Закон «О персональных данных» с точки зрения разработчика медицинских информационных систем.

Аннотация

В настоящем документе автором рассмотрены особенности практического исполнения требований Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных" с точки зрения разработчика медицинских информационных систем. А так же исполнения требований иных руководящих документов по данной тематике.

Оглавление

1. Введение 4
1.1. От автора 4
1.2. Цель документа 5
2. Исходные данные 5
2.1. Архитектура МИС 5
2.2. Функционал МИС 7
3. Классификация данных используемых в МИС и типа обработки 8
3.1. Категория данных 8
3.2. Категория данных 9
3.3. Обработка персональных данных 10
4. Проблемы и опыт выполнения требований 11
4.1. Ограничение доступа к нормативно-правовым документам. 12
4.2. Необоснованно жесткие требования к разработчикам информационных систем 12
4.3. Длительность и высокая стоимость сертификации информационных систем 16
4.4. Существенные затраты на аттестацию рабочих мест пользователей со стороны заказчика МИС 18
5. Пример простого расчета затрат в связи с новыми требованиями нормативных документов по защите персональных данных. 19
6. Заключение 19

1. Введение

1.1. От автора

В соответствии с требованиями ст.25 п.3 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных" в 2010 году истекает срок отведенный на приведение в соответствии с требованиями вышеупомянутого закона всех информационных систем созданных до дня вступления закона в силу.

Автор документа с 2005 года является сотрудником компании, которая занимается разработкой медицинских информационных систем. И поэтому данных закон имеет к нему непосредственное отношение, т.к. регулирует сферу с которой работает компания. Тем не менее в целом документ будет разрабатываться без точного указания на имени компании, а так же других организаций, которые будут упоминаться при описании опыта исполнения закона.

В соответствии со страховой программой автор так же обслуживается в одном из коммерческих ЛПУ оборудованных медицинской информационной системой

(МИС), где в частности используется МИС для подготовки и формирования печатной истории болезни, а так же хранятся ее копии в электронном виде.

Сразу хочу подчеркнуть, что автора ни в коем случае нельзя отнести к противникам закона. Как пациент ЛПУ, персональные данные которого обрабатываются в МИС, я поддерживаю общую проблему, которая обозначена данным законом. Однако как у специалиста по информационным технологиям и сотрудника компании разработчика у меня есть целый ряд вопросов и проблем, которые я хотел бы поднять в этом документе.

Так же хочу подчеркнуть, что я не являюсь юристом или человеком, который в постоянно и профессионально занимается изучением законодательства по указанному вопросу. Поэтому замечания по тексту приветствуются.

1.2. Цель документа

Целями данного документа являются:

- Представить опыт, полученный нашей компанией при подготовке к исполнению требований закона «О персональных данных» в письменном виде;
- Продемонстрировать проблемы, возникающие при реализации требований закона.

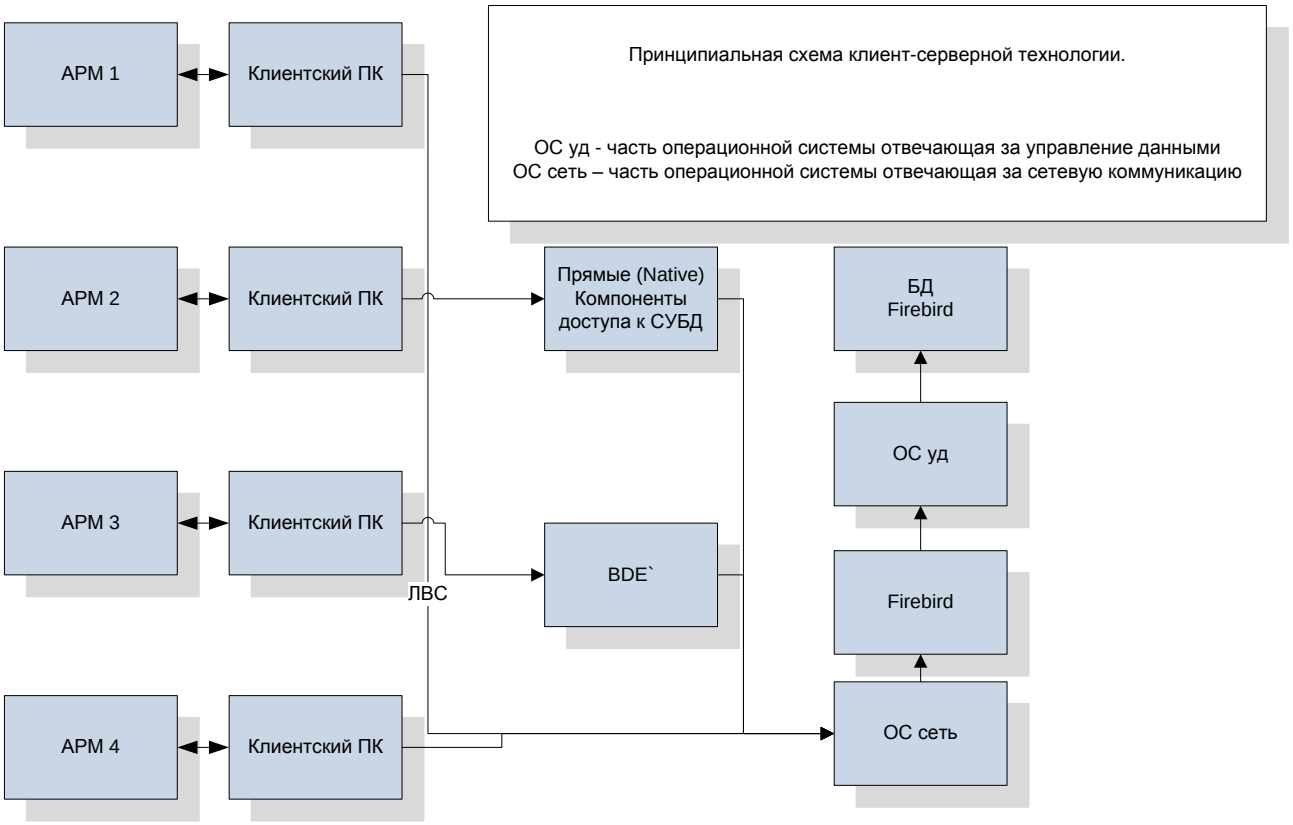
Документ разрабатывался по заданию руководства компании. Окончательно неизвестно для чего будет применяться данный документ, поэтому стиль документа остается свободным.

2. Исходные данные

С 1998 года нашей компанией разрабатывается МИС, предназначенная для ЛПУ различного профиля и формы собственности.

2.1. Архитектура МИС

Мы используем клиент серверную технологию. В качестве СУБД используется свободная СУБД Firebird. В качестве операционной системы сервера базы данных могут использоваться либо ОС Microsoft Windows либо LINUX системы. Клиентская часть (непосредственно приложение) может работать под управлением Windows.



Система устанавливается в ЛПУ, рабочие места персонала обеспечиваются своим АРМ, характерным для конкретного должностного лица. Все пользователи системы работают с единой базой данных.

В случае, если организация состоит из территориально-распределенных подразделений (филиалов), то каждое подразделение обеспечивается собственной инсталляцией системы и собственной филиальной базой данных (ФБД).

Все данные о работе подразделений в режиме реального времени поступают в головное подразделение. Таким образом, руководство учреждения всегда обладает информацией о работе всех подразделений для получения сводной и детальной статистической информации.

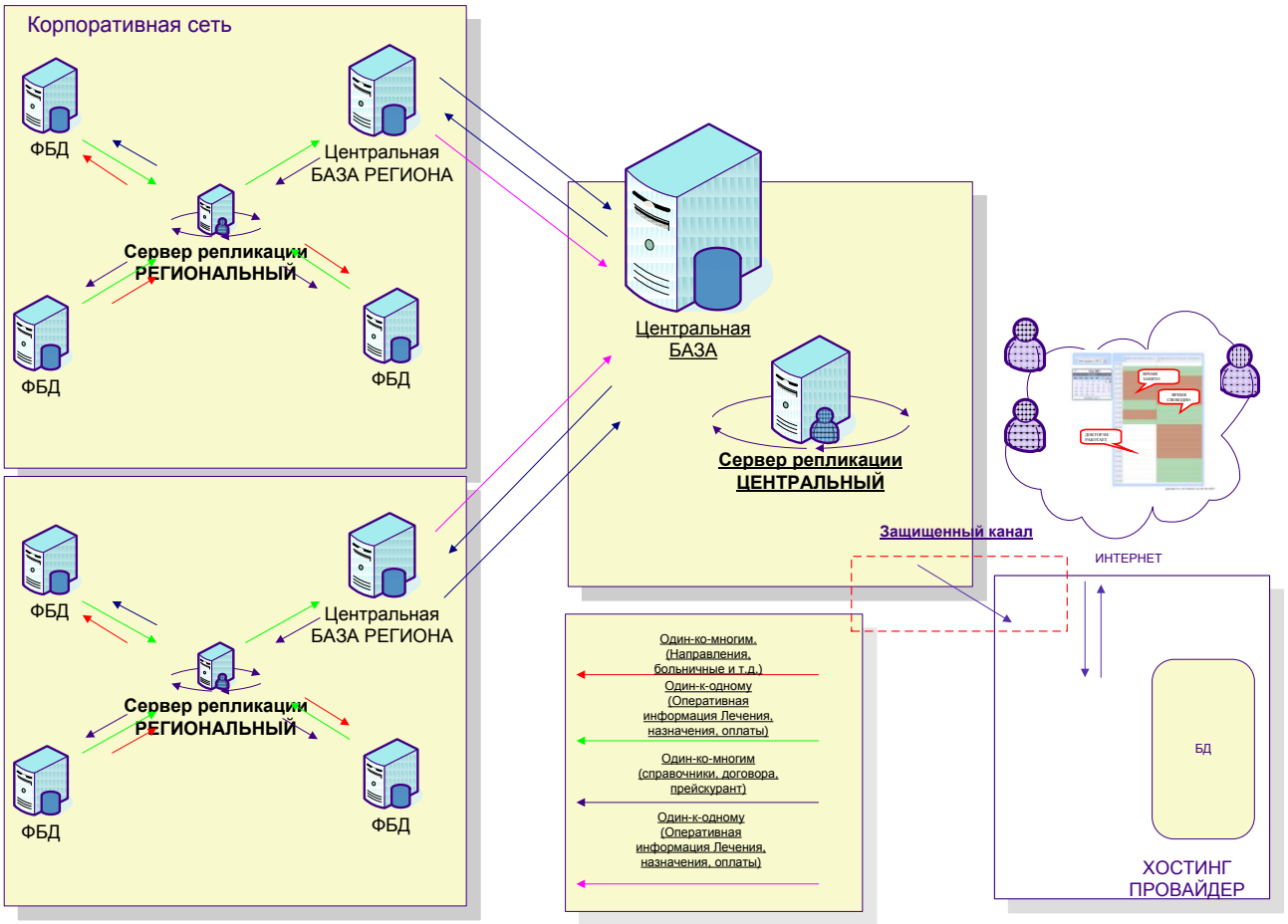
При необходимости данные могут переноситься в другие базы данных, например в случае, если учреждение хочет предоставлять возможности по доступу к информации в ЛПУ через интернет.

Например, с помощью сети Интернет, предоставление пациентам возможности:

- Получения данных о состоянии лицевого счета, расчетах с организацией;
- ON-LINE записи на прием;
- Доступа к электронной истории болезни (ЭМПЗ).

А так же другие возможности на усмотрение заказчика.

В общем случае схема обмена может быть представлена на рисунке ниже.



2.2. Функционал МИС

Функции МИС охватывают практически все сферы деятельности учреждения. Рассмотрим функции важные для нашего вопроса, к ним относятся:

- Ведение базы данных контингента ЛПУ (Ф.И.О. , телефон, данные прикрепления к страховой компании);

- Формирование, печать, хранение электронной персональной медицинской записи (ЭПМЗ) по пациенту в соответствии с требованиями ГОСТ Р 52636-2006;
- Ведение единой (центральной) БД всех пациентов, во избежание искажения общей статистики по компании и предоставления сводных данных;
- Доступ к ЭПМЗ из территориально-удаленных подразделений (при наличии прав доступа врач может получить ЭПМЗ по пациенту из любой филиальной базы данных);
- Управление доступом на основе ролей и идентификация пользователей с помощью биометрических данных;
- Учет фактического времени работы сотрудников (учет прихода и ухода с работы) с использованием биометрических данных;
- Ведение базы данных о сотрудниках ЛПУ для кадрового учета.

3. Классификация данных используемых в МИС и типа обработки

Для того, чтобы применить закон документы разработанные на основании закона, необходимо:

- правильно классифицировать данные используемы в МИС;
- определить их категорию;
- определить производится ли автоматизированная обработка этих данных.

3.1. Категория данных

Наша МИС эксплуатируется более чем в 800 различных ЛПУ. Некоторые компании эксплуатируют МИС уже около 10 лет. Одна из самых крупных баз данных насчитывает данные о более чем 200 000 пациентов. И по каждому из данных пациентов существуют данные об оказанных услугах, ЭМПЗ, контактная информация и другие.

Таким образом, в соответствии с п.1 ст.3 закона «О персональных данных» в нашей системе используются персональные данные.

3.2. Категория данных

В соответствии с классификацией (приказом N 55/86/20 от 13 февраля 2008 года ФСТЭК России, ФСБ России и Мининформсвязи России) их можно отнести к первой категории. Т.к. а нашей системе содержатся Ф.И.О., телефон, номер паспорта, год рождения и др., а так же сведения о состоянии здоровья по большому количеству пациентов. Крупные базы данных наших клиентов содержат до 250000 пациентов. И это количество со временем может только расти, т.к. удаление данных о пациенте нецелесообразно. Т.к. вместе в этим теряет актуальность финансовая, статистическая и медицинская информация.

Например.

Нальзя удалять пациента Петрова, т.к у него может быть как долг, так и аванс.

Нельзя удалять данные о пациенте, т.к. в системе может храниться значимая информация, которая может автоматически доводиться до медицинского персонала. Например, информации о наличии аллергии. Обезличивание данной информации не имеет смысла и более того опасно.

Очевидно, что практически любая информационная система с помощью которой осуществляется работа с клиентом подпадает под действие закона. И чем крупнее организация, тем серьезнее становится категория. Закон охватывает практически все информационные системы, начиная от системы в любом банке или платежном терминале при осуществлении оплаты за телефон, баз сотовых операторов, интернет-провайдеров и любой организации эксплуатирующей МИС с использованием данных позволяющих идентифицировать человека.

Очевидно, что практически любая система должна содержать эти данные, т.к. в противном случае невозможно установить человека по информации системы, а следовательно информация содержащаяся в системе не имеет никакого смысла.

Отнесение Фамилии, Имени, Отчества, телефона и даты рождения делает невозможной создание информационной системы не использующей персональные данные, а круг лиц имеющий к ним доступ не может быть

ограничен, т.к. любой пользователь ИС, который осуществляет операции в системе по добавлению или изменению данных должен получить доступ к ним. Возможно исключением могут стать лица, которые имеют доступ только к статистическим данным, общим отчетам. Но что делать если Вы просто решили детально проверить построенный отчет ? Таким образом практически любой разработчик ИС и любая организация применяющая информационные системы подпадают под действие закона и связаны с финансовыми тратами и проблемами, которые будут рассмотрены ниже.

3.3. Обработка персональных данных

Данный вопрос встает отдельно в связи с послаблениями, которые предоставляются Постановлением Правительства РФ от 15 Сентября 2008 г. N 687 "ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОСОБЕННОСТЯХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ".

Ниже приведено определение информационной системы персональных данных в соответствии с законом «О персональных данных» (ст.3 п. 9).

Информационная система персональных данных *- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.*

В соответствии с постановлением правительства:

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов

персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

В нашей информационной системе ввод данных осуществляется вручную, однако данный документ так же не дает возможности избежать формулировки «автоматизированная обработка данных». А следовательно в отношении нашей системы действует положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781.

4. Проблемы и опыт выполнения требований

Закон «О персональных данных» несет позитивные требования по обеспечению безопасности персональных данных граждан, и направлен на выполнение их конституционных прав, однако нормативные документы раскрывающие требования данного закона ведут серьезному увеличению затрат как со стороны разработчиков информационных систем, так и стороны потенциальных пользователей этих систем. А следовательно создают дополнительные препятствия при использовании информационных технологий и повышении эффективности труда с их применением.

К проблемам исполнения закона, а так же факторам, которые влияют на увеличение стоимости разработки можно отнести:

- ограничение доступа к нормативно-правовым документам;
- необоснованно жесткие требования к уровню защищенности информационных систем;
- длительность и высокая стоимость сертификации информационных систем;

- существенные затраты на аттестацию рабочих мест пользователей со стороны заказчика МИС.

4.1. Ограничение доступа к нормативно-правовым документам.

С началом работ по выполнению требований законодательства мы столкнулись с ограничением доступа к нормативно-правовым документам. Так часть документов регламентирующих работу с персональными данными имеют гриф «Для служебного пользования». А именно:

Так ознакомиться с данными документами можно лишь в специализированной организации. Очевидно, что для оценки необходимости и стоимости услуг подобной организации необходимо заранее ознакомиться с данными документами.

4.2. Необоснованно жесткие требования к разработчикам информационных систем

В настоящее время законодательство в области защиты систем персональных данных является очень жестким. Однако многие требования остаются необоснованными и ведут к серьезным финансовым затратам.

Вызывают вопрос многие подходы, которые были использованы при разработке требований к обеспечению сохранности персональных данных при обработке в информационных системах. Создается впечатление, что к требованиям по обеспечению сохранности персональных данных применяются точно такие же подходы как при обеспечении безопасности государственной тайны. Хотя очевидно, что они не могут применяться в связи с:

- Отсутствием системы защиты данных вне информационных систем;
- Широким кругом лиц и областью использования персональных данных, а следовательно более значительными общими экономическими затратами на их защиту;
- Иным объемом и характером ущерба, который может быть нанесен в связи с утечкой или разглашением персональных данных.

Многие требования носят формальный характер и не могут быть реализованы на практике.

Так положением «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных предусмотрено:

1. использование системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии;
2. использование программных средства удовлетворяющих устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации;
3. что средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия;
4. обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств;
5. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
6. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий

Так в соответствии с классификацией наша система должна соответствовать 1 классу защищенности от несанкционированного доступа.

Требования рассмотрены в Руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992.

За годы разработки, в соответствии с требованиями заказчиков в нашей МИС была реализована ролевая модель управления, которая позволяет проводить разграничение доступа пользователей, как к отдельным функциям системы, так и к отдельным объектам используемых системой.

Администраторы системы имеют возможность гибко изменять права пользователей на доступ к модулям системы, отдельным функциям системы, разграничивать права на просмотр, изменение, удаление определенных типов данных системы, а так же доступ к конкретным наборам данных.

Однако в случае применения нормативных документов этого недостаточно. Поскольку в России отсутствуют сертифицированные операционные системы, системы управления базами данных, необходимо применение дополнительных средств защиты.

Очевидно, что 1 компания не может одинаково успешно заниматься разработкой сертифицированных средств защиты и медицинских информационных , а следовательно:

- либо разработчик МИС должен продавать конечное решение совместно со сторонними средствами защиты увеличивая стоимость системы;
- либо заказчик должен отдельно приобретать дополнