Содержание:

ВВЕДЕНИЕ

В мировом рейтинге из самых технологичных направлений деятельности современного общества ведущее место занимает отрасль телекоммуникаций. Мир переживает настоящий бум разработки и внедрения все новых и новых методов и технологий передачи, обработки и хранения информации. В результате чего за последние 10-15 лет наблюдается глобализация телекоммуникационных сетей, стирание границ и создание единого мирового информационного пространства[2, с. 12]. Лавинообразное и революционное внедрение различных технологий и методов передачи, обработки и хранения информации в телекоммуникационных сетях заставляют принципиально по-новому рассматривать роль и значение технической защиты информации.

Рост угроз информации вызван либерализацией общественных и межгосударственных отношений, применением технических средств обработки информации и средств связи, распространением средств несанкционированного доступа к информации и воздействия на нее.

Обеспечение безопасной деятельности необходимо для любых предприятий и учреждений, начиная от государственных организаций и заканчивая мелким частным предприятием, которое занимается розничной торговлей. Разница будет заключаться лишь в том, какие средства и методы и в каком объеме потребуются для обеспечения их безопасности.

Прежде чем приступить к анализу современного состояния задачи информационной безопасности, необходимо рассмотреть задачи безопасности вообще. Сначала необходимо определить, что подлежит защите, и какими основными принципами следует руководствоваться при организации защиты. Исходя из исторической и международной практики, объектами защиты, с учетом их приоритетов, являются:

1) человек (личность);

2) информация;

3) материальные ценности.

Исследование курсовой работы направлено на рассмотрение вопросов связанных с защитой информации, классификацию и анализ угроз.

Информацию можно продать, купить, импортировать, фальсифицировать, украсть и т. д., из этого следует, что она должна каким-то образом защищаться. Следует отметить, что защите подлежит не вся информация, а только та, которая имеет цену, то есть ценная информация. Ценной же становится информация, обладание которой позволит ее действительному или потенциальному владельцу получить какой-либо выигрыш: моральный, материальный, политический и т. д.

Поскольку в обществе всегда существуют люди, желающие иметь какие-либо преимущества над другими, то неизбежно возникает желание незаконным путем получить ценную информацию, а следовательно - возникает необходимость ее защищать. Проблема защиты информации возникла в мете с понятием информация и знания, цели злоумышленников и мотивация владельцев не изменяется, изменяются только методы и средства.

Проблема защиты информации неоднократно рассмотрены в различных, как зарубежных, так и отечественных источниках. Так, например, Жельников В. рассматривает историю криптографических методов, Мельников В. П. и Клеймов С.А. описывают защищенность с точки зрения систем, анализируют возможные атаки и меры противостояния таковым, ряд авторов: Гашков С. Б., Аграновский А.В., Балакин А.В., Городецкий В.И., Самойлов В.В. – посвятили свои исследования отдельному направлению защиты информации и рассматривают непосредственно особенности реализации и применения стеганографии. Следовательно –угрозы и методы защиты информации, которые будут рассмотрены в работе, не являются чем-то новым. Тем не менее, комплексное применение средств защиты и правильная ее организация используется крайне редко, что дает дополнительный стимул для изучения возможностей их применения. Рассмотренные работы указанных авторов рассматривают алгоритмы и подходы в общем, основной же задачей курсовой работы является анализ ситуации, обнаружение мест в информационной среде организации, где могут быть применены рассматриваемые подходы, выбор наиболее подходящего набора средств и методов для достижения максимального эффекта в рассматриваемых условиях.

Методы, средства и подходы к защите информации очень зависимы от типа информационных ресурсов, организации документооборота, информационной

инфраструктуры и ряда других параметров. Достаточно сложно рассматривать подобные вопросы в общем, исследование необходимо проводить на примере выбранного целевого объекта.

Основное исследование работы направленно на сферу медицины и защиту, в первую очередь, персональных данных пациентов. То есть - рассматривая ИБ в целом, необходимо вычленить методы и средства применимые в исследуемой предметной области.

Актуальность исследования подтверждена большим интересом к этому вопросу, как в профессиональных медицинских кругах, так и в области специалистов по защите информации. И хотя право на защиту персональных данных и гарантии конфиденциальности формально закреплены на законодательном уровне, в большинстве медицинских учреждений вопросы информационной безопасности не рассматриваются в принципе, отсутствуют какие либо мероприятия направленные на обеспечение информационной безопасности и сохранении врачебной тайны.

Информационная безопасность становится главным направлением развития ИТ в медицине. Такую точку зрения высказал Г. Ройтберг, президент клиники «Медицина», во время выступления на конференции «Информационная безопасность медицинских и страховых компаний – новые угрозы и технологии защиты». Он озвучил мнение, из которого следует - недостаточность защищенности информации о пациенте может не только нарушать основные деонтологические принципы, но и способна нанести существенный экономический ущерб клинике и степени доверия к медицине в целом [8]

Целью курсовой работы является анализ комплексных мер по обеспечению защиты информации в медицинских учреждениях, обеспечения сохранности и конфиденциальности личных данных пациентов.

Предметом исследования курсовой работы является информационная инфраструктура медицинских учреждений и программно-аппаратные комплексы обеспечения защиты конфиденциальной информации в информационной системе медучреждений

Объект исследования является информационная структура медицинского учреждения – медицинский центр ООО «Danke», способы и типы представления информации, информационный сегмент обеспечения деятельности предметной области.

Методы, применяемые в курсовой работе: исследование, методы анализа, теория статистики, теории цифровой обработки сигналов и изображений, экспериментальные методы, исследование литературных источников, синтез и генерация идеи.

Задачами работы являются:

- анализ бизнес-процессов и информационных потоков предметной области;
- анализ основных понятий в сфере ИБ;
- исследование целей информационных атак и рисков связанных с этим;
- ИТ аудит исследуемой организации;
- анализ результатов полученных в ходе аудиторской проверки;
- разработка предложений по увеличению степени защиты и снижению рисков несанкционированного доступа к информационным источникам.

ГЛАВА 1 АНАЛИЗ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ИССЛЕДОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Краткая характеристика ЦМД (центр медицинской диагностики) ООО "Данке"

Многопрофильный медицинский центр ООО «Danke» с 1998 года работает на рынке платных медицинских услуг, осуществляя полный спектр амбулаторно-поликлинической помощи детям, взрослым и людям пожилого возраста. Деятельность центра основана на четкой организации работы широкого круга специалистов, владеющих современными клиническими и инструментальными методами исследования, а также лаборатории – отдельного самостоятельного подразделения в составе центра.

Деятельность организации начиналась с оказания диагностических услуг. Услуги производились в области обследования центральной нервной системы, компьютерная томография, высококачественные рентгеновские снимки. Высокое качество диагностики достигалось, не в последнюю очередь, благодаря использованию сверхсовременного медицинского оборудования производства

немецкого концерна Siemens. Специалисты проходили обучения и сертифицированы в Германии. По прошествии 5 лет работы центр достаточно расширился, он, по-прежнему, оказывал только услуги диагностики, но спектр услуг существенно расширился.

В 2012 году, с приходом новых инвесторов, было принято решения расширить спектр медицинских услуг и, кроме диагностики, предложить: поликлинические услуги, лечебно-профилактические услуги, обследование и забор анализов на дому пациента, неотложная медицинская помощь

Многопрофильность и комплексность оказываемых услуг дали возможность закрепиться на рынке медицинских услуг г. Москвы и региона.

Оказываемые услуги:

1. Полный спектр поликлинической медицинской помощи на базе одиннадцати амбулаторий.

2. Полный спектр поликлинической медицинской помощи на дому. Специалисты Центра готовы приехать в любой район Москвы и Московской области круглосуточно и без выходных.

3. Индивидуальные и групповые лечебно-профилактические программы.

4. Организация скорой и неотложной помощи.

5. Организация специализированной помощи в ЛПУ.

6. Комплексное медицинское обеспечение организаций.

Организационная структура МЦ представлена на следующем рисунке

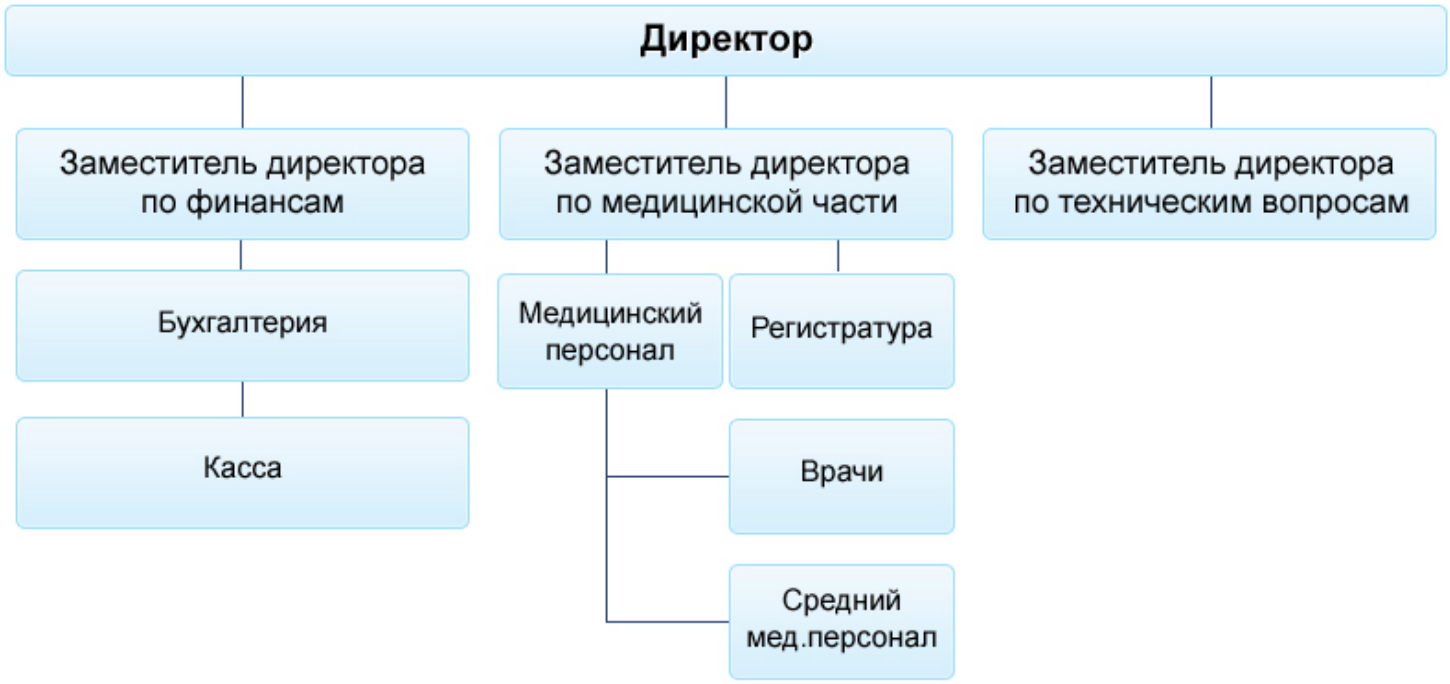

Рисунок 1.1 – Организационная структура МЦ «Danke»

1.2 Общие понятия ИБ организации

Под термином информационная безопасность понимают защищенность информации и поддерживающей ее инфраструктуры от различны непреднамеренных или злонамеренных воздействий, результатом которых может являться нанесенный ущерб, как самой информации, так и ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. [14]

Основные составляющие информационной безопасности

Направления информационных систем, которые нуждаются в защите, следует разделить на категории: обеспечение целостности, доступности и конфиденциальности информационных ресурсов.

- **Доступность** следует рассматривать как возможность получения, за конечный, желательно как можно более короткий промежуток времени, требуемой информации или информационной услуги.

- **Целостность** информации определяет ее актуальность и непротиворечивость, степень защищенности от разрушения и несанкционированного изменения.
- **Конфиденциальность** определяет защиту от несанкционированных доступов к информации, ее утечку или передачу третьим заинтересованным лицам.

Информационные системы создаются для получения определенных информационных услуг. Если получение информации по каким-либо причинам становится невозможным, это приносит ущерб всем субъектам информационных отношений, и как следствие общий ущерб организации. Из этого можно определить, что доступность информации стоит на первом месте.

Целостность является основным аспектом информационной безопасности, так как нарушение точности и правдивости информации фактически можно рассматривать как ее потерю, а в большинстве случаев неправдивая искаженная информация носит еще более пагубный характер, чем ее отсутствие. Например, рецепты медицинских лекарств, поставленные диагнозы, назначения препаратов и методов лечения.

Наиболее проработанной составляющей информационной безопасности в нашей стране является конфиденциальность. Но практическая реализация мер по обеспечению конфиденциальности современных информационных систем сталкивается в России с большими трудностями.

Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках.

Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препятствия и технические проблемы. [15]

Первичной задачей в процессе повышения уровня информационной безопасности является выявление проблем и их локализация. Для выявления проблем и слабых мест в информационной структуре в целом и исследования информационной безопасности проводится IT аудит. Эта процедура может быть проведена с задействованием внутренних или внешних ресурсов. Рассмотрим основные моменты проведения аудита.

1.3 IT аудит

Аудит IT-инфраструктуры - это комплекс мер по инвентаризации, обследованию, тестированию работы элементов IT-инфраструктуры, а также анализ соответствий функционирования систем относительно текущих и будущих требований, включая рекомендации по её модернизации. Одним из важнейших элементов аудита есть анализ системы на предмет защищенности и информационной безопасности (ИБ).

Аудит IT-инфраструктуры состоит из следующих этапов:

1. Аудит технических средств и оборудования:

- 1. инвентаризация серверного, компьютерного, активного сетевого оборудования и оргтехники,
  2. анализ состояния структурированной кабельной системы,
  3. анализ достаточности ресурсов серверного оборудования выполняемым задачам,
  4. анализ организации системы бесперебойного электропитания.

2. Аудит программного обеспечения:

- 1. инвентаризация используемого прикладного программного обеспечения,
  2. анализ серверного и пользовательского программного обеспечения,
  3. анализ программного обеспечения на предмет наличия лицензий на его использование.

3. Аудит сетевых решений и электронных коммуникаций:

3.1 анализ организации внешних каналов передачи данных и телефонии для обмена информацией с внешними по отношению к объекту сетями и системами связи,

3.2 аудит учетных данных хостинга,

3.3 анализ организации системы корпоративной электронной почты.

4. Аудит информационной безопасности:

4.1 анализ систем информационной безопасности,

4.2 анализ систем защиты от вирусов и нежелательной электронной почты,

4.3 анализ систем защиты от внешнего проникновения,

4.4 анализ возможных путей утечки информации внутри организации,

4.5 анализ принципов межсетевого взаимодействия,

4.6 анализ существующих политик IP-адресации, IP-маршрутизации,

4.7 анализ системы хранения и резервирования данных.

Аудит может быть внешним (независимая экспертная организация) и внутренним (реализация проверок, тестов, анализа силами штатных сотрудников). Более объективным и результативным считается внешний аудит, тем более для реализации внутреннего аудита компания может и не иметь в штате нужных кадров (имеющих нужную квалификацию и владеющих методиками и подходами в проведении аудита). После проведения аудита (в случае внешнего аудита) заказчик получает независимую оценку актуального состояния IT-инфраструктуры, информацию об её узких местах и участках, влияющих на стабильность работы информационных систем и предоставления услуг, а также рекомендации по используемым технологиям, оборудованию и его настройкам.

Аудит ИБ организации определяется как систематический, независимый и документированный процесс, для получения свидетельств аудита ИБ и объективного их оценивания с целью установления степени выполнения критериев аудита ИБ.

По содержанию аудит ИБ разделяется на следующие виды:

аудит ИБ СИТ, эксплуатирующийся в организации;

аудит ИБ организации.

Задачей аудита ИБ СИТ, эксплуатирующихся в организации, является проверка состояния защищенности конфиденциальной информации в организации от внутренних и внешних угроз, а также программного и аппаратного обеспечения, от которого зависит бесперебойное функционирование СИТ.

Задачей аудита ИБ организации является проверка состояния защищенности интересов (целей) организации в процессе их реализации в условиях внутренних и внешних угроз, а также предотвращение утечки защищаемой конфиденциальной информации, возможных несанкционированных и непреднамеренных воздействий

на защищаемую информацию.

Проведение аудита ИБ основывается на ряде принципов, следование которым является предпосылкой для обеспечения объективных заключений по результатам аудита ИБ. Эти принципы должны быть признаны и соблюдены всеми сторонами, участвующими в аудите ИБ.

Принципы, относящиеся к аудиту ИБ:

Аудит ИБ должен проводиться независимыми организациями или независимыми аудиторами. Независимость является основанием для беспристрастности при проведении аудита ИБ и объективности при формировании заключения по результатам аудита ИБ;

Аудит ИБ должен охватывать все области ИБ и защитные меры, указанные в договоре на проведение аудита ИБ. Кроме того, полнота аудита ИБ определяется достаточностью предоставленных материалов, документов и уровнем их релевантности. Полнота аудита ИБ является необходимым условием для формирования объективных заключений по результатам аудита ИБ;

Оценка на основе свидетельств является единственным способом, позволяющим получить повторяемое заключение по результатам аудита, что повышает к нему доверие. Для повторяемости заключения свидетельства аудита ИБ должны быть воспроизводимыми;

При проведении аудита аудитор должен понимать деятельность проверяемой организации в достаточной степени, чтобы идентифицировать и правильно оценивать события, процессы, относящиеся к области ИБ, с учетом возможностей применения методов и способов оценки рисков, которые могут оказывать существенное влияние на достоверность проверяемых данных, на ход проведения проверки или на выводы, содержащиеся в аудиторском заключении.

ГЛАВА 2 ЗАЩИТА ИНФОРМАЦИИ В МЕДИЦИНЕ. АНАЛИЗ АТАК ЗЛОУМЫШЛЕННИКА, ОЦЕНКА РИСКОВ

В данный момент в медицинской сфере наблюдается процесс всеобщей информатизации: переход к технологиям электронных регистратур и электронных медицинских карт, интеграция медицинских систем со всеми процессами деятельности ЛПУ. В различных учреждениях в медицинских системах могут обрабатываться не только персональные данные пациентов, включая их истории болезни, но и другие данные – например, касающиеся коечного фонда, или результаты лабораторных исследований либо статистические данные, на основе которых проводится анализ работы учреждения (список можно продолжить). Выгода от внедрения процессов автоматизации очевидна, но, как известно, запуск новых электронных сервисов приводит к появлению новых уязвимостей и угроз и, как следствие, – новых рисков не только для медицинских учреждений, но и для пациентов.

Исследование вопросов защиты информации в медицинском секторе начали рассматривать сравнительно недавно. Актуальность данного исследования определена тем, что в большинстве случаев в рядовом медицинском учреждении вопрос информационной безопасности не ставится вообще. Информационные системы и комплексы, разрабатываемые ранее для использования в медучреждениях, или не предусматривали необходимости защиты или рассматривали ее на примитивном стандартном уровне. Такой подход привел сегодня к ощутимой проблеме. Современная информационная система медучреждения не защищена от действий любого сотрудника, обладающего минимальной технической грамотностью в обращении с компьютерами. А если и используются более продвинутые системы, предусматривающие минимальные уровни защиты от собственных сотрудников, абсолютно уязвимы перед администраторами ИТ-инфраструктуры учреждения. Поэтому перед такими учреждениями здравоохранения встает проблема создания соответствующей всем нормативным требованиям интегрированный системы защиты для уже существующих информационных систем, либо перехода к применению новых информационных систем персональных данных (ИСПДн) с реализованными функциями защиты.

Только в последнее время на эти вопросы начали обращать внимание как со стороны государства так и стороны специалистов и функционеров медицинского сектора и ИТ сектора.

