ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
ВЛАДИМИРСКОЙ ОБЛАСТИ

М И А Ц

МЕДИЦИНСКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР

Организация защиты персональных данных

Примерные формы документов

Адрес:600000, г.Владимир,
ул. Никитская, д.3.
Тел./факс (4922) 32-65-39,
32-53-71, 32-21-80,
32-74-98

Адрес сайта:
http://www.medctat.narod.ru

Адрес электронной почты:
Vlad@medstat.elcom.ru

СОДЕРЖАНИЕ:

1. Выписка из Постановления правительства РФ «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 №781

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных,

разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

2. Пример оформления перечня списка сведений конфиденциального характера

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

ПЕРЕЧЕНЬ
сведений конфиденциального характера

(примерный перечень)

№ п/п	Наименование сведений	Типы документов, места хранения , классификация сведений.
1.	Регистр выписанных Федеральных рецептов	Файлы базы данных в каталоге D:\medbase\database\ хранящиеся на сервере базы данных «IBM» инв.№_____, «Персональные данные»
2.	Регистр выписанных региональных рецептов	Файлы базы данных в каталоге D:\medbase\database\ хранящиеся на сервере базы данных «IBM» инв.№_____, «Персональные данные»
3.	Регистр выписанных рецептов на дорогостоящие медикаменты	Файлы базы данных в каталоге D:\medbase\database\ хранящиеся на сервере базы данных «IBM» инв.№_____, «Персональные данные»
4.	Медицинские карты пациентов	На бумажном носителе, хранятся в помещении №___, «Персональные данные»
5.	Анкеты сотрудников	Файлы с расширением *.doc в каталоге D:\КАДРЫ хранящиеся на ПЭВМ инв.№_____, Персональные данные
6.	и т.д.	

должность ФИО

3. Пример оформления перечня защищаемых информационных ресурсов

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

Перечень защищаемых ресурсов информационной системы персональных данных «_____»

(примерный перечень)

1. Медицинские карты пациентов, находящиеся на хранении в помещении «_____», содержащие персональные данные граждан, каб. №____. *(Регистратура, архив)*

2. Файлы с конфиденциальной информацией на жеском магнитном диске в составе персонального компьютера инв. №_____, содержащие персональные данные граждан, каб.№____. *(ПК с установленными медицинскими программами)*

3. Файлы с конфиденциальной информацией на жестком диске в составе персонального компьютера инв. №_____, содержащие персональные данные сотрудников «_____» , каб. №____ *(бухгалтерия)*

4. Файлы с конфиденциальной информацией на жестком магнитном диске в составе персонального компьютера инв.№_____, содержащие персональные данные сотрудников «_____» каб.№ ____. *(отдел кадров)*

5. Файлы с конфиденциальной информацией на переносимых носителях информации, прошедших регистрацию в установленном порядке, имеющих гриф «Для служебного пользования».

6. и т.д.

должность ФИО

4. Пример оформления списка сотрудников допущенных к обработки персональных данных

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г

Список сотрудников допущенных к работе в информационной системе персональных данных «_____»

№	Наименование сведений	Должность	Фамилия, имя, отчество
1			
2			
3			

должность ФИО

5. Пример оформления списка сотрудников обслуживающих информационную систему персональных данных

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

СПИСОК

сотрудников, обслуживающих информационную систему персональных данных «_____»

№	Должность	Фамилия, имя, отчество
1		
2		
3		

должность ФИО

6. Пример оформления схемы расположения информационных ресурсов относительно границ контролируемой зоны

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

СХЕМА

расположения информационных ресурсов

(схема расположения информационных ресурсов относительно плана здания, под ресурсом понимается физическое место хранения информации: медицинские карты, ПЭВМ с медицинскими программами и т.д.)

должность ФИО

7. Пример оформления списка сотрудников имеющих право самостоятельного доступа в защищенное помещение

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

Перечень лиц, имеющих право самостоятельного доступа в защищенное помещение № «___»

№	Должность	Фамилия, имя, отчество
1		
2		
3		

должность ФИО

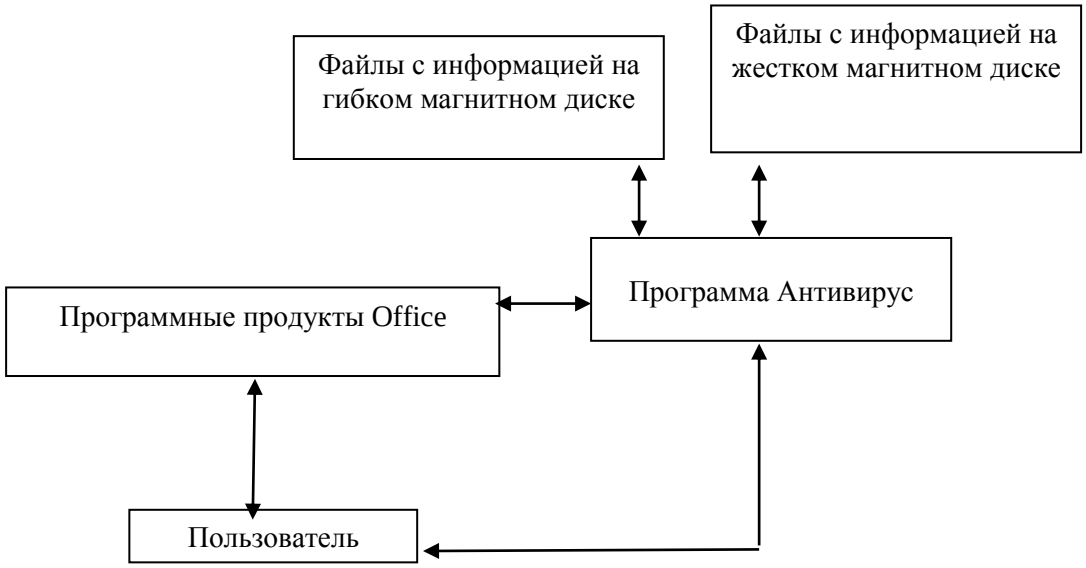
8. Пример оформления схемы информационных потоков информационной системы персональных данных

(может быть изложена в текстовой форме, литературным языком)

«УТВЕРЖДАЮ»

_____
_____
«____»_____2009г.

СХЕМА
информационных потоков системы обработки персональных данных
«_____»



должность ФИО

9. Пример оформления акта классификации информационной системы

«УТВЕРЖДАЮ»
Руководитель учреждения

"____"_____"____"г.

А К Т

классификации информационной системы обработки персональных данных

наименование информационной системы

Комиссия в составе:

председатель:

члены комиссии:

рассмотрев исходные данные на информационную систему обработки персональных данных *наименование системы* условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д.) и в соответствии с руководящими документами Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" и "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)" и т.д.,

РЕШИЛА:

Установить *наименование информационной системы*

класс _____.

Председатель

Члены комиссии

10. Пример описания системы защиты персональных данных в информационной системе

«УТВЕРЖДАЮ»

_____
_____
«____»_____2009г.

Система защиты персональных данных информационной системы персональных данных «_____»

(Литературным языком описывается весь комплекс предпринятых мер по защите персональных данных со ссылками на ранее утвержденные документы)

Пример:

2. Защищаемые информационные ресурсы

1. Помещение № 12 (Регистратура). Доступ имеют сотрудники, согласно «Списку сотрудников имеющих право самостоятельного доступа в защищенное помещение №12», утвержденному «25» марта 2009г., а так же «Списку сотрудников обслуживающих информационную систему персональных данных _____» утвержденному «25» марта 2009г. В помещении установлены охранные датчики движения и датчики пожарной безопасности, реагирующие на задымление. В нерабочее время помещение опечатывается бумажными лентами с оттисками мастичной печати учреждения «Для пакетов №4» и сдается под охрану на пульт дежурного. Ключи от помещения имеются у Заведующего хозяйственного отдела учреждения, основной ключ храниться у дежурного по зданию и выдается по требованию сотрудников указанных в списках с обязательной отметкой в журнале.

3. Сведения конфиденциального характера

1. Медицинские карты пациентов. Доступ имеют сотрудники согласно «Списку сотрудников допущенных к работе в информационной системе _____» утвержденному «25» марта 2009г. Медицинские карты выдаются лично пациентам, которые обязаны предъявить документы удостоверяющие личность. Так же медицинские карты выдаются медицинскому персоналу учреждения по требованию. Все факты выдачи медицинских карт регистрируются в журнале. Медицинские карты хранятся в защищенном помещении №12, система защиты которого описана в п. 1 раздела 2 настоящего документа.

должность ФИО

11. Типовое положение о конфиденциальной информации

Экз.№___

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

ПОЛОЖЕНИЕ

о конфиденциальной информации Государственного учреждения здравоохранения

«_____»

г.Владимир
2009г.

(Примерный текст)

1. Общие положения.

1.1. Настоящее Положение регулирует в соответствии с Гражданским кодексом РФ, Федеральным законом РФ "Об информации, информатизации и защите информации", иными федеральными законами и нормативными правовыми актами РФ отношения, связанные с охраной и использованием конфиденциальной информации Государственного учреждения здравоохранения «_____» (далее по тексту настоящего Положения – «ГУЗ»).

1.2. Конфиденциальная информация «ГУЗ» - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления и существования, отнесенная к таковой в соответствии с настоящим Положением, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, ограничения к доступу и разглашению которой предпринимаются согласно настоящего Положения.

1.3. «ГУЗ» имеет исключительное право на использование конфиденциальной информации любыми незапрещенными законом способами по собственному усмотрению.

1.4. В соответствии с настоящим Положением «ГУЗ» принимает меры к охране конфиденциальной информации, ограничению доступа к ней третьих лиц.

1.5. Целью охраны конфиденциальной информации является обеспечение экономической и правовой безопасности «ГУЗ».

1.6. В случае если в связи с осуществлением своей деятельности «ГУЗ» становятся известны сведения, составляющие в соответствии с законодательством РФ государственную тайну, «ГУЗ» обязано

предпринимать меры по их охране в соответствии с Федеральным законом РФ "О государственной тайне" и иными нормативными правовыми актами о государственной тайне.

1.7. Действие настоящего Положения распространяется на все структурные подразделения «ГУЗ».

2. Коммерческая тайна ГУЗ.

2.1. Коммерческой тайной «ГУЗ» является следующая информация:

2.1.1. Данные первичных учетных документов бухгалтерского учета «ГУЗ»;

2.1.2. Содержание регистров бухгалтерского учета «ГУЗ»;

2.1.3. Содержание внутренней бухгалтерской отчетности «ГУЗ»;

2.1.4. Совершаемые и совершенные «ГУЗ» сделки, в том числе договоры, их предмет, содержание, цена и другие существенные условия;

2.1.5. Сведения об открытых в кредитных учреждениях расчетных и иных счетах, в том числе в иностранной валюте, о движении средств по этим счетам, и об остатке средств на этих счетах, сведения о имеющихся вкладах в банках, в том числе в иностранной валюте (банковская тайна);

2.1.6. Секреты производства (ноу-хау) и иная информация, составляющая производственную тайну;

2.1.7. Иные сведения, отнесенные к коммерческой тайне в соответствии с действующим законодательством РФ.

2.2. Любая иная информация, за исключением информации, которая в соответствии с законодательством не может быть отнесена к коммерческой тайне, может быть отнесена к коммерческой тайне по решению Директора «ГУЗ».

2.3. К коммерческой тайне не может быть отнесена следующая информация:

2.3.1. Учредительные документы «ГУЗ»;

2.3.2. Регистрационные удостоверения, лицензии, патенты и иные документы, дающие право заниматься своей деятельностью;

2.3.4. Документы о платежеспособности;

2.3.5. Сведения о численности, составе работников «ГУЗ», их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

2.3.6. Документы об уплате налогов и обязательных платежах;

2.3.7. Сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РФ и размерах причиненного при этом ущерба, в случае если данные факты установлены вступившим в законную силу решением (приговором) суда, арбитражного суда;

2.3.8. Идентификационный номер налогоплательщика (ИНН);

2.3.9. Содержание внешней бухгалтерской отчетности «ГУЗ», в том числе содержание: бухгалтерского баланса; отчета о прибылях и убытках; приложений к ним, предусмотренных нормативными актами; аудиторского заключения, подтверждающего достоверность бухгалтерской отчетности «ГУЗ»; пояснительной записки к данным внешней бухгалтерской отчетности

2.3.10. Иная информация, которая не может быть отнесена к коммерческой тайне в соответствии с законодательством РФ.

2.4. Отнесение информации, указанной в пункте 2.1. настоящего Положения, к информации, составляющей коммерческую тайну «ГУЗ», не требует издания каких-либо иных актов помимо настоящего Положения.

2.5. Отнесение информации, указанной в пункте 2.2. настоящего Положения, к информации, составляющей коммерческую тайну «ГУЗ», осуществляется путем издания в каждом конкретном случае приказа Директора «ГУЗ». Инициатива в издании приказа Директора об отнесении той или иной информации к коммерческой тайне «ГУЗ» может исходить от Учредителей «ГУЗ», руководителей структурных подразделений «ГУЗ», контрагентов.

2.6. К коммерческой тайне не относится информация, разглашенная «ГУЗ» самостоятельно или с его согласия.

3. Служебная тайна «ГУЗ».

3.1. Служебную тайну «ГУЗ» составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику «ГУЗ» в связи с исполнением им возложенных на него трудовых обязанностей.

3.2. К служебной тайне не относится информация, разглашенная «ГУЗ» самостоятельно или с его согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

4. Банковская тайна «ГУЗ».

4.1. Банковскую тайну составляют сведения о состоянии банковского счета и банковского вклада, операций по счету и сведений о клиенте.

4.2. Сведения, составляющие банковскую тайну, могут быть предоставлены только «ГУЗ» или его представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законодательством РФ.

5. Налоговая тайна «ГУЗ».

5.1. Налоговую тайну составляют любые переданные налоговым органам, органам налоговой полиции, органам государственных внебюджетных фондов и таможенным органам сведения о «ГУЗ».

5.2. Не относятся к налоговой тайне следующая информация:

5.2.1. Информация, разглашенная «ГУЗ» самостоятельно или с его согласия;

5.2.2. Информация об идентификационном номере налогоплательщика;

5.2.3. Информация о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;

5.2.5. Информация, предоставляемая налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам).

5.3. В соответствии с законодательством РФ налоговая тайна не подлежит разглашению налоговыми органами, органами налоговой полиции, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом.

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу коммерческой (в том числе производственной) тайны «ГУЗ», ставшей известной должностному лицу налогового органа, органа налоговой полиции, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей.

Поступившие в налоговые органы, органы налоговой полиции, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют в соответствии с законодательством РФ специальный режим хранения и доступа.

6. Охрана конфиденциальной информации «ГУЗ».

6.1. Охрана конфиденциальной информации «ГУЗ» состоит в принятии комплекса мер, направленных на ограничение доступа к конфиденциальной информации третьих лиц, на предотвращение несанкционированного разглашения конфиденциальной информации, выявление нарушений режима конфиденциальной информации «ГУЗ», пресечение нарушений режима конфиденциальной информации «ГУЗ»,

привлечение лиц, нарушающих режим конфиденциальной информации «ГУЗ» к установленной ответственности.

6.2. Обязательным условием трудовых договоров, заключаемых с работниками «ГУЗ», является условие о соблюдении работником служебной и коммерческой тайны.

6.3. Каждый работник «ГУЗ» при принятии на работу предупреждается под расписку об ответственности за нарушение режима служебной и коммерческой тайны.

6.4. Инженер по защите информации обязан не реже двух раз в год проводить среди сотрудников «ГУЗ» инструктаж по соблюдению режима служебной и коммерческой тайны. Вновь принятый на работу работник проходит инструктаж при принятии на работу.

Данные о проведенном инструктаже фиксируются в специальном журнале.

6.5. Заключаемые «ГУЗ», в лице любых уполномоченных лиц договоры должны содержать условие о сохранении контрагентами конфиденциальности.

6.6. В рабочих и иных помещениях «ГУЗ» создаются условия, ограничивающие доступ к конфиденциальной информации третьих лиц и несанкционированное разглашение конфиденциальной информации, в том числе устанавливаются технические средства защиты от несанкционированного доступа к информации (сейфы и металлические ящики для хранения документов и пр.).

6.8. «ГУЗ» предпринимает меры по выявлению фактов нарушения режима конфиденциальной информации.

6.9. «ГУЗ» предпринимает все допустимые законом способы по пресечению выявленных нарушений режима конфиденциальной информации.

6.10. Лица, виновные в нарушении режима конфиденциальной информации «ГУЗ» привлекаются к установленной ответственности.

7. Порядок использования и предоставления конфиденциальной информации «ГУЗ».

7.1. Использование конфиденциальной информации «ГУЗ» допускается только теми работниками, которым доступ к такой информации необходим в силу выполняемых ими функций.

7.2. Предоставление конфиденциальной информации «ГУЗ» третьим лицам возможно не иначе как с санкции Директора «ГУЗ».

7.3. Внешняя бухгалтерская отчетность «ГУЗ» является публичной.

Публичность бухгалтерской отчетности заключается в возможности ее опубликования в средствах массовой информации, доступных пользователям бухгалтерской отчетности, либо распространении среди них брошюр, буклетов и других изданий, содержащих бухгалтерскую отчетность, а также в ее передаче

территориальным органам государственной статистики по месту регистрации организации для предоставления заинтересованным пользователям.

Годовая бухгалтерская отчетность публикуется «ГУЗ» в порядке, установленном законодательством РФ.

7.4. «ГУЗ» представляет годовую бухгалтерскую отчетность в соответствии с учредительными документами учредителям, а также территориальным органам государственной статистики по месту их регистрации. Другим органам исполнительной власти, банкам и иным пользователям бухгалтерская отчетность представляется в соответствии с законодательством РФ.

7.5. Иные случаи предоставления конфиденциальной информации предусмотрены действующим законодательством РФ.

8. Заключительные положения.

8.1. Лица виновные в нарушении режима конфиденциальной информации «ГУЗ» привлекаются в установленном порядке к уголовной, административной, дисциплинарной и гражданско-правовой ответственности.

8.2. Во всем ином, что не урегулировано настоящим Положением, применяются положения действующего законодательства РФ.

должность ФИО

СОГЛАСОВАНО:

должность ФИО

Отп. 3 Экз.
1 в Дело
2 Бухгалтерия
3 Отдел «_____»
Исп.Отп. ФИО
«__» марта 2009г.

12. Типовая инструкция по обеспечению защиты в ЛВС

Экз.№___

«УТВЕРЖДАЮ»

_____

_____

«____»_____2009г.

ИНСТРУКЦИЯ

по обеспечению защиты конфиденциальной информации, обрабатываемой в локальной вычислительной сети Государственного учреждения здравоохранения

«_____»

г.Владимир
2009г.

(Примерный текст)

1. Общие Положения

1.1. Инструкция устанавливает основные требования по обеспечению сохранности конфиденциальной информации при работе в локальной вычислительной сети Государственного учреждения здравоохранения «_____» (далее по тексту ЛВС)

1.2. Ответственность за обеспечение режима конфиденциальности проводимых в ЛВС работ, своевременную разработку и осуществление необходимых мероприятий по защите информации возлагается на инженера по защите информации, либо сотрудника на которого возложены данные обязательства.

1.3. Лица виновные в нарушении требований настоящей Инструкции и других руководящих документов по вопросам обеспечения и соблюдения требований по защите информации, в зависимости от причиненного ущерба, привлекаются к уголовной, административной, дисциплинарной и гражданско-правовой ответственности.

1.4. К обработке конфиденциальной информации в ЛВС допускаются только сотрудники ГУЗ «_____», которым в установленном порядке оформлен допуск к конфиденциальной информации. Решение о допуске сотрудников к работе с конфиденциальной информацией в ЛВС принимает Директор ГУЗ «_____». В дальнейшем сотрудник, допущенный к обработке конфиденциальной информации в ЛВС, будет именоваться пользователь.

1.5. Настоящая Инструкция доводится до пользователей под расписку.

2. Мероприятия по защите информации

2.1.1 Помещение № ____, в котором размещен сервер доступа, а так же сервер базы данных хранящий персональные данные граждан, располагается на втором этаже здания по адресу _____.

2.1.2 Помещение №_____, в котором размещаются автоматизированные рабочие места для обработки и хранения сведений бухгалтерской отчетности учреждения располагается на втором этаже здания по адресу _____.

2.1.3 Помещение №_____, в котором происходит обработка и хранение сведений о сотрудниках учреждения располагается на третьем этаже здания по адресу _____.

По окончании рабочего дня помещения должны сдаваться под охрану в соответствии с установленным порядком и опечатываться.

2.2. ЛВС организованна на базе сервера _____ под управлением операционной системы _____.

2.2.1 Сервер баз данных _____.

2.2.2 Автоматизированные рабочие места сотрудников построены на базе операционной системы _____.

2.3 Класс защищенности конфиденциальной информации в ЛВС от несанкционированного доступа установлен – 1Д.

2.4 В ЛВС может обрабатываться информация с грифом не выше «Конфиденциально».

2.5. Технические средства ЛВС в помещениях размещаются таким образом, чтобы исключить визуальный просмотр экрана видеомонитора лицами, не имеющими отношения к конкретно обрабатываемой информации.

2.6. При эксплуатировании ЛВС должна обеспечиваться длина пароля пользователя не менее 8 (восьми) буквенно-цифровых символов. Смена пароля не реже одного раза в _____.

2.7. В целях предотвращения разрушения и утери обрабатываемой в ЛВС информации должно осуществляться копирование необходимой информации по мере ее обновления на учтенные в установленном порядке съемные носители;

2.8. Техническое обслуживание технических средств, входящих в состав объекта информатизации, должно осуществляться только персоналом, допущенным к техническому обслуживанию. При проведении данных работ обработка конфиденциальной информации на обслуживаемом участке ЛВС ЗАПРЕЩЕНА.

3. Порядок работы с программным обеспечением автоматизированного рабочего места.

3.1. Работа на автоматизированных рабочих местах (далее по тексту АРМ) должна осуществляться на базе общесистемного программного обеспечения, утвержденного в «Составе программного обеспечения автоматизированных рабочих мест».

3.2. Изменение рабочего программного обеспечения на АРМ проводится по согласованию с инженером по защите информации либо сотрудником, на которого возложены данные функции и с санкции Директора ГУЗ «_____». Вносимые изменений регистрируются в утвержденном «Составе программного обеспечения автоматизированного рабочего места».

3.3. Защита АРМ, программных средств и информации от несанкционированного доступа реализуется установленными программными продуктами (Внутренние средства защиты, антивирусные программы, программы зашиты от несанкционированного доступа).

3.4. Сообщение программ контроля при загрузке или в процессе работы с системой о нарушении целостности рабочего программного обеспечения является признаком его несанкционированной модификации или проникновения программы-«вируса». В этом случае в комиссионном порядке проводится разбор и анализ ситуации с принятием решения о возможности продолжения работ на автоматизированном рабочем месте. Для проведения анализа возникших ситуаций привлекаются сотрудники отдела обслуживания и администрирования, а так же отдела программирования.

3.5. Обнаруженное несанкционированное изменение (модификация) программного обеспечения регистрируется как нарушение режима конфиденциальности на автоматизированном рабочем месте, по факту происшедшего проводиться проверка аналогичная п.3.4 настоящей инструкции.

3.6. При установлении факта обнаружения программ-«вирусов» необходимые антивирусные процедуры проводятся пользователем, при необходимости, с привлечением специалистов отдела обслуживания и администрирования, а так же отдела программирования.

4. Порядок использования магнитных носителей информации

4.1. Обработка и хранение конфиденциальной информации обрабатываемой в ЛВС разрешается только с использованием взятых на инвентарный учет носителях информации и на жестких магнитных дисках (ЖМД) ученных АРМ. Копирование конфиденциальной информации на носители информации, не взятые на инвентарный учет, ЗАПРЕЩЕНО.

4.2. Учет защищаемых носителей производится с помощью маркировки. Выдача пользователям носителей информации, предназначенных для работы с конфиденциальной информацией, производится инженером по защите информации, либо сотрудником на которого возложены

данные обязанности, с обязательной регистрацией в журнале. По окончании работ, для выполнения которых требовались переносимые носители информации, носители информации должны сдаваться инженеру по защите информации, либо сотруднику на которого возложены данные обязанности. В журнале регистрации съемных носителей информации делает отметку об их возврате.

4.3. Вышедшие из строя носители, подлежат сдаче инженеру по защите информации, либо сотруднику на которого возложены данные обязанности для последующего уничтожения в установленном порядке.

5. Обязанности пользователя при работе в ЛВС на АРМ.

5.1. Перед началом работы на АРМ с конфиденциальной информацией следует убедиться в отсутствии в помещении посторонних лиц, в целостности программных средств защиты от несанкционированного доступа, актуальности антивирусных баз.

5.2. Работу с программными продуктами, установленными на АРМ, пользователь осуществляет в соответствии с «Руководством пользователя» для конкретных программных продуктов.

5.3. При обработке конфиденциальной информации на АРМ следует руководствоваться требованиями настоящей инструкции (разделы 2,3,4).

5.4. Обработка на АРМ конфиденциальной информации производится только на носителях информации, предназначенных для обработки конфиденциальной информации, либо на жестких магнитных дисках в составе учтенных АРМ, в специально отведенных каталогах.

5.5. При завершении работы пользователя на АРМ необходимо провести полное выключение системы.

5.6. Пользователю запрещается:

- Оставлять бесконтрольно включенное АРМ, магнитные носители, либо иную документацию содержащую сведения конфиденциального характера;
- Изменять и тиражировать программное обеспечение;
- Вести разговоры с посторонними лицами о процедурах доступа к АРМ и информации;
- Набирать на клавиатуре при посторонних лицах персональный пароль и записывать его;
- Сообщать устно или письменно свой персональный пароль;
- Сохранять обрабатываемую информацию в каталогах, не предназначенных для хранения конфиденциальных сведений;

5.7. Инженер по защите информации либо сотрудник, на которого возложены данные функции не реже одного раза в квартал осуществляет контроль эффективности внедренных на объекте защитных мер и средств защиты информации.

Обязательным является контроль:

- при вводе АРМ в эксплуатацию;

- после ремонта АРМ и средств защиты информации;
- при изменении условий эксплуатации АРМ и размещении технических средств.

6. Ответственность за нарушение требований инструкции при обработке конфиденциальной информации в ЛВС

6.1 Лица виновные в нарушении требований инструкции при обработке конфиденциальной информации «_____» привлекаются в установленном порядке к уголовной, административной, дисциплинарной и гражданско-правовой ответственности.

7. Заключение

7.1.Настоящая Инструкция доводится до пользователей под роспись.

должность ФИО

СОГЛАСОВАНО:

должность ФИО

Лист ознакомления

Должность	ФИО	Подпись

Отп. 3 Экз.
1 в Дело
2 Бухгалтерия
3 Отдел «_____»
Исп.Отп. ФИО
«__» _____ 2009г.

13. Образец уведомления об обработке персональных данных

Исх. № ___ от «___» _____ 200_г.

Руководителю Управления Федеральной службы
по надзору в сфере связи и массовых коммуникаций
по Владимирской области
В.В.Никонорову

Уведомление
об обработке персональных данных
Юридическое лицо
(указывается тип оператора)

Полное наименование: Центральная районная больница ХХХХХХХХХ муниципального района Владимирской области (согласно Устава).
Краткое наименование: ЦРБ ХХХХХХХХХ района (согласно Устава).
Главный врач: Фамилия Имя Отчество.
Юридический (почтовый) адрес:
(Тел./Факс/E-mail):

(наименование (фамилия, имя, отчество), адрес оператора)

ИНН: ХХХХХХХХХХ КПП: ХХХХХХХХХ ОГРН: ХХХХХХХХХХХХХ

руководствуясь ст. 6 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»; ст.ст. 85-90 Трудового кодекса Российской Федерации (Федерального закона от 30.12.2001г. №197-ФЗ), Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», (учредительными документами оператора, определяющими деятельность), Лицензией (№ ХХХ от ХХ.ХХ.ХХХХг.), Уставом (утвержден ХХ.ХХ.ХХХХг.)

(правовое основание обработки персональных данных)

с целью обеспечения, необходимых для установления медицинских диагнозов, оказания медицинских услуг, персональных данных сотрудников для обеспечения кадровой работы

(цель обработки персональных данных)

осуществляет обработку следующих категорий персональных данных: основных (непосредственных):
фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ИНН, паспортные данные, медицинский полис, страховое свидетельство), специальных: состояние здоровья
принадлежащих: Пациентам ЦРБ, сотрудникам ЦРБ.

(категории субъектов, персональные данные которых обрабатываются)

Класс информационной системы- КХХ Смешанная обработка вышеуказанных персональных данных будет осуществляться с использованием ПЭВМ (информация доступна лишь для строго определенных сотрудников юридического лица) с передачей полученной информации, с использованием сети общего пользования Интернет, (не используется) используется средства криптозащиты (наименование, регистрационный номер и производитель криптографических средств, уровень криптографической защиты, уровень специальной защиты от утечки по каналам побочных излучений и наводок, уровень защиты от несанкционированного доступа). Хранение сведений (базы данных) организовано на электронных носителях с паролем, на бумажных носителях - в сейфах

(Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке)

на территории Владимирской области код 33..

(указывается территория субъекта (ов), на которой (ых) осуществляется обработка персональных данных)

Дата начала обработки персональных данных: ХХ.ХХ.ХХХХг.

(число, месяц, год)

Срок или условия прекращения обработки персональных данных: прекращение дчеятельности как юридического лица.

Главный врач

(должность) (подпись) (Ф.И.О.)

М.П.

“ ” _____. 200Х г.
(число) (месяц) (год)

14. Основные нормативные правовые акты и методические документы по защите конфиденциальной информации.

1. Федеральный закон от 27.07.2006 г. №149-ФЗ "Об информации, информационных технологиях и защите информации".
2. Федеральный закон от 07.07.2003 г. №126-ФЗ "О связи".
3. Федеральный закон от 08.08.2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности".
4. Указ Президента Российской Федерации от 19.02.99 г. № 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации".
5. "Доктрина информационной безопасности Российской Федерации", утверждена Президентом Российской Федерации 9.09.2000 г.
6. Указ Президента Российской Федерации от 17.12.97 г. № 1300 "Концепция национальной безопасности Российской Федерации" в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.
7. Указ Президента Российской Федерации от 06.03.97 г. № 188 "Перечень сведений конфиденциального характера".
8. Постановление Правительства Российской Федерации от 03.11.94 г. №1233 "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органов исполнительной власти".
9. Решение Гостехкомиссии России и ФАПСИ от 27.04.94 г. № 10 "Положение о государственном лицензировании деятельности в области защиты информации" (с дополнением).
10. Постановление Правительства Российской Федерации от 11.04.2000 г. № 326 "О "лицензировании отдельных видов деятельности".
11. «Сборник руководящих документов по защите информации от несанкционированного доступа» Гостехкомиссия России, Москва, 1998 г.
12. ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения"
13. ГОСТ Р 50922-96 "Защита информации. Основные термины и определения"
14. ГОСТ Р 51583-2000 "Порядок создания автоматизированных систем в защищенном исполнении"
15. ГОСТ Р 51241-98 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний".
16. ГОСТ Р ИСО 7498-1-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель".
17. ГОСТ Р ИСО 7498-2-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации".
18. ГОСТ 2.114- 95 "Единая система конструкторской документации. Технические условия".

19. ГОСТ 2.601- 95 "Единая система конструкторской документации. Эксплуатационные документы".
20. ГОСТ 34.201- 89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем".
21. ГОСТ 34.602- 89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создании автоматизированных систем".
22. ГОСТ 34.003- 90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения".
23. РД Госстандарта СССР 50-682-89 "Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения".
24. РД Госстандарта СССР 50-34.698-90 "Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов".
25. РД Госстандарта СССР 50-680-89 "Методические указания. Автоматизированные системы. Основные положения".
26. ГОСТ 34.601- 90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания"
27. ГОСТ 6.38-90 "Система организационно-распорядительной документации. Требования к оформлению".
28. ГОСТ 6.10- 84 "Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствам вычислительной техники, ЕСКД, ЕСПД и ЕСТД".
29. ГОСТ Р-92 "Система сертификации ГОСТ. Основные положения".
30. ГОСТ 28195-89 "Оценка качества программных средств. Общие положения".
31. ГОСТ 28806-90 "Качество программных средств. Термины и определения".
32. ГОСТ Р ИСОМЭК 9126- 90 "Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению".
33. ГОСТ 2.111-68 "Нормоконтроль".
34. ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации".
35. РД Гостехкомиссии России "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей", Москва, 1999г.
36. РД Гостехкомиссии России "Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам", Москва, 2000г.

37. ГОСТ В 15.201-83 "Тактико-техническое (техническое) задание на выполнение ОКР".
38. ГОСТ В 15.101-95 "Тактико-техническое (техническое) задание на выполнение НИР"
39. ГОСТ В 15.102-84 "Тактико-техническое задание на выполнение аванпроекта"
40. ГОСТ В 15.103-79 "Порядок выполнения аванпроекта. Основные положения"
41. ГОСТ В 15.203-96 "Порядок выполнения ОКР. Основные положения"
42. Решение Гостехкомиссии России от 14.03.95 г. № 32 "Типовое положение о подразделении по защите информации от иностранных технических разве док и от ее утечки по техническим каналам на предприятии (в учреждении, организации)".
43. СанПиН 2.2.2.542-96 "Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организация работы".
44. ГОСТ Р 50948-96. "Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности".
45. ГОСТ Р 50949-96 "Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности."
46. ГОСТ Р 50923-96 "Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения."
47. Решение Гостехкомиссии России от 03.10.95 г. № 42 "Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте".

Приложение №
Приказу Минздравсоцразвития России

В_____
(орган исполнительной власти)

Форма № 1-ВМП

_____
субъекта Российской Федерации

_____
в сфере здравоохранения)

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных

Я, _____
(фамилия, имя, отчество)

даю согласие органу исполнительной власти субъекта РФ в сфере здравоохранения _____ на обработку и использование данных, содержащихся в настоящем заявлении, с целью организации оказания высокотехнологичной медицинской помощи.

1. Дата рождения _____
(число, месяц, гол)

2. Пол _____
(женский, мужской - указать нужное)

3. Документ, удостоверяющий личность _____
(наименование, номер и

_____
серия документа, кем и когда выдан)

4. Адрес по месту регистрации _____
(почтовый адрес по месту регистрации)

_____

5. Адрес фактического проживания _____
(почтовый адрес факти ческою проживания, контактный телефон)

_____

6. Наименование страховой компании, серия и № страхового полиса обязательного медицинского страхования (при наличии)
_____

7. Страховой номер индивидуального лицевого счета (СНИЛС) (при наличии) _____

8. Сведения о законном представителе_____
(фамилия, имя, отчество)

_____
(почтовый адрес места жительства, пребывания, фактического проживания, телефон)

9. Дата рождения законного представителя _____
(число, месяц, год)

10. Документ, удостоверяющий личность законного представителя_____

_____
(наименование, номер и серия документа, кем и когда вычан)

_____

11. Документ, подтверждающий полномочия законного представителя_____

_____
(наименование, номер и серия документа, кем и когда выдан)

Примечание: пункты с 8 по 11 заполняются в том случае, если заявление заполняет законный представитель гражданина Российской Федерации.

Об ответственности за достоверность представленных сведений предупрежден (предупреждена),
(нужное подчеркнуть)

На передачу лично мне сведений о дате госпитализации и иных данных по телефонам, указанным в заявлении согласен (согласна).
(нужное подчеркнуть)

Данные, указанные в заявлении, соответствуют представленным документам.

Заявление и документы гражданина (гражданки)_____

Зарегистрированы _____
(№ Талон на оказание ВМП)

Принял _____ _____
(дата приема заявления) (подпись специалиста)

_____
(линия отреза)

Расписка-уведомление

Заявление и документы гражданина (гражданки)_____
(№ Талон на оказание ВМП)

Принял _____ _____
(дата приема заявления) (подпись специалиста