Приложение №2
к приказу № 38-О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

Обязательство
о неразглашении персональных данных работников
ГУЗ "Липецкая ГБ № 4 "Липецк-Мед"

г Липецк «.....».....20...г.

Я,_____
(фамилия, имя, отчество работника - полностью)
_____
_____
(должность, наименование структурного подразделения)

предупрежден (а), что на период исполнения трудовой функции, предусмотренной соответствующим трудовым договором, мне будет предоставлен допуск к персональным данным работников, а также к персональным данным, содержащимся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

Настоящим я добровольно принимаю на себя следующие обязательства:

1. Не разглашать третьим лицам персональные данные работников, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам персональные данные работников, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня персональные данные работников, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, сообщать непосредственному начальнику.

4. Не использовать персональные данные работников, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, с целью извлечения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

6. После прекращения права на допуск к персональным данным работников, а также к персональным данным, содержащимся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, не разглашать и не передавать третьим лицам известные мне персональные данные.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности, предусмотренной законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись работника)

Приложение №3
к приказу № 38 -О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

Обязательство
о неразглашении персональных данных пациентов
ГУЗ "Липецкая ГБ № 4 "Липецк-Мед"

г. Липецк «.....».....20...г.

Я,_____
(фамилия, имя, отчество работника - полностью)

_____

_____
(должность, наименование структурного подразделения)

предупрежден (а), что на период исполнения трудовой функции, предусмотренной соответствующим трудовым договором, мне будет предоставлен допуск к персональным данным пациентов, а также к персональным данным, содержащимся в документах, полученных из других организаций (лечебных учреждений), в обращениях родственников(законного представителя) и иных субъектов персональных данных.

Настоящим я добровольно принимаю на себя следующие обязательства:

1. Не разглашать третьим лицам персональные данные о пациентах, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных о пациентах, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам персональные данные пациентов, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных о пациентах, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня персональные данные пациентов, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных о пациентах, сообщать непосредственному руководителю.

4. Не использовать персональные данные пациентов, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных о пациентах, с целью извлечения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных пациентов (врачебная тайна ст. 13 «Соблюдение врачебной тайны», ФЗ от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в РФ»).

6. После прекращения права на допуск к персональным данным пациентов, а также к персональным данным, содержащимся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных о пациентах, не разглашать и не передавать третьим лицам известные мне персональные данные.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности, предусмотренной законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись работника)

Приложение №4
к приказу № 38 -О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

_____
(наименование должности, инициалы, фамилия руководителя)

_____

от _____
(фамилия, имя, отчество заявителя)

_____
паспорт, серия, номер _____
кем выдан _____
адрес _____
телефон _____

Заявление.

Я, _____,
даю свое согласие на сбор, обработку, накопление, хранение и другое использование своих
персональных данных:
- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- ИНН;
- номер пенсионного страхового свидетельства;
- адрес прописки и проживания, номер телефона, личный e-mail;
- семейное, социальное положение;
- образование;
- специальность (профессия);
- отношение к воинской обязанности;
- доходы, полученные мной в ГУЗ "Липецкая ГБ № 4 "Липецк-Мед",
а также для передачи своих персональных данных: в налоговую инспекцию - по форме 2-НДФЛ, в Пенсионный Фонд Российской Федерации - индивидуальные сведения о начисленных страховых взносах на обязательное пенсионное страхование и данных о трудовом стаже; в страховые медицинские компании; в военный комиссариат, согласно прописки- для выполнения мероприятий по вопросам воинского учета. Передача персональных данных разрешается на срок действия трудового договора.

Подтверждаю, что ознакомлен (а) с Положения об обработке и защите персональных данных работников и пациентов ГУЗ "Липецкая ГБ № 4 "Липецк-Мед"

Права и обязанности в области защиты персональных данных мне разъяснены.

_____	_____	_____
(дата)	(подпись)	(Ф.И.О.)

Приложение №5
к приказу № 38 -О от 27.01 .2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

Государственное учреждение здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

ИНФОРМИРОВАННОЕ СОГЛАСИЕ
на выполнение инвазивного исследования,
вмешательства, операции
«____» _____ 20____г.

Настоящее добровольное согласие составлено в соответствии с Федеральным законом от 21.11.2011г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации

1. Мне _____
(ф.и.о. пациента или его законного представителя)
Разъяснены состояние моего здоровья и характер необходимых диагностических и лечебных мероприятий.

2. Настоящим я доверяю Врачу (в дальнейшем Врач) _____
и его коллегам выполнить следующие инвазивные исследования, вмешательства, операции
_____
_____
_____

3. Содержание указанных выше медицинских действий, связанный с ними риск, возможные осложнения и последствия, включая нетрудоспособность и неблагоприятный исход, мне известны. Я хорошо понял(а) все разъяснения врача.

4. Я понимаю, что в ходе выполнения указанных выше медицинских действий может возникнуть необходимость выполнения другого вмешательства; исследования или операции, не указанных в п.2. Я доверяю Врачу и его ассистентам принять соответствующее решение в соответствии с их профессиональным суждением и выполнить любые медицинские действия, которые Врач сочтет необходимым для улучшения моего состояния. Содержание настоящего документа мною прочитано, разъяснено мне Врачом, оно полностью мне понятно, что я и удостоверяю своей подписью.

5. Я согласен(на) на переливание донорской крови и ее компонентов в ходе операции или в послеоперационном периоде, если возникнет такая необходимость.

6. Я разрешаю своему Врачу делать фотографии и видеозаписи, связанные с моим лечебным процессом, и использовать их для научных и образовательных целей.

7. Я подтверждаю свое согласие на обработку моих персональных данных (ф. и. о.), пол,, дату рождения, адрес м/ж, контактные телефоны, реквизиты полиса (ОМС, ДМС), данные о моем состоянии здоровья, заболевания в целях установления медицинского диагноза и оказания мне медицинских услуг при условии, что лица осуществляющие медицинскую деятельность обязаны сохранять врачебную тайну.

Подпись пациента _____

Если пациент не может подписать документ вследствие своего физического состояния или является несовершеннолетним, подпись законного представителя пациента (ближайшего родственника):
Ф., и., о. _____ подпись_____
Ф., и., о. Врача_____ подпись_____
От проведения указанных в п.2 _____
_____
_____ отказываюсь,
_____
что и удостоверяю своей подписью. Мне разъяснены возможные последствия отказа от
_____
а именно поздняя или неправильная диагностика заболевания, нетрудоспособность, смерть.
Пациент (или его законный представитель):
Ф. и. о. _____ подпись_____
Врач: Ф. и. о. _____ подпись_____

Приложение №6
к приказу № 38-О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

1. Общие положения и термины

1.1. Настоящий Регламент устанавливает правила учета и использования программного обеспечения, т.е. программного обеспечения, установленного на компьютеры персонала и включенного в Реестр программного обеспечения (в дальнейшем ПО).
1.2. Реестр ПО - текущий перечень установленных и используемых программ и пакетов программ ПО (включающий в себя наименование программного продукта, тип, в каких подразделениях и на каких компьютерах используется, номера лицензий или лицензионных соглашений, дата приобретения, где приобретен, номера счетов-фактур и накладных, где хранится резервная копия).
1.3. Пользователь ПО – работники учреждения, которым предоставлено право доступа к ПО в соответствии с их должностными обязанностями.
1.4. Ответственные за ПО – работники соответствующих подразделений учреждения, отвечающие в соответствии с настоящим Регламентом за подготовку предложений по приобретению и/или модернизации ПО, установку, обновление, сопровождение ПО, ведение Реестра и контроль выполнения лицензионных требований.
1.5. Правила, указанные в настоящем Регламенте, обязательны для исполнения всеми пользователями ПО.

2. Права и обязанности пользователей

2.1. Пользователи ПО имеют право использовать ПО, установленное в учреждении, в порядке и объемах, определяемых данным Регламентом, и в соответствии с другими нормативными документами, действующими в учреждении (Устав, Положения, приказы, и др.).
2.2. Пользователям запрещается самостоятельно устанавливать какое-либо ПО на компьютеры учреждения, переустанавливать, обновлять или удалять уже установленное на компьютеры учреждения ПО.
2.3. Пользователи учреждения не должны использовать (устанавливать или загружать в память) на компьютерах учреждения без специального разрешения т.н. «бесплатное» и «условно-бесплатное» ПО, т.к. в случае использования в учреждении может быть нарушено авторское право или не выполнены требования лицензии.
2.4. Пользователям учреждения запрещается несанкционированное копирование ПО или иных информационных ресурсов, являющихся собственностью учреждения и и/или защищенных авторским правом.

3. Правила установки и использования ПО

3.1. ПО, используемое в учреждении, делится по характеру своего использования и сопровождения на три группы:
- первая – типовое ПО, установленное на компьютерах в структурных подразделениях учреждения, и включающее в себя операционную систему, офисный пакет, программы, поставляемые в комплекте с периферийным оборудованием, антивирусный пакет, архиваторы, другие вспомогательные программы.
- вторая - ПО, установленное на серверах учреждения.
- третья – специализированные программы и пакеты программ, используемые в профессиональной деятельности структурными подразделениями и сотрудниками

учреждения в соответствии с их функциями и должностными обязанностями (в том числе разработанные в учреждении).

3.2. За подготовку предложений по приобретению и/или модернизации ПО, установку, обновление, сопровождение, ведение Реестра и контроль выполнения лицензионных требований отвечают:

- ПО 1-ой группе – ведущий инженер Панкин Сергей Викторович
  программист Кудинова Ирина Борисовна
- ПО 2-ой группе - ведущий инженер Панкин Сергей Викторович
  программист Кудинова Ирина Борисовна
- ПО 3-ой группе - начальник ИАО Зайцев Алексей Сергеевич

3.3. В обязанность ответственных за ПО также входит обеспечение хранения всей лицензионной документации (лицензионные соглашение, оригиналы дисков, копии платежных документов, руководства пользователя, и т.д.) и резервных копий ПО.

3.4. В случае обнаружения нелицензионного ПО, установленного пользователем, удаления лицензионного ПО, либо нарушения лицензионных требований по лицензионному ПО, ответственный за соответствующее КПО обязан составить докладную записку на имя проректора по ИТДО и принять меры по установлению лица, нарушившего данный Регламент, и по устранению обнаруженных нарушений.

4. Ответственность

4.1. Грубое или систематическое нарушение правил пользования ПО может служить основанием для применения мер по ограничению или лишению прав на использование ПО, наложению дисциплинарных взысканий, вплоть до увольнения, а также привлечения пользователя ПО к ответственности в соответствии с законами Российской Федерации.

Начальник информационно-аналитического отдела А.С. Зайцев

Приложение №7
к приказу № 38-О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

Инструкции
о применении средств антивирусной защиты информации
в ГУЗ "Липецкая ГБ № 4 "Липецк-Мед"

В Инструкции о применении средств антивирусной защиты информации в ГУЗ "Липецкая ГБ № 4 "Липецк-Мед" (далее - Инструкция) использованы следующие термины и определения:
Пользователи - должностные лица, а также все другие лица, использующие в работе средства электронно-вычислительной техники.
Локально-вычислительная сеть (далее - ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными (не арендуемыми) высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.
Антивирусная защита информации - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами информационно-вычислительных ресурсов посредством применения средств антивирусной защиты информации.
Вредоносная программа - программа для электронно-вычислительных машин (ЭВМ), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.
Программные вирусы - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена зараженная программа.

I. Общие положения

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях структурных подразделений учреждения, от несанкционированного копирования, модификации и разрушения персональных данных работников и пациентов, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.
2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в структурных подразделениях учреждения, задачи, обязанности и права ответственных лиц, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, а также порядок ликвидации последствий воздействия программных вирусов.
3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями и ответственными лицами, а также иными лицами, использующими средства вычислительной техники.
4. Ответственный за информационную безопасность и техническую защиту информации осуществляет непосредственное руководство организацией проведения работ и практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в структурных подразделениях учреждения.

II. Порядок применения средств антивирусной защиты информации в учреждении

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в учреждении. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться.
2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:
обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;
внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;
восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.
3. Ответственный за информационную безопасность обеспечивает:
управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты информации;
управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;
ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;
настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;
удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации.
4. Для рабочих станций и серверов, которые не имеют подключения к ЛВС средства антивирусной защиты информации устанавливаются локально.
5. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.
6. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.
7. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов учреждения от их модификации и уничтожения.

III. Порядок обновления баз данных средств антивирусной защиты информации

1. Обновление баз данных средств антивирусной защиты информации на рабочих станциях и серверах с подключенной сетью Internet (Интернет) осуществляется в автоматическом режиме.
2. Для рабочих станций и серверов, которые не имеют подключения к Internet (Интернет) осуществляется через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается
3. Обновление баз данных средств антивирусной защиты информации на рабочих станциях, установленных локально, должно производиться не реже одного раза в

IV. Обязанности, права и порядок назначения ответственных за информационную безопасность.

1. Ответственные за информационную безопасность обязаны обеспечивать соблюдение политики антивирусной защиты информации и выявление фактов заражения программными вирусами в учреждении.

2. К основным задачам ответственных за информационную безопасность относятся организация процесса установки и обновления средств антивирусной защиты информации на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации в учреждении.

3. Ответственный за информационную безопасность учреждения несет ответственность:
за своевременную установку средств антивирусной защиты информации;
за эксплуатацию системы антивирусной защиты информации;
за своевременное обновление лицензий на средства антивирусной защиты информации;
за своевременное обновление баз данных средств антивирусной защиты информации.

4. Ответственный за информационную безопасность имеет право:
вносить предложения по совершенствованию системы антивирусной защиты информации в структурных подразделениях учреждения;
принимать участие в планировании мероприятий по антивирусной защите информации в учреждении и планировании оснащения средствами антивирусной защиты информации структурных подразделений учреждения;
осуществлять контроль состояния средств антивирусной защиты информации в структурных подразделениях учреждения;
проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в структурных подразделениях учреждения;
оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в структурных подразделениях учреждения.

5. Назначение ответственных за информационную безопасность учреждения осуществляется на основании приказа с обязательным отражением обязанностей в должностной инструкции либо должностном регламенте.

V. Обязанности пользователей средств антивирусной
защиты информации

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.

2. Пользователям запрещается:
отключать средства антивирусной защиты информации во время работы;
использовать средства антивирусной защиты информации, отличные от поддерживаемых в учреждении;
без разрешения ответственного за информационную безопасность учреждения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного за информационную безопасность учреждения.

4. В случае появления подозрений на наличие программных вирусов пользователи должны немедленно проинформировать об этом ответственного за информационную безопасность учреждения. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом ответственному за информационную безопасность и техническую защиту информации.

VI. Порядок действий пользователей и ответственного за информационную безопасность

учреждения при обнаружении вирусов
1. Основными путями проникновения вирусов в информационно-вычислительную сеть являются: гибкие магнитные диски, компакт-диски, иные съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в структурные подразделения учреждения, пользователь должен:
приостановить процесс приема-передачи информации;
сообщить ответственному за информационную безопасность учреждения о факте обнаружения программного вируса;
принять по согласованию ответственным за информационную безопасность учреждения меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
сообщить о факте обнаружения программного вируса в структурное подразделение учреждения, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.
2. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:
немедленно приостановить все работы;
сообщить ответственному за информационную безопасность учреждения о факте обнаружения программных вирусов;
принять по согласованию с ответственным за информационную безопасность учреждения меры по удалению программного вируса с использованием средств антивирусной защиты информации.
3. При невозможности ликвидации последствий заражения программными вирусами ответственный за информационную безопасность учреждения должен:
обратиться организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
осуществить полную переустановку программного обеспечения на зараженном компьютере.
4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за информационную безопасность учреждения.
5. Все факты модификации и разрушения данных на серверах или рабочих станциях учреждения, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования.

VII. Ответственность за выполнение требований Инструкции

1. За нарушение настоящей Инструкции ответственный за информационную безопасность учреждения несет ответственность, установленную действующим законодательством Российской Федерации.
2. Начальники структурных подразделений учреждения несут ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными должностными лицами, и за ознакомление их (под роспись) с настоящей Инструкцией в своем структурном подразделении.
3. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих

местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации и получение новых лицензионных ключей, несут пользователи, за которыми закреплены средства вычислительной техники, и ответственный за информационную безопасность учреждения.
4. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность.

VIII. Порядок оснащения учреждения средствами антивирусной защиты информации

1. Оснащение средствами антивирусной защиты информации учреждения является видом материального обеспечения.
2. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.

IX. Порядок информирования о вирусной активности в структурных подразделениях учреждения.
1. Своевременное информирование структурных подразделений учреждения является составной частью системы антивирусной защиты информации.
2. Информирование (распространение предупреждений) о вирусной активности осуществляется централизованно по электронной почте и по телефонам.

Начальник информационно-аналитического отдела А.С. Зайцев

Приложение №
к приказу № 38-О от 27.01.2020
Об утверждении Положения об обработке
и защите персональных данных работников и пациентов
Государственного учреждения здравоохранения
"Липецкая городская больница № 4 "Липецк-Мед"

Журнал регистрации программного обеспечения

Наименование учреждения: **Государственное учреждение здравоохранения "Липецкая городская больница № 4 "Липецк-Мед"**
Составитель: **Зайцев А.С.**
Дата: 20.01.2020

Программный продукт (учетная единица)	Кол-во фактич. копий	Где установлено ПО	Кол-во лицензий в наличии	Недостаток или избыток лицензий	Комментарии
КМИС «Квазар»	222	Поликлиника, стационар, Межмуниципальный акушерско – гинекологический центр			
«Медицинская статистика»	1 4 1 1	программист медицинские статистики отдел кадров планово-экономический отдел			
«Государственный регистр больных сахарным диабетом»	1	каб. электр. вып. рецептов 4 эт			
«Кадры-тарификация»	1 1	отдел кадров программист			
«Картотека»	1 1	картотека взрослой поликлиники программист			
«Родовые сертификаты»	1 1 1	оперативный отдел картотека детской поликлиники Межмуниципальный акушерско – гинекологический центр			
ФРМО/ФРМР	1	отдел кадров			

	1 1 1	машинистка планово-экономический бухгалтерия			
«Регистр детей-инвалидов»	1 1	картотека детской поликлиники программист			
АРМ «Льгота 2.5»	2 1	кабинеты выписки рецептов программист			
АРМ «Флюорография»	1 1	картотека взрослой поликлиники программист			
«1С бухгалтерия»	10	бухгалтерия	10		
«Парус зарплата»	6 1	расчетный отдел бухгалтерии кадры	6		
«2НДФЛ»	1	расчетный отдел бухгалтерии			
«Перечень льготных профессий»	1	отдел кадров			
«Vip Net»	1 1	программист планово-экономический отдел	2		
Сэд-Дело	1	секретарь			
SPU_ORB	1	отдел кадров			
«Свод-Смарт»	1 1 1	бухгалтерия планово-экономический отдел касса			
«OpenOffice»	1	Режимно -секретное подразделение			
«Контур-Экстерн»	1 1 1 1	отдел кадров бухгалтерия расчетный отдел планово-экономический			
«Гарант»	2	юрист			
«ГрандСмета»	1	инженеры	1		
«КриптоПро CSP»	151	поликлиники, стационар, Межмуниципальный акушерско – гинекологический центр	2		
«DrWeb»	100	стационар, поликлиника			
«НалогоплательщикЮЛ»	1	расчетный			