 2
к приказу ОГУП «Липецкфармация»
от «17» марта 2017 г. № 131

Перечень мест хранения материальных носителей информации ограниченного доступа, не составляющей государственную тайну

№ п/п	Месторасположение, наименование помещения, подразделение	Документы, содержащие информацию ограниченного доступа, не составляющей государственную тайну	Сотрудники, ответственных за хранение атрибутов доступа к местам хранения

Приложение №3

Утверждена
приказом ОГУП «Липецкфармация»
от «17» марта 2017 г. №131

ИНСТРУКЦИЯ
по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации

1. Общие положения

1.1. Настоящая Инструкция определяет правила хранения и учета материальных носителей информации ограниченного доступа (в том числе персональные данные), включая машинные носители информации в ОГУП «Липецкфармация» (далее – Предприятие).

1.2. Действие настоящей Инструкции распространяется на сотрудников Предприятия, допущенных к обработке информации ограниченного доступа.

2. Порядок хранение материальных носителей информации

2.1. Хранение материальных носителей информации должно происходить в порядке, исключающем их утрату или неправомерное использование.

2.2. При работе с документами, содержащими информацию ограниченного доступа, запрещается оставлять их на рабочем месте или оставлять шкафы (сейфы) с данными документами открытыми (незапертыми) в случае выхода из рабочего помещения.

2.3. По окончании работы с документами, содержащими информацию ограниченного доступа, они незамедлительно должны быть убраны в шкафы (сейфы).

2.4. Личные дела сотрудников, картотеки, учетные журналы и книги учета должны храниться в запирающихся шкафах. Трудовые книжки должны храниться в несгораемом сейфе.

2.5. Хранение ПДн субъектов ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки в соответствии со сроками хранения, определяемыми законодательством Российской Федерации и нормативными документами Предприятия.

2.6. Информация ограниченного доступа на бумажных носителях должна находиться в помещениях Предприятия в сейфах, металлических или запираемых шкафах, обеспечивающих защиту от несанкционированного доступа.

2.7. При уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие информацию ограниченного доступа, лицу, на которое приказом или распоряжением генерального директора Предприятия будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, документы и иные носители, содержащие информацию ограниченного доступа, передаются другому работнику, имеющему доступ к информации ограниченного доступа по указанию руководителя структурного подразделения.

2.8. При увольнении работника, имеющего доступ к информации ограниченного доступа, документы и иные носители, содержащие информацию ограниченного доступа, сдаются работником своему непосредственному руководителю.

2.9. Режим конфиденциальности ПДн снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законом.

2.10. После увольнения работника папка «Личное дело сотрудника» перемещается в архив уволенных работников и хранится в архиве.

3. Порядок учета машинных носителей информации

3.1. Все машинные носители информации, используемые в информационных системах ОГУП «Липецкфармация» для хранения и обработки информации ограниченного доступа должны быть учтены.

3.2. Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

3.3. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

3.4. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации (Приложение 1).

3.5. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

3.6. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

3.7. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

3.8. Маркировка машинных носителей информации (технических средств), дополнительно должна включать в себя информацию о возможности использования машинного носителя информации вне информационной системы.

3.9. Учет машинных носителей информации осуществляется в подразделениях, осуществляющих обработку информации ограниченного доступа (в том числе ПДн).

3.10. Ежегодно необходимо проводить инвентаризацию всех носителей информации, на которых хранится и обрабатывается информация ограниченного доступа. Результаты инвентаризации должны документироваться.

4. Порядок работы с материальными носителями информации ограниченного доступа

4.1. При работе с материальными носителями информации ограниченного доступа необходимо соблюдать требования данной Инструкции.

4.2. При потере или краже материального носителя информации ограниченного доступа незамедлительно ставить в известность руководителя подразделения. Отметки об утрате вносятся в журнал.

4.3. При передаче информации ограниченного доступа необходимо передавать минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

4.4. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы, содержащие сведения ограниченного доступа, изымаются.

4.5. При работе с материальными носителями информации ограниченного доступа запрещается:

- использовать документы, содержащие информацию ограниченного доступа в личных целях;

- передавать документы, содержащие информацию ограниченного доступа, третьим лицам без соответствующего разрешения руководителя подразделения;

- хранить документы, содержащие информацию ограниченного доступа, с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить документы, содержащие информацию ограниченного доступа, из служебных помещений для работы с ними на дому и т. д.

- оставлять документы, содержащие информацию ограниченного доступа, без присмотра.

4.6. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

5. Порядок уничтожения (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

5.1. При передаче машинных носителей информации между пользователями, в сторонние организации для ремонта или утилизации должно обеспечиваться уничтожение (стирание) информации на машинных носителях, а также контроль уничтожения (стирания) информации.

5.2.Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

5.3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

5.4. Процедуры уничтожения информации и контроля осуществляются администратором информационной безопасности с использованием встроенных механизмов средств защиты информации от несанкционированного доступа в соответствии с эксплуатационной документацией на средства защиты информации. Должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

- очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти.

5.5. Действия по удалению защищаемой информации и уничтожению машинных носителей информации должны регистрироваться и контролироваться администратором информационной безопасности.

6. Порядок доступа к машинным носителям информации

6.1. Руководители подразделений, в которых ведется обработка информации ограниченного доступа, определяют должностные лица своего подразделения, имеющие физический доступ к машинным носителям информации, а именно к следующим:

- съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

6.2. Предоставление физического доступа к машинным носителям информации осуществляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

7. Контроль использования интерфейсов ввода (вывода)

7.1. В информационных системах ОГУП «Липецкфармация» разрешено использование интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации исключительно для работы с учтенными машинными носителями информации.

7.2. Доступ к использованию интерфейсов ввода (вывода) информационных систем разрешен лицам, допущенным к данному средству вычислительной техники и администраторам информационных систем (системные и администраторы безопасности).

7.3. Контроль использования интерфейсов ввода (вывода) осуществляется встроенными механизмами средства защиты от несанкционированного доступа.

- Приложение 1. Типовая форма журнала учета машинных носителей

ЖУРНАЛ

учета машинных носителей информации ограниченного доступа

Начат ____._____.2017г.

Ответственный за организацию и обеспечение безопасности ПДн _____

№ п/п	Учётный номер	Тип носителя	Номер (серийный/ инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					ФИО, дата получения, подпись	ФИО, дата сдачи, подпись			
1	2	3	4	5	6	7	8	9	10

Приложение №4

Утверждено

приказом ОГУП «Липецкфармация»

от «17» марта 2017 г. № 131

ПОЛОЖЕНИЕ

об организации режима безопасности помещений, в которых ведется обработка персональных данных и (или) расположены средства криптографической защиты информации в структурных подразделениях ОГУП «Липецкфармация»

- **Общие положения**

Настоящее Положение определяет порядок доступа и правила обеспечения безопасности помещений, в которых обрабатываются персональные данные (ПДн) и (или) размещаются средства криптографической защиты информации (далее – Помещения) в ОГУП «Липецкфармация» (Далее - Предприятие).

- **Перечень помещений, в которых ведется обработка ПДн и /или в которых размещаются средства криптографической защиты информации (СКЗИ)**

Перечень помещений, в которых ведется обработка ПДн и/или размещаются средства криптографической защиты информации (СКЗИ), утверждается руководителем Предприятия отдельно и прикладывается к данному Положению.

- **Правила доступа и обеспечение безопасности помещений, в которых ведется обработка ПДн и (или) размещаются СКЗИ**

Целью организации режима обеспечения безопасности в помещениях обработки ПДн и (или) размещения СКЗИ является обеспечение конфиденциальности ПДн, сохранности носителей ПДн и средств защиты информации (СЗИ, в том числе СКЗИ), обеспечивающих техническую защиту ПДн. Правила обеспечения безопасности помещений должны исключать возможность неконтролируемого проникновения или пребывания в помещениях посторонних лиц.

Для обеспечения безопасности помещений должны выполняться следующие мероприятия и правила безопасности:

- Приказом по Предприятию утверждается уполномоченное лицо, несущее ответственность за порядок и организацию режима безопасности Помещений Предприятия.
- Перечни лиц, имеющих право доступа в Помещения, утверждается руководителем Предприятия (допускается утверждение списков руководителями подразделений по согласованию с ответственным за обеспечение безопасности ПДн).
- Допуск посетителей в Помещения в рабочее время, должен осуществляться по согласованию с руководителем подразделения (отдела), или по распоряжению ответственного за обеспечение безопасности ПДн на Предприятии.
- Запрещается нахождение в Помещениях посторонних лиц, не имеющих полномочий по доступу к ПДн и (или) к СКЗИ, без сотрудника, допущенного к работе в Помещение соответствующим приказом руководителя Предприятия.
- В рабочее время, в случае ухода всех сотрудников, или в нерабочее время, Помещения должны закрываться на ключ.
- Нахождение сотрудников в нерабочее время должны быть согласованы с руководителями подразделений.
- Нахождение посетителей в нерабочее время в Помещениях запрещено.
- Должны выполняться все предписания на эксплуатацию СКЗИ, средства связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении, где происходит обработка ПДн.
- Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.
- Выносить технические средства обработки ПДн за пределы контролируемой зоны Предприятия с целью их ремонта, замены и т. п. без согласования с ответственным за обеспечение безопасности персональных данных запрещено.
- Входные двери Помещений должны быть оснащены замками, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

- Мониторы технических средств обработки ПДн должны быть размещены таким образом, чтобы исключалась возможность случайного или преднамеренного визуального просмотра отображаемой на них информации посторонними лицами.

- **Ответственность за режим безопасности**

Ответственность за режим безопасности в Помещениях отдела (подразделения) и правильность использования установленных в нем технических средств, в том числе средств защиты информации, несет руководитель подразделения, а также ответственный за обеспечение безопасности ПДн на Предприятии, уполномоченный на то соответствующим приказом.

Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением или ответственным за обеспечение безопасности ПДн в ОГУП «Липецкфармация».

Приложение №1

**Перечень помещений ОГУП «Липецкфармация»
по адресу: г. Липецк, ул.Гагарина, д.113,
в которых ведется обработка персональных данных**

В ОГУП «Липецкфармация» осуществляется обработка ПДн и располагаются СКЗИ в следующих помещениях:

- кабинет № 9 (главная бухгалтерия) – АРМ ИС «Льгота»;
- кабинет № 10 (отдел льготного обеспечения) – АРМ ИС «Льгота».