Например - на конференции, организованной компанией «ДиалогНаука» и клиникой «Медицина» (г. Москва) в текущем 2016 году, обсуждались актуальные тенденции в сфере информационной безопасности, остро стоящие проблемы, с

которыми сталкиваются сегодня страховые и медицинские организации, а также опыт их решения.

Первичным мотивирующим фактором стало принятие и дальнейший контроль выполнения ряда законов регламентирующих вопросы защиты личной информации и данных. Обязанность соблюдать постоянно меняющиеся требования законодательства по защите информации и перспектива проверок со стороны регуляторов вызывает серьезное напряжение в медучреждениях, так как действующие нормативные документы трактуются весьма неоднозначно, а ответственность за нарушения ужесточается. В то же время ИТ-инфраструктура медицинских организаций усложняется: вводятся в действие новые прикладные системы и открываются новые филиалы, появляются удаленные пользователи и сотрудники, работающие со своими мобильными устройствами.

2.1 Правовые аспекты и нормативы о защите информации и персональных данных

Защита персональных данных - важное направление информатизации здравоохранения и автоматизации ЛПУ, составная часть и необходимое условие работы любого медицинского учреждения. Федеральный закон от 27.07 2006 пн 152-ФЗ определяет персональные данные (ПДн) как «любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)». В состав персональных данных входят фамилия, имя, отчество субъекта ПДн, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение и т.д. Сведения о состоянии здоровья субъекта ПДн отнесены к специальным категориям персональных данных, и действующее законодательство обязывает ЛПУ обеспечить надежную защиту этой информации.

Контроль за соответствием обработки персональных данных требованиям законодательства осуществляют регуляторы — ФСБ России, Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Несоблюдение и/или нарушение требований по защите персональных данных может привести к следующим последствиям:

• судебные иски к медицинским учреждениям со стороны их сотрудников, пациентов и посетителей;

• принудительное приостановление или прекращение обработки персональных данных (что блокирует всю текущую деятельность ЛПУ);

• приостановление действия или аннулирование лицензии на основной вид деятельности ЛПУ;

• привлечение ЛПУ и/или его руководителя к административной или иной ответственности.

Правовыми основаниями для обработки персональных данных пациентов медицинского учреждения являются:

• "Основы законодательства Российской Федерации об охране здоровья граждан" (№ 5487-1 от 22.07.1993 г.);

• Закон РФ "О донорстве крови и ее компонентов";

• Приказ Минздрава "Об утверждении форм первичной медицинской документации учреждений здравоохранения";

• Приказ Минздрава "Об утверждении учетной и отчетной медицинской документации";

• Приказ Минздрава " Об утверждении форм первичной медицинской документации для учреждений службы крови";

• Приказ Минздрава "Об утверждении порядка медицинского обследования договора крови и ее компонентов";

• и другие.

Правовыми основаниями для обработки персональных данных работников медицинского учреждения являются:

• Трудовой кодекс РФ (Глава 14);

• Постановление Госкомстата РФ от 05.01.2004 г. № 1 "Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты";

• "Основы законодательства Российской Федерации об охране здоровья граждан" (№ 5487-1 от 22.07.1993 г.);

• Сроки обработки ПДн в ЛПУ, как правило, определятся вышеуказанными приказами Минздрава, Госкомстата, а также приказом "О введении в действие положения о медицинском архиве лечебного учреждения".

При обработке ПДн пациентов медицинских учреждений следует учитывать, что Федеральный закон от 27.07.2006 г. № 152-ФЗ "О персональных данных" относит данные о состоянии здоровья пациента к специальной категории ПДн, обработка которых разрешается только при наличии письменного согласия субъекта ПДн или в исключительных случаях, предусмотренных статьей 10 данного закона (например, когда обработка ПДн необходима для защиты жизни или здоровья субъекта, либо жизни и здоровья других лиц, и получение согласия субъекта невозможно или когда обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну).

Характерной особенностью организации обработки ПДн в ЛПУ является то обстоятельство, что "Основы законодательства РФ об охране здоровья граждан" (ст.31) требуют предусмотреть в ИСПДн возможность предоставления пациенту в доступной для него форме информации о состоянии здоровья, включая сведения о результатах обследования, наличии заболевания, его диагнозе и прогнозе, методах лечения, связанном с ним риске, возможных вариантах медицинского вмешательства, их последствия и результатах проведенного лечения. Это требование вполне соотносится с положениями ст.143 Федерального закона "О персональных данных", определяющей право субъекта на доступ к своим ПДн. Так же следует обеспечить возможность информирования пациентов о способах и сроках обработки и хранения ПДн, а также лицах, имеющих к ним доступ.

Для обеспечения безопасности ПДн пациентов медицинских учреждений необходимы не только технические, но и организационные меры защиты. Особенность обработки ПДн заключается так же в том, что передача сведений, составляющих врачебную тайну, разрешена только с согласия пациента, за исключением случаев, предусмотренных ст. 61 "Основ законодательства РФ об охране здоровья граждан" (аналогичное требование ст. 6 Федерального закона "О персональных данных"). [36]

2.2 Информация подлежащая защите

Для определения средств и методов защиты необходимо определить структуру, тип и особенности информации, которая подлежит защите. Проведем анализ информационных потоков в медучреждении.

Одним из главных объектов защиты является врачебная тайна. В России взаимоотношения врача и пациента регулируются Основами законодательства Российской Федерации «Об охране здоровья граждан» и понятие врачебной тайны там так же присутствует. В частности, в статье 61 указано, что «информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну». Это означает, что без согласия пациента или его законного представителя (родителей, опекунов для подростков до 15 лет) не может разглашаться никакая информация, полученная врачами об этом человеке. И не важно, для чего эти сведения планируется использовать – для проведения исследований, публикаций в научной литературе, в учебном процессе медицинского ВУЗа или съемок теленовостей в больнице – эта информация конфиденциальна[30].

Необходимость в надежной защите этих сведений наиболее остро ощущают негосударственные клиники, частные медицинские учреждения, которые на сегодняшний день обладают лучшим техническим оснащением и могут предложить пациенту набор услуг, качественно отличающийся от предлагаемых в государственных поликлиниках и больницах и соответствующих передовым мировым стандартам. В связи с этим, в числе пациентов частных клиник встречаются иностранные гости (имеющие возможность общаться с медицинским персоналом на родном языке), крупные бизнесмены, политики, известные спортсмены, представители шоу-бизнеса, то есть – публичные фигуры. Интерес к ним со стороны публики, приобретающий, зачастую, причудливые формы, всегда был высоким, а эксклюзивная информация о «сильных и известных мира сего» ценилась на вес золота. Но не только праздным интересом читателей бульварной прессы подогревается обстановка вокруг VIP-персон. В сложившейся в нашей стране, на настоящий момент, экономической и политической обстановке, обладание врачебной (да и иной другой) информацией о конкуренте, и не важно - политик он или бизнесмен, звезда спорта или сцены, является реальным рычагом воздействия на оппонента.

Таким образом, использование беспроводных технологий и электронного документооборота накладывает на медиков значительные обязательства по сохранению этих данных в неприкосновенном виде, так как риск увидеть информацию о пациентах, размещенную в сети Интернет.

Естественно не только врачебная тайна и личные данные пациента являются объектом защиты. Если рассматривать частные клиники, то это уже коммерческое предприятие. И, следовательно, стоит рассматривать весь информационный комплекс (внутренние и внешние информационные потоки) как объект информационных атак. Рынок медицинских услуг имеет очень высокую конкуренцию. Конкурентная борьба зачастую ведется с применением «грязных» приемов, и это обуславливает интерес к перспективным направлениям, маркетинговым инициативам, планам работы, разрабатываемым конкурирующими компаниями. Конкуренты постоянно проявляют интерес к информации о сопернике: внутренняя обстановка в коллективе, кадровый состав, уровень доходности и зарплаты ведущих специалистов, дальние и ближние перспективы развития и другие аспекты, которые характеризуют бизнес-деятельность клиники.

В работе врача информация являет собой и инструмент и продукт работы, она должна быть объективной, полной и своевременной, а требования к обеспечению информационной безопасности должны сводиться к трем основным пунктам:

- недопущение несанкционированного доступа к собственным информационным ресурсам, а также к информации клиентов и партнеров, использующейся в работе

- противодействие намеренному или случайному вмешательству с целью уничтожения или модификации информации

- обеспечение непрерывности функционирования информационных систем, их аппаратных модулей и программного обеспечения

Задача сбора большего количества информации неразрывно связана с необходимостью использования технических средств. (анализаторами, датчиками, сенсорами и пр.), а хранение и передача данных является «обязанностью» технических средств, необходимо учитывать и технико-технологические угрозы, реализация которых повлечет за собой невосполнимую потерю информации и значительные затруднения (если не полную остановку) работы медицинского учреждения. Имеются в виду возможные отказы оборудования, причиной которых может быть как механическая поломка, отключение питания или программный сбой, так и умышленная порча либо случайные действия персонала, не

обладающего достаточной квалификацией.

Все рассмотренные направления информационных потоков можно представить в виде следующей схемы (рис. 2.1)

Рисунок 2.1 – Общая схема информационного ядра медицинского учреждения

2.3 Модель злоумышленника, анализ рисков

Для дальнейшего анализа и построения схемы защиты необходимо рассмотреть модель злоумышленника и оценить возможные риски.

Рассматривать риски будем на основе коммерческой организации – частной клиники или лечебно-профилактического учреждения

Возможные риски и их оценка приведены в таблице 1.

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие три качественных класса информационных активов:

- высокое влияние на бизнес (ВВБ) – влияние на этот тип активов может нанести организации катастрофический ущерб и поставить под сомнение возможность ее дальнейшего существования;
- среднее влияние на бизнес (СВБ) – влияние на этот тип активов хоть и не наносит катастрофический ущерб организации, но требует значительных ее изменений;
- низкое влияние на бизнес (НВБ) – влияние на данные активы не наносит ущерб организации, но, возможно, может потребовать ее незначительных изменений.

