**УТВЕРЖДАЮ:**

Главный врач

ГБУЗ « Ленинградский областной Центр

специализированных видов

медицинской помощи»

Ю.С Егорова

«10» 10 2016 год

# ПОЛОЖЕНИЕ

# ОБ ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

«Государственного бюджетного учреждения здравоохранения Ленинградский областной Центр специализированных видов медицинской помощи»

## 1. Общие положения

1.1.Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в «Государственного бюджетного учреждения здравоохранения Ленинградский областной Центр специализированных видов медицинской помощи» (далее «ГБУЗ ЛенобЦентр»).

1.2. Настоящее Положение утверждается и вводится в действие Приказом Главного врача и является обязательным для исполнения всеми сотрудникам учреждения, имеющими доступ к конфиденциальной информации.

1.3. Должностные лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением под роспись.

1.4. Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.5. Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

1.6. Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке.

1.7. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных

интересов других лиц. *(Федеральный законот 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»).*

1.8.Изменения и дополнения в настоящее Положение вносятся приказом Главного врача «ГБУЗ ЛенобЛЦентр».

## 2. Основные термины и понятия

В настоящем Положении используются следующие основные термины и понятия:

1) *информация* - сведения (сообщения, данные) независимо от формы их представления;

2) *информационные технологии* - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) *информационная система* - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) *информационно-телекоммуникационная сеть* - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) *обладатель информации* - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) *доступ к информации* - возможность получения информации и ее использования;

7) *конфиденциальность информации* - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) *предоставление информации* - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) *распространение информации* - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) *электронное сообщение* - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) *документированная информация* - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) *электронный документ* - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

*(п.1-11.1. введен Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации»)*

## 3. Охраняемые сведения

Объектами защиты в «ГБУЗ ЛенобЦентр» являются:

Средства и системы информатизации и связи (средства вычислительной техники, средства, системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС).

## 4. Организационные и технические мероприятия по технической защите конфиденциальной информации

4.1. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

4.2. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на специалистов допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

4.3. Исключение неконтролируемого доступа к линиям связи.

4.4. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ.

4.5. Техническая защита информации в средствах вычислительной техники (СВТ) от несанкционированного доступа должна обеспечиваться путем выполнения необходимых организационных мер защиты, установки сертифицированных программных и аппаратно-технических средств защиты информации, защиты информации от воздействия программ-закладок и компьютерных вирусов.

4.6. Организация и проведение работ по антивирусной защите информации.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

-установки и применения средств антивирусной защиты информации;

-обновления баз данных средств антивирусной защиты информации;

-действий(уведомление) должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

4.7. Методическое руководство и контроль над организацией работ по антивирусной защите информации и эффективностью предусмотренных мер защиты информации возлагается на специалиста по обслуживанию вычислительной техники.

4.8. К использованию допускается только лицензированные, сертифицированные антивирусные средства.

4.9. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

-Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

-Входной антивирусный контроль всей информации поступающей с электронной почтой;

-Входной антивирусный контроль всей поступающей информации из сети Internet;

-Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

4.10.Периодическая антивирусная проверка на отсутствие компьютерных вирусов на сервере;

4.11.Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ.

4.12.Восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

4.13.Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

4.14. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

4.15. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения компьютеров, входящих в состав локальных компьютерных сетей и сервера.

4.16.Владельцы паролей должны быть ознакомлены и предупреждены об ответственности за парольной информации.

4.17. Формирование личных паролей пользователей осуществляется централизованно. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

## 5. Планирование работ по технической защите конфиденциальной информации и контролю

5.1. В «ГБУЗ ЛенОблЦентр» составляется годовой план работ по технической защите конфиденциальной информации и контролю ответственным сотрудником совместно с подразделениями «ГБУЗ ЛенОблЦентр», выполняющими работы с защищаемой информацией и утверждаются Главным врачом «ГБУЗ ЛенОблЦентр».

5.2. В годовые планы по технической защите конфиденциальной информации и контролю включаются:

-мероприятия по выполнению организаций по вопросам защиты конфиденциальной информации;

-подготовка проектов распорядительных документов по вопросам организации технической защиты информации в «ГБУЗ ЛенОблЦентр», инструкций, рекомендаций, памяток и других

документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах;

-проведение периодического контроля состояния технической защиты информации;

-мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

-мероприятия по совершенствованию технической защиты информации.

5.3. Контроль выполнения планов и отчетность по ним возлагается на ответственного сотрудника.

## 6. Обязанности и права должностных лиц

6.1. Специалист по обслуживанию вычислительной техники организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах.

6.2. Ответственный сотрудник по технической защите конфиденциальной информации осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в «ГБУЗ ЛенобЛЦентр».

6.3. Ответственный сотрудник по технической защите конфиденциальной информации имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

## 7. Защита конфиденциальной информации

7.1. В соответствии с Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации», защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

7.2. Работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих служебных обязанностей, знать какие конкретно сведения подлежат защите, а также строго со блюдать правила пользования ими.

7.3. Ответственный за конфиденциальную информацию, обязан обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

7.4.При увольнении представить письменный отчет Руководителю, либо уполномоченному лицу о документах, содержащих конфиденциальные сведения, которые указанное лицо использовало при исполнении своих трудовых обязанностей, а также передать уполномоченному лицу при прекращении трудовых отношений имеющиеся в пользовании сотрудника материальные и иные носители конфиденциальной информации.

## 8.Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

8.1.В соответствии с Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации», ответственность за правонарушения в сфере информации, информационных технологий и защиты информации наступает:

8.1.1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
8.1.2. По факту разглашения конфиденциальной информации, потери документов и иного несанкционированного доступа к конфиденциальным сведениям, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

**Согласовано:**

_____**Юрисконсульт**

«10» мая **2016года**

*Приложение*

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации

Я, _____,

(ФИО)

в качестве _____

(должность, место работы)

в период трудовых отношений с учреждением «ГБУЗ ЛенОблЦентр» обязуюсь:

1.Не разглашать сведения, составляющие конфиденциальную информацию «ГБУЗ ЛенОблЦентр», которые мне будут доверены или станут известны по работе;

2.Не передавать третьим лицам и не раскрывать публично сведения, составляющие конфиденциальную информацию «ГБУЗ ЛенОблЦентр»;

3.Выполнять требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информации «ГБУЗ ЛенОблЦентр»;

1.В случае попытки посторонних лиц получить от меня сведения о конфиденциальной информации «ГБУЗ ЛенОблЦентр»сообщить об этом факте непосредственному руководителю;

4.В случае моего увольнения все носители конфиденциальной информации «ГБУЗ ЛенОблЦентр» (рукописи, черновики, машинные носители, распечатки на принтерах, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в «ГБУЗ ЛенОблЦентр» передать непосредственному руководителю;

Я предупрежден(а), что в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, ко мне могут быть применены меры дисциплинарного взыскания в соответствии с трудовым законодательством РФ.

Я ознакомлен(а) с Положением об охране конфиденциальной информации в «ГБУЗ ЛенОблЦентр», о порядке организации и проведения работ по защите конфиденциальной информации.

Мне известно, что нарушение требований по обеспечению сохранности конфиденциальной информации «ГБУЗ ЛенОблЦентр» может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Российской Федерации, обязанности по возмещению ущерба учреждению и других наказаний.

_____ _____ _____

Дата подпись расшифровка