Таблица 1- Риски и их анализ

Информационный объект		**Подверженность воздействию**		**Уровень**
Название объекта	**Класс данных**	**Описание угрозы**	**Описание уязвимости**	**подверженности воздействию**
Информация о финансовых потоках и инвестициях	**ВВБ**	Несанкционированный доступ к финансовой информации путем физического взлома помещения с серверной машиной	Хищение данных вследствие отсутствия или нерабочего состояния средств безопасности и несвоевременного обновления или нерабочего состояния средств информационной защиты	5

Информация о сбытовой деятельности	**СВБ**	Несанкционированный доступ к информации о предоставляемых услугах и реализации деятельности	Хищение данных вследствие несвоевременного обновления средств защиты или их аварийного отключения. Необходимо рассматривать как полную утечку информации (например дамп БД) так и частичную (отдельные файлы, документы, списки)	4
Информация о бизнес-планах, дальние и ближние перспективы развития организации	**ВВБ**	Несанкционированный доступ к информации о бизнес-планах путем взлома ПК директора или главных менеджеров организации	Хищение данных вследствие несвоевременного обновления средств защиты или их аварийного отключения. Кража ПК или ноутбука. Копирование информации с помощью подкупа сотрудника	5

Конфиденциальная информация пациентов	**СВБ**	Несанкционированный доступ к информации о пациентах путем хищения данных, взлома защиты корпоративной сети	Хищение данных вследствие отсутствия или нерабочего состояния средств безопасности. Открытых точках доступа, физических и программных уязвимостей ЛВС организации	3

продолжение таблицы 1

Внесение умышленных неправдивых данных	**СВБ**	Изменение данных в назначениях, диагнозах, архивах данных о пациентах	В большинстве случаев реализуется подменой данных удаленным способом или посредством вовлечения сотрудников организации	3
Сведенья о структуре организации	**НВБ**		Хищение данных вследствие несвоевременного обновления защиты или их ав. отключения	1

Подверженность воздействию, помогает определить величину влияния нарушений конфиденциальности или целостности информации (табл. 2).

Таблица 2 -Влияние уровня воздействия и целостность актива

Уровень подверженности воздействию	**Конфиденциальность или целостность актива**
5	Серьезные повреждения или полный выход актива из строя (например данные, воздействие на которые, критически влияют на ведение бизнеса)
4	Серьезные повреждения, не приводящие к полному выходу актива из строя (например данные, воздействие на которые хоть и влияет довольно критически на ведение бизнеса, но не фатально)
3	Средние повреждения или ущерб
2	Незначительные повреждения или ущерб
1	Небольшие изменения или отсутствие изменений в видении бизнеса

Далее рассмотрим модель нарушителя, проведем классификацию возможных форм доступа и типов злоумышленников в разрезе информационных атак и шпионажа. Данные представлены в таблице 3.

Таблица 3 - Модель нарушителя

Ид.	**Наименование**	**Описание**

A1	Внешний злоумышленник (промышленный шпионаж)	Навыки и опыт использования уязвимостей и не декларированных возможностей ОС, распространенного прикладного ПО; опыт взлома подобных систем; намерение нанести ущерб компании; изначально отсутствуют какие-либо знания об инфраструктуре ИС организации; высокий технический уровень; практически неограниченные ресурсы; изначально не имеет доступа к данным пациентов и внутренним данным организации; время воздействия – от нескольких минут до нескольких часов; кража информации сопровождается взломом с проникновением.

A2	Внешний злоумышленник (хакер)	Навыки и опыт использования уязвимостей и не декларированных возможностей ОС, распространенного прикладного ПО; опыт взлома подобных систем; намерение нанести ущерб компании; изначально отсутствуют какие-либо знания об инфраструктуре ИС организации; высокий технический уровень; изначально не имеет доступа к данным организации; время воздействия краткосрочно – от нескольких секунд до нескольких минут.
B1	Внутренний легальный пользователь (сотрудник)	Средний технический уровень; знание внутренней инфраструктуры ИС; легальный доступ в ИС (имя пользователя и пароль); намерение нанести ущерб компании; права ограничены занимаемой должностью; изначально не имеет доступа к данным; срок воздействия может быть очень длительным: до 0.5 года при конкретном заказе на информацию, на протяжении нескольких лет в случае инсайдера торгующего внутренней информацией организации

		Средний технический уровень; физический доступ к ИС; изначально отсутствуют какие-либо знания об инфраструктуре ИС; намерение нанести ущерб компании;
B2	Внутренний пользователь (гость)	изначально не имеет доступа к данным; время воздействия может быть разным, в здание злоумышленник проникает легально например под видом обслуживающего персонала или партнера в бизнес отношениях (например поставщика). Для входа в систему применяются хакерские приемы или подкуп сотрудников с целью получения хотя бы минимальных прав доступа

Как показывает практика, современные компьютерные системы подлежат следующим наиболее распространенным угрозам [1-3]:

1. непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц (35%)
2. кражи и фальсификации. В большинстве случаев, которые расследовались, виновными оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты (15%);
3. «обиженные сотрудники» - нынешние и бывшие, например, путем внедрения «логической бомбы», введение неверных данных, удаление или модификации данных (36%);
4. угрозы окружающей среды (отключение связи, пожар и т.д.)(10%);
5. действия хакеров и преступников, которые могут осуществлять обман путем создания ложных или модифицированных подлинных документов (информации)(4%).

Рисунок 2.2 – Распределение угроз по типу нарушителя

В процессе реализации угроз нарушители и преступники могут реализовывать следующие стратегии:

1. выдачи себя за другого пользователя, чтобы снять с себя ответственность;
2. выдачи себя за другого пользователя, чтобы использовать его полномочия с целью:
3. формирование ложной информации;
4. изменения истинной информации;
5. применение ложного удостоверения для получения несанкционированного доступа (НСД);
6. санкционирование ложных обменов информацией или их не подтверждения;
7. отказ источника от факта формирования и передачи информации;
8. утверждение источника о том, что получателю была отправлена информация, в том числе в определенное время, что на самом деле не была отправлена или отправлена в другое время;
9. отказ получателя от факта получения информации, хотя на самом деле она была получена, или ложное утверждение о время ее получения;
10. утверждение о том, что информация получена от определенного пользователя, хотя на самом деле она сформирована самим же нарушителем;
11. нарушение конфиденциальности;
12. несанкционированное расширение (изменение) своих полномочий;
13. несанкционированное изменение полномочий других лиц (ограничение или расширение);
14. введение в систему или активизация вирусов или других "вредных" программ с целью перехвата ключей и паролей, а также модификации (незаметно) документов;
15. попытка помешать передаче сообщений другим пользователям, в частности, внесение сообщению скрытых помех для того, чтобы это сообщение при аутентификации было опровергнуто;
16. модификация программного обеспечения, например, путем добавления новых функций;
17. подрыв доверия к протоколу путем вызова нарушений или принуждения других возбудить протокол путем введения ложной информации и т.д.

Защищать инфраструктуру, состоящую из таких устройств, нужно от следующего диапазона угроз: от эпидемиологических заражений, от таргетированных атак, от взломов и от действий собственных сотрудников. Вредоносные действия сотрудников, в свою очередь, делятся на две категории - это использование

компьютеров малограмотными с точки зрения применения информационных технологий людьми, причиняющими вред системе по неосторожности, и злонамеренные действия инсайдеров от кражи или модификации отдельных данных до полного уничтожения системы.

Но, согласно данным статистики, до 85% проблем, возникающих у компаний – итог проявления негативной активности собственного персонала. И с точки зрения обеспечения безопасности, внутренний враг гораздо опаснее врага внешнего, потому как нелояльному, обиженному (и не важно, является ли причина его обиды объективной или же она – продукт его воображения) сотруднику или авантюристу «по жизни» не нужно искать пути проникновения в помещения и разрабатывать хитроумные ходы для получения паролей. Он уже внутри, он многое знает и умеет и, главное, он обладает четкой целью, идущей вразрез с интересами работодателя.

Два примера: 26 октября 2005 г. в Интернете появилось объявление о продаже базы данных одного из крупнейших регистраторов России – компании «НИКойл». Этот регистратор ведет реестры акционеров таких гигантов, как «Лукойл», МТС, «Скайлинк» и еще нескольких сотен корпораций национального масштаба[33]. Спустя всего неделю в продажу поступила база «Налоговая инспекция – 2004», содержащая, как легко догадаться, информацию о доходах москвичей за 2004 год.

Детали этих двух и множества других инцидентов, связанных с разглашением конфиденциальной информации, позволяют сделать неутешительный вывод: почти все утечки происходят с участием инсайдеров – сотрудников компании и фирм, имеющих доступ к конфиденциальной информации в силу служебных обязанностей.

Недостаточный контроль над действиями своих же сотрудников часто перерастает в серьезные проблемы для предприятия. Последствия таких инцидентов очень плачевны: прямые убытки и снижение числа клиентов сопровождаются штрафами и судебными преследованиями со стороны регулирующего органа. Таким образом, над всеми операциями с чувствительными данными должен быть установлен прозрачный, но жесткий контроль[26].

На данный момент можно смело утверждать, что поддержание режима информационной безопасности, как состояния защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести

неприемлемый ущерб субъектам информационных отношений (в т. ч. владельцам и пользователям информации и поддерживающей инфраструктуры) [27], находится в тесной и неразрывной связи с другими направлениями обеспечения жизнедеятельности медицинского учреждения, такими как:

- физическая безопасность (обеспечение контроля доступа в учреждение и помещения с находящимися в них компьютерами, сетевым оборудованием, иной информационно-вычислительной техникой и т. д.),

- технико-технологическая безопасность (соблюдение правил эксплуатации и использования, соблюдение техники безопасности и т. д.)

- кадровая безопасность (оценка и подбор персонала, повышение квалификации, изучение уровня лояльности и благонадежности и т. д.)

- нормативно-правовые меры (издание распоряжений, приказов, разработка инструкций, правил, алгоритмов и планов и схем действий персонала и т. д.)

Конечно, приведенный перечень не полон и нуждается в расширении и детализации.

ГЛАВА 3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ

Сегодня существует огромное количество средств и методов защиты информации. Естественно степень защиты, в первую очередь, определяется ценностью информации, а средства и методы – особенностями функционирования информационной среды организации и наличными информационными потоками. В целом средства защиты можно разделить на:

- технические;

- аппаратные;

- программные;

- программно-аппаратные;

- с привлечением человеческих ресурсов.

Технические и аппаратные средства включаю различные системы «антипрослушки», противостояния утечке информации по физическим каналам: скрытая видео съемка, прослушивание кабинетов, телефонов и т.д. Сюда также стоит отнести контрольно пропускные системы, системы видеонаблюдения, электронные замки. Эти средства не являются темой нашего исследования и в дальнейшем рассматриваться не будут.

Аппаратные средства включаю специальные приспособления и техническое оснащение для защиты информационных потоков в сетях.

Человеческие ресурсы подразумевают обеспечение охраны с использованием человеческих сил (охранников), визуальный контроль и мониторинг, пропускные системы с внешним человеческим контролем. Высокий уровень защиты можно обеспечить только комплексным применением ряда различных мер, но основное внимание в работе мы уделим именно программным и программно-аппаратным средствам и методам защиты.

Программные методы

- Аутентификация и разграничение доступа

Одним из направлений защитных технологий данного класса является аутентификация, которая позволяет сопоставить вводимые пользователем пароль и имя с информацией, хранящейся в базе системы защиты. При совпадении вводимых и эталонных данных разрешается доступ к соответствующим ресурсам.

- Антивирусы

Антивирусная защита является одной из тех первых технологий защиты электронной информации, которая до сих пор активно используется как и рядовыми пользователями, так и крупными предприятиями. Так и рассматриваемое предприятие не исключение. На каждом компьютере и серверной машине стоит антивирус, который предохраняет информацию от посягательств различных вредоносных программ.

- Межсетевые экраны

Межсетевой экран это многофункциональный комплекс, который помогает решить множество задач — от межсетевого экранирования и балансировки нагрузки до

контроля пропускной способности и управления динамическими адресами.

- Цифровые водяные знаки

Цифровые водяные знаки (ЦВЗ) используются для защиты компьютерных файлов (в основном фото-документов), которые представляют собой объекты авторского права. Они представляют собой специальные метки, внедряемые в файл, в цифровое изображение или цифровой сигнал в целях контроля их правомочного использования.

Невидимые цифровые водяные знаки представляют собой встраиваемые в компьютерные файлы вставки, не воспринимаемые человеческим глазом или ухом. Выделены следующие требования для ЦВЗ:

- незаметность для пользователей;
- индивидуальность алгоритма нанесения (достигается с помощью стеганографического алгоритма с использованием ключа);
- возможность для автора обнаружить несанкционированное использование файла;
- невозможность удаления неуполномоченными лицами;
- устойчивость к изменениям носителя-контейнера (к изменению его формата и размеров, к масштабированию, сжатию, повороту, фильтрации, введению спецэффектов, монтажу, аналоговым и цифровым преобразованиям).
- Шифрование и криптография – программные средства, основанные на специальных криптоалгоитмах. Предназначением данных программ является обеспечение защиты информации в том случае, если она все же попала в руки злоумышленника. Эффект достигается за счет того, что информация хранится и передается не в открытом, доступном для понимая злоумышленника виде, а в зашифрованном виде. То есть даже получив доступ к файлам злоумышленник не сможет получить доступ к информационной сути файла.

Аппаратные методы

- Криптотелефония

Криптотелефония используется для защиты данных в мобильных телефонах и ПК. Зашифрованную информацию с помощью криптотелефонии невозможно не только расшифровать, но и перехватить стандартными средствами. Естественно все

переговоры на разных уровнях нет смысла защищать с помощью таких специализированных средств, но на высшем управленческом или государственном уровне эти технологии вполне могут быть использованы.

Основные характеристики криптотелефонии:

- Симметричный алгоритм шифрования гарантированной стойкости, длина ключа -256 бит
- Асимметричный алгоритм шифрования на основе эллиптических кривых с длиной ключа 384 бит
- Разовые сеансовые ключи - стираются в конце сеанса
- Комбинированный метод вычисления с помощью алгоритма Диффи-Хэллмана на эллиптических кривых и полной ключевой матрицы
- Аутентификация сторон в режиме шифрования телефонных разговоров, защита от атаки «человек посередине» (MITM)
- Защита от несанкционированного доступа и утраты
- Использование протокола IPSec в туннельном режиме для связи с SIP-сервером

Программно-аппаратные методы

- Технология VPN

Для защиты информации между собственными подсетями и компьютерами и при передаче адресату может быть использована технология виртуальных защищенных сетей VPN. С помощью данной технологии компьютеры могут идентифицироваться, как «обезличенные» узлы сети (по IP-адресу) и как рабочие места заданных индивидуальных пользователей (такая идентификация производится, как правило, по сертификату пользователя). Для обеспечения защиты могут использоваться множественные алгоритмы шифрования, сложные конфигурации туннелей и защищенных периметров.

Криптографическая стойкость технологии обеспечивается применением соответствующих криптографических алгоритмов. Гибкость обеспечивается применением множества сценариев защиты информации (от периметрических сценариев до защиты трафика отдельных приложений из конца в конец), подбором индивидуальной политики защиты при необходимости это возможно для каждого, отдельно взятого сетевого соединения.

Схематически методы защиты представлены на схеме (приложение 1)

ГЛАВА 4 МОДЕЛЬ ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА ПО ЗАЩИТЕ ДАННЫХ

4.1 Анализ информационных потоков

Под информационными потоками подразумевается физическое перемещение информации от одного сотрудника предприятия к другому или от одного подразделения к другому. В целом информационные предприятия можно подразделить на собственные (внутренние) и внешние. Собственное информационное поле объединяет информацию, зарождающуюся внутри предприятия. В свою очередь внешнее информационное поле касается рыночной среды, внешних условий, в которых работает организация.

К внутренней информации следует относить:

- данные бухгалтерского учета и другой обязательной отчетности;
- первичные документы бухгалтерского, торгового и оперативного учета;
- приказы и распоряжения руководителя и менеджеров всех звеньев (письменные и устные);
- данные внутреннего документооборота (бумажного и электронного);
- результаты собственного анализа финансово-хозяйственной деятельности;
- другие данные (например, результаты анкетирования сотрудников предприятия)
- результаты обследований и история болезни пациентов.

Последний пункт имеет отдельное значение. Если злоумышленник получает доступ к информации, описанной в предыдущих пунктах – это чревато частичным подрывом экономического положения организации, информированностью конкурентов о текущем положении в организации. Последний пункт может не только стать предметом многотысячных (возможно многомиллионных) судебных исков, но и серьёзно подорвать репутацию медицинского учреждения вплоть до полной потери рынка и клиентов.

В целом, МЦ «Danke» имеет вполне типичную и налаженную структуру внутренних информационных потоков. Однако стоит отметить, что их качество напрямую зависит от четкой организации управления и постоянного контроля.

4.2 Модель защиты данных "Как есть" (текущее состояние)

На данный момент в МЦ «Danke» защита информации происходит на элементарном уровне. Сотрудники не прибегают к надежным методам криптографической защиты, а предпочитают использовать более обыденные и не всегда надежные методы, такие как защита документа или архива с данными паролем.

Такие способы защиты не всегда могут предохранить данные от взлома, так как методов дешифровки паролей существует огромное количество, да и много чего зависит от уровня сложности самого пароля, о чем сами сотрудники могут забывать.

На рис. 4.1 –4.2 показаны модели управления информационной защитой «как есть».

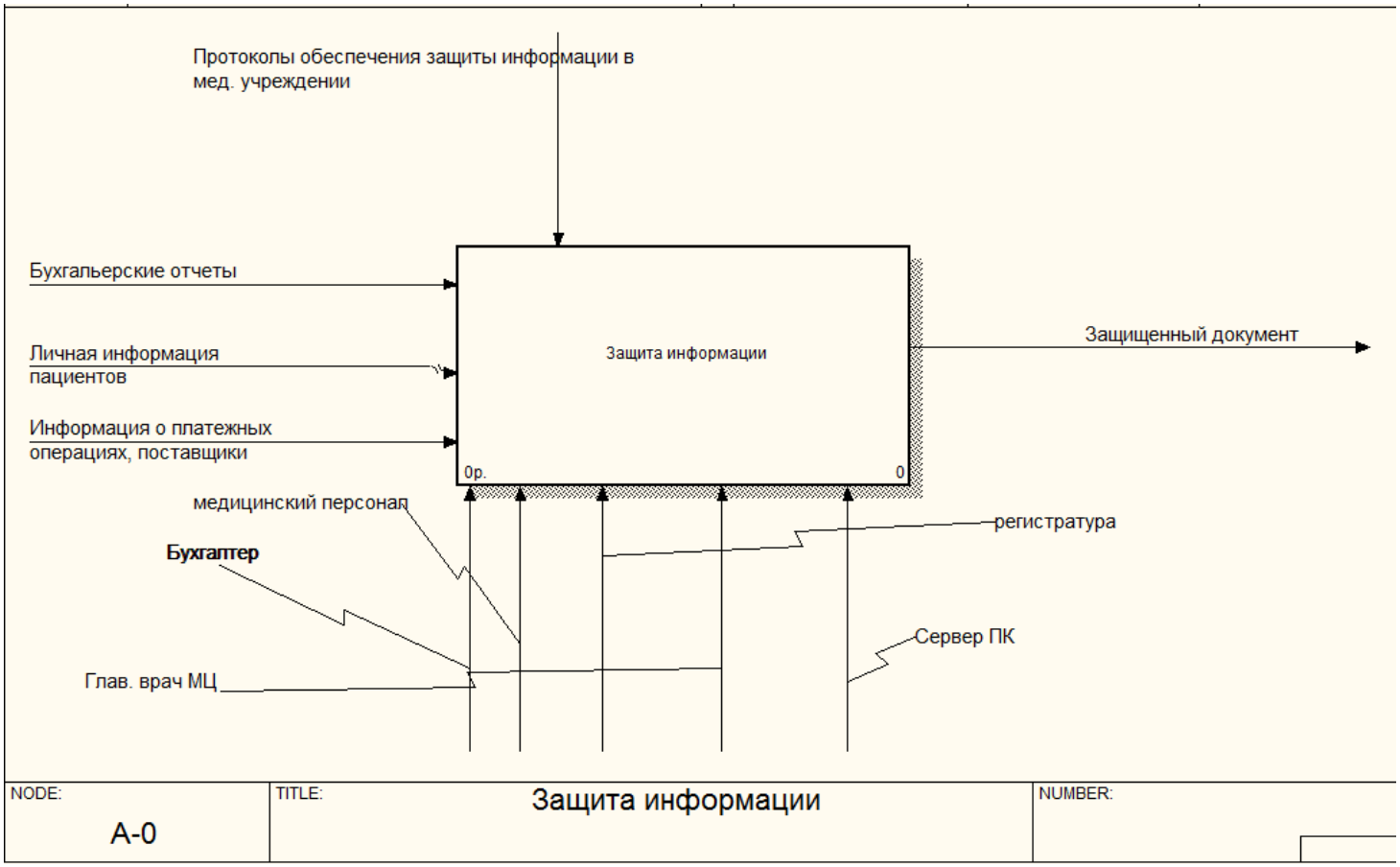

Рисунок 4.1 - Диаграмма первого уровня управления информационной защитой в МЦ «Danke»

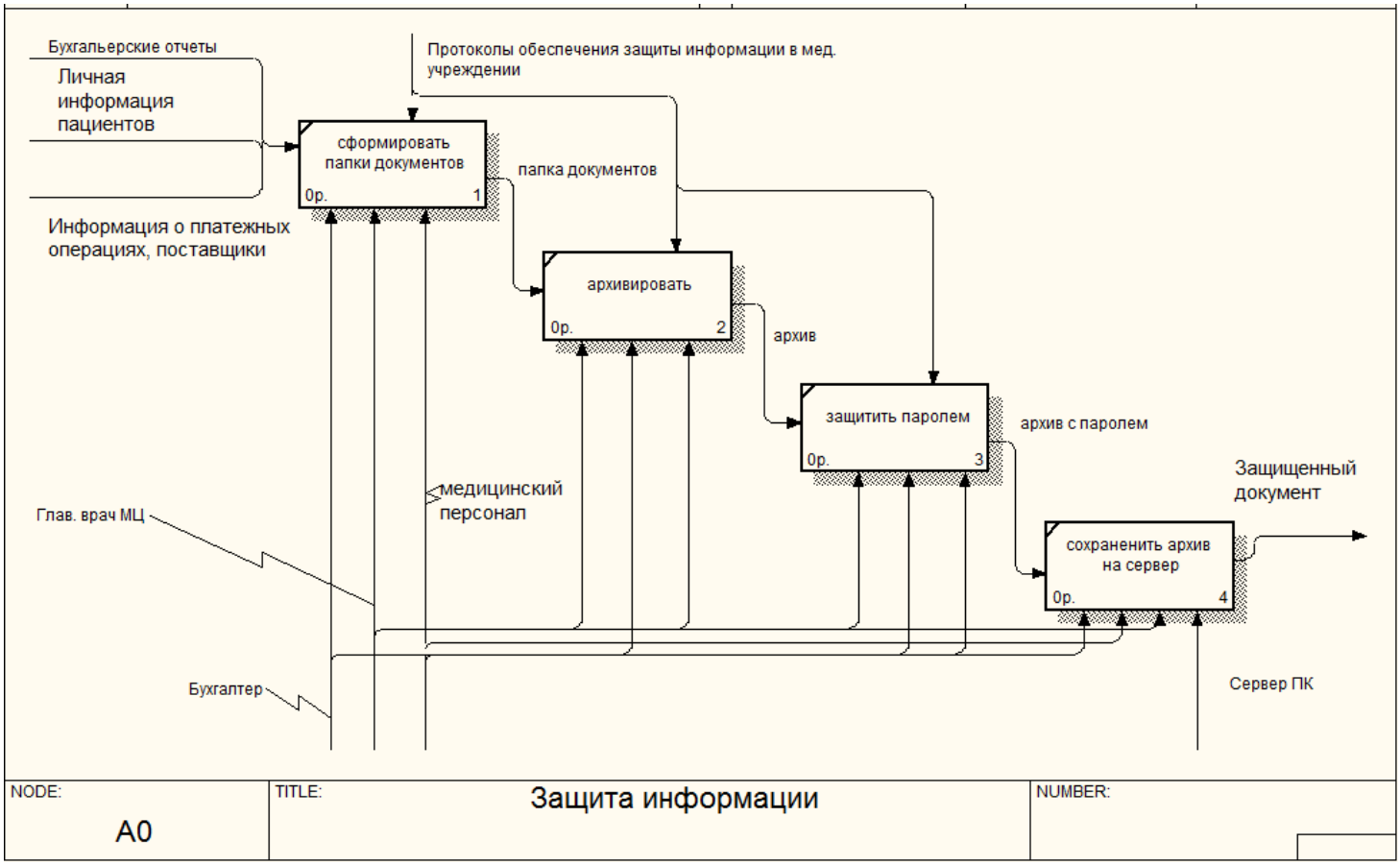

Рисунок 4.2 - Диаграмма второго уровня управления информационной защитой. Декомпозиция

Информацию, которую нужно защитить внутри информационной среды МЦ можно распределить по категориям важности таким образом:

- важная незаменимая информация, наличие которой необходимо для функционирования системы (организации);
- важная информация – информация, которая может быть заменена или восстановлена, но процесс ее восстановление тяжелый и связанный с большими затратами;
- полезная информация – информация, которую трудно восстановить, однако система (организации) может достаточно эффективно функционировать и без нее;
- личная информация пациентов;
- информация, которая является коммерческой тайной.

Особое внимание стоит выделить информацию, связанную с личной информацией пациентов и их медицинской историей, на второе место стоит поставить информацию, связанную с коммерческой тайной и дать ее точную характеристику. Под коммерческой тайной понимаются сведения связанные с особенностью технологий, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам.

4.3 Модель защиты данных "Как будет" (после внедрения программного комплекса)

В качестве продукта для внедрения рассматриваются альтернативы: собственная разработка или готовый продукт (например - Max File Encryption). Мы рассматриваем только модель внедрения защитного комплекса на основе использования программных продуктов для обеспечения ИБ, объемы работы не позволяют детально рассматривать сами продукты.

После внедрение системы методика работы зашиты закрытой электронной информации изменится кардинально в лучшую сторону. Теперь, помимо защиты документов паролем, появилась возможность защиты криптографическими методами и методами стеганографии. Такой подход позволяет сокрыть информации от доступа злоумышленника даже при взломе основного файла с паролем, где находятся документы.

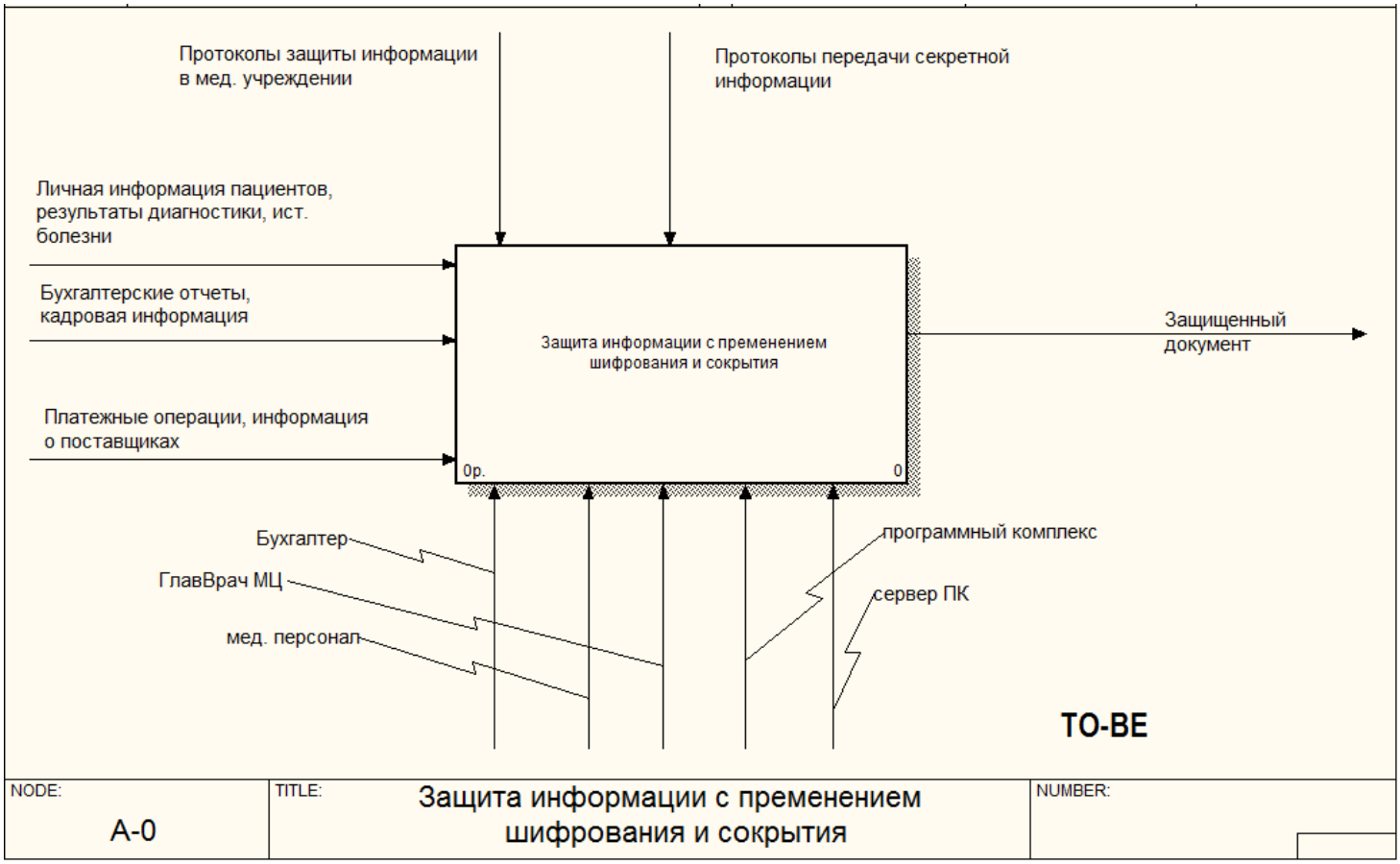

Рисунок 4.3 - Контекстная диаграмма (TO-BE)

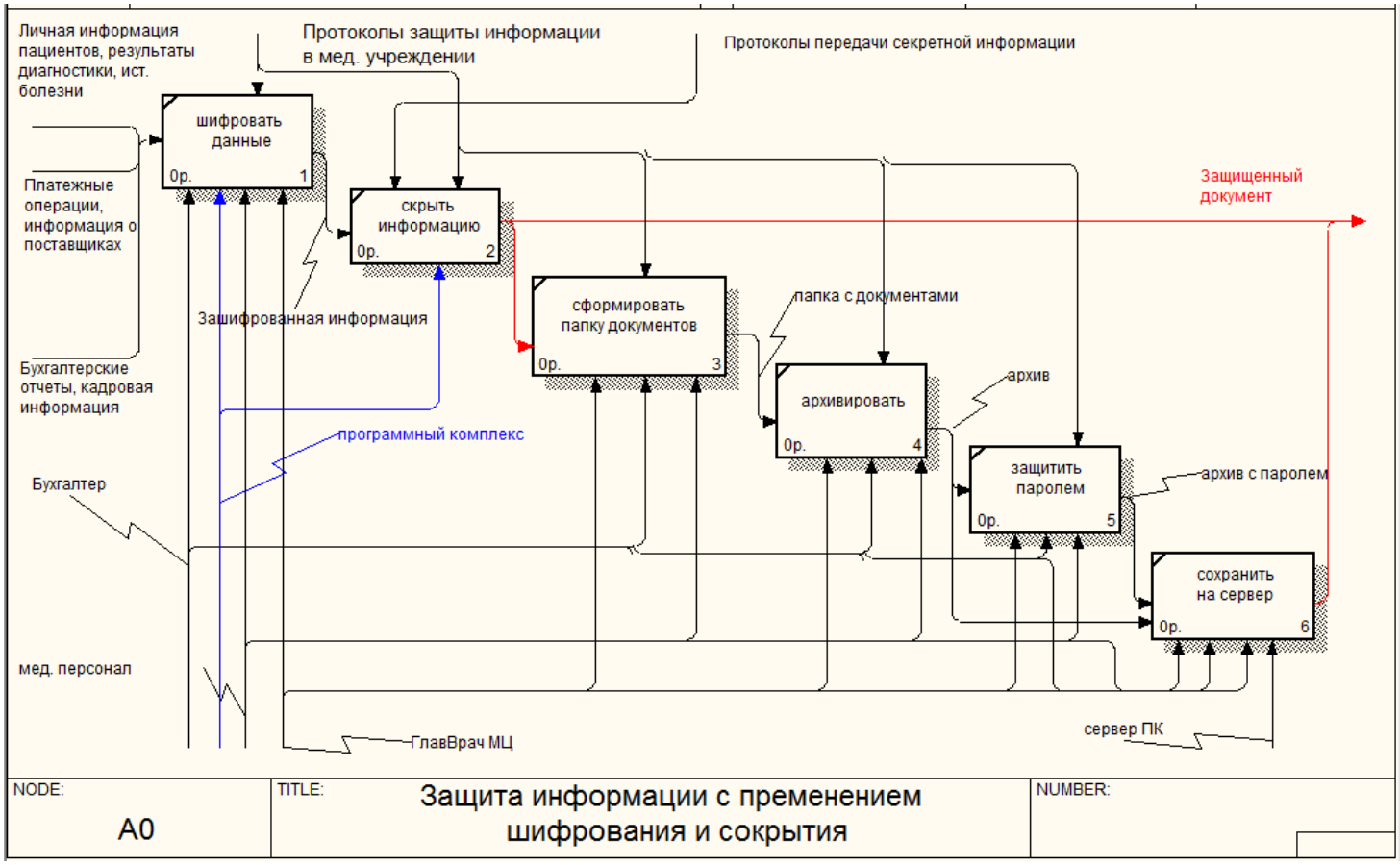

Рисунок 4.4 - Диаграмма деятельности второго уровня защиты информации после внедрения системы. Декомпозиция

За основные операции по повышению защиты отвечают этапы 1-2 (блоки), уже после второго блока в качестве исходящего потока мы имеем защищенный документ. Далее возможны два варианта: отправка информации по внешним каналам (сеть, почтовые сервисы и т.д.) или дальнейший этап внутреннего документооборота. На этапе 5 уровень защиты дополняется наложением пароля на архив. Этот этап уже не является обязательным и после этапа 4 (Архивирование) архив сразу может быть отправлен на внутренний сервер (минуя парольную защиту). Все эти взаимодействия отображены на диаграмме (рис 4.4)

На следующей диаграмме представлены основные прецеденты использования внедряемой системы пользователем

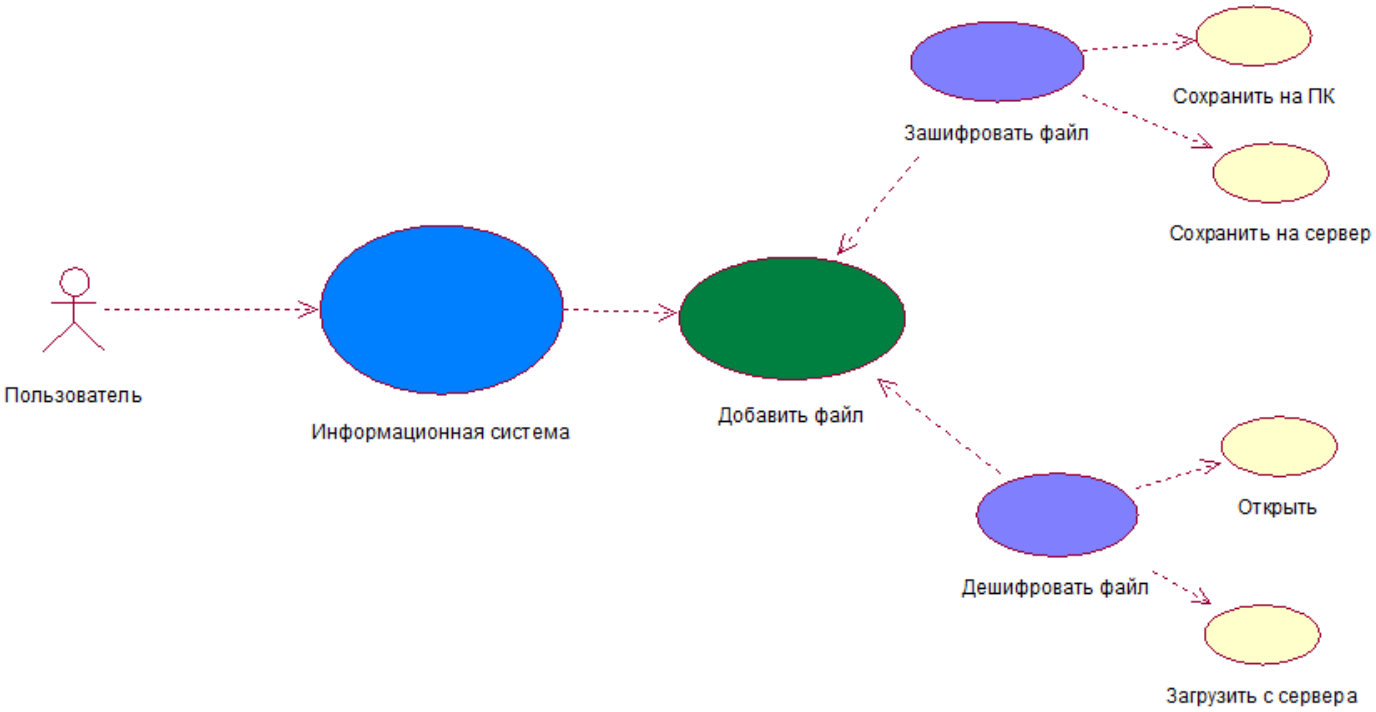

Рисунок 4.5 - Варианты использования системы программной защиты информации

Как отмечалось ранее, информацию стоит защищать не только от взлома или несанкционированного доступа третьих лиц, но и от техногенных катастроф, сбоев и подобных факторов. В данном случае речь идет не о доступе к информации злоумышленника, а о физической потере данных.

Для упреждения таких ситуаций наиболее распространённым и надежным способом является дублирование информации. Желательно что бы дублирующий сервер был как можно менее зависим от общей информационной среды и имел определенный уровень физической защиты.

Как видно с приведенных диаграмм, подход к защите важной информации стали более прогрессивным и надежным. Теперь стоит уточнить и указать более точный спектр применения внедряемой программы.

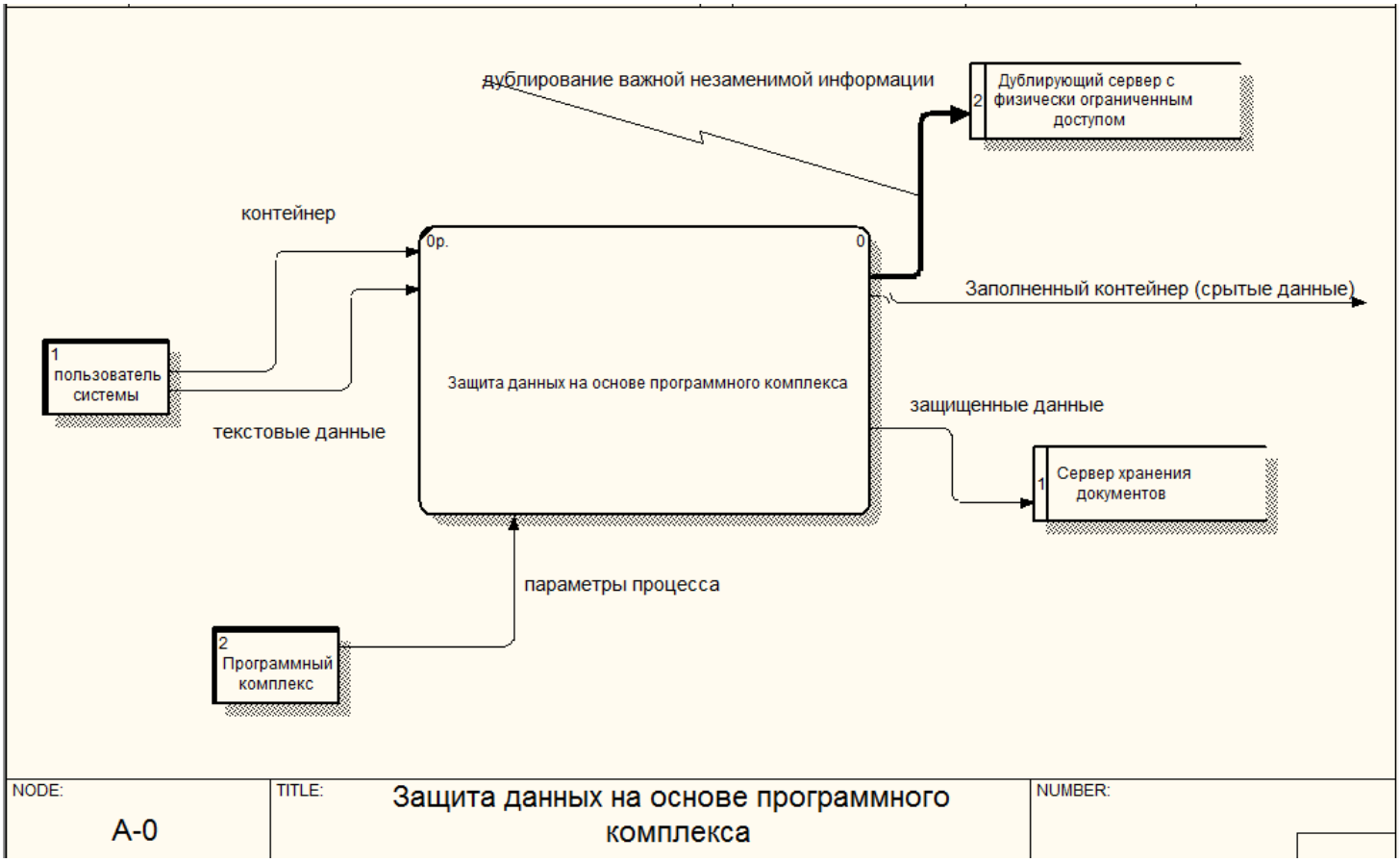

Рисунок 4.6 – DFD диаграмма

Как правило, любые документы, связанные с историей болезни пациента или данными диагностики, хранятся на серверной машине в электронном виде. Под каждого пациента создан свой каталог с документами (это может быть и БД), в котором имеется вся история, начиная от регистрации в ИС медицинского учреждения, заканчивая смертью пациента. Да и в этом случае, по правилам медицинских учреждений, информация не удаляется из системы, а оправляется в архив, где должна сохраняться определенный срок. Эту информацию, порой, нужно предоставлять различным отделениям МЦ, то есть создавать ее копии. Или отправлять информацию по внешним каналам в случае территориально - разнесенной организации отделений МЦ. В этом случае крипто защита данных имеет особое значение. Другим примером может служить воровство информации внутренними сотрудниками. В этом случае криптозащиту стоит комбинировать с политиками доступа и другими организационными средствами защиты данных.

ВЫВОДЫ

Учитывая вышеизложенное, и говоря о применении в работе медицинских учреждений последних достижений компьютерных и телекоммуникационных технологий, необходимо осознавать следующее – несмотря на то, что эти технологии приносят неоспоримую пользу и качественно облегчают труд врачей, у этого процесса есть и обратная сторона, о которой говорилось в начале: на лицо зависимость человека от высокотехнологичного оборудования, накладывающая огромную ответственность на специалистов, поддерживающих функционирование этого оборудования в частности и жизнедеятельность медицинского учреждения в целом, а так же повсеместно возникающая необходимость заниматься решением задач ИБ.

Любую угрозу информационной безопасности необходимо первоначально выделить и классифицировать. Классификация нужна для своевременного применения различных действий для устранения причин, которые могут повлечь к повреждению информации.

Информационный шпионаж и утечка персональной информации пациентов и сотрудников однозначно критично скажется как на отдельно взятом человеке так и на работе организации в целом.

Для повышения уровня защищенности и противостоянию информационных угроз необходимо применять комплексные меры защиты, которые включают:

- организационные;

- программные;

- программно-аппаратные;

- технические.

Курсовая работа состоит из трех разделов.

В первом рассмотрена структура исследуемой организации, анализ информационных потоков и информационных угроз. Отдельным пунктом в первом разделе рассмотрена правовая база, которая регламентирует и требует от медицинского учреждения защищать конфиденциальную информацию пациентов.

Второй раздел является основным в данной работе. Он посвящен классификации угроз и оценке рисков для организации, то есть в этом разделе раскрываются целевые вопросы согласно теме работы.

Третий раздел рассматривает различные средства защиты, тут приводится только общая классификация подходов, так как основной темой работы является анализ угроз.

В четвертом разделе моделируется текущий уровень и изменения после внедрения системы, при помощи структурного моделирования анализируются основные преимущества от внедрения системы.

Поставленные во введении, задачи и цели достигнуты в полном объеме.

СПИСОК ЛИТЕРАТУРЫ

1. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. СПб.: Изд-во "Альпина Паблишерз" 2011. - 286 с.
2. Политики безопасности компании при работе в интернет / Петренко С.А., Курбатов В.А.; М: ДМК Пресс, 2011. - 396 с.
3. Информационная безопасность часть 1 / Блинов А.М; СПб.: Изд-во "СПбГУЭФ" 2010. 346 с.
4. Технологии и продукты Microsoft в обеспечении информационной безопасности / Авдошин С.М., Сердюк В.А., Савельева А.А.Интернет СПб.: Изд-во - Университет Информационных 2011. - 455 с.
5. Служба Active Directory. Ресурсы Windows Server 2008 / Стен Реймер, Конан Кезема, Майк Малкер, Байрон Райт СПб.: Изд-во "Лидер" 2009 - 470 с.
6. Active Directory подход профессионала / Зубанов Федор; М.:"Русская редакция" 2003 - 342 с.
7. Информационная безопасность предприятия: цикл статей. URL: http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya (дата обращения: 6.12.2015)
8. ИТ в медицине// Ирина Шеян Источник: Computerworld Россия/MedIT 28.03.2014 Электронный ресурс [http://www.osp.ru/] дата обращения: 4.12.2015)
9. «Бремя защиты», Эрик Ландквист, PC WEEK/RE, № 37, 11 октября 2005 г.
10. «О чем должен молчать врач», Алексей Водовозов, http://mednovosti.ru/main/2004/07/26/privacy
11. «Мобильные устройства и пользователи», Александр Семенов, «PC WEEK/RE», № 41, 8 ноября 2005 г.

12. Вячеслав Лупанов, руководитель отдела системного ПО компании «Гелиос Компьютер»,http://www.cnews.ru/reviews/articles/index.shtml?2005/12/02/192675_2 «12 самых громких случаев ИТ-воровства в России»
13. «Основы информационной безопасности», Галатенко В. А., Лекция№1, http://publish.abitu.ru
14. http://www.kaspersky.ru – Концепция информационной безопасности
15. http://skif.pereslavl.ru/psi-info/interin/interin-publications/pib.pdf - Проблемы информационной безопасности в медицинских информационных системах
16. http://www.cis21.ru/default.aspx Центр Информационной Безопасности
17. ФСТЭК: Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).
18. В.Ф. Шаньгин – Информационная безопасность компьютерных систем и сетей, Москва, ИД «ФОРУМ» - ИНФРА-М, 2008 г.
19. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г.).
20. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
21. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных; Учебник для высших учебных заведений / Под ред. проф. А.Д. Хомоненко. - 4-е изд., доп. и перераб. - СПб.: КОРОНА принт, 2004. - 736 с. ISBN 5-7931-0284-1.
22. Медицинская документация, форма № 025/у-87 утверждена Минздравом СССР № 1338 1987 г.
23. ФСТЭК. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (выписка).
24. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. Волгоград: Изд-во ВолГУ, 2002. – 122с. – (Серия «Информационная безопасность»). ISBN 5-85534-640-4.
25. ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения.
26. Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения. - М.: ИД «ФОРУМ»; ИНФРА-М, 2008. - ISBN 978-5-8199-0342-1.

27. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2.
28. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004. - 544 с. ISBN 5-8291-0408-3.
29. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288 с: ил. ISBN 5-94157-331-6.
30. Э. Мэйволд – Безопасность сетей [Электронный ресурс] – Режим доступа: http://www.intuit.ru/department/security/netsec/11/1.html.
31. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г.).
32. Информационный бюллетень Jet Info №5 (192)/2009.
33. http://www.newsru.com/finance/31oct2005/reg.html

Приложение 1 Способы и средства защиты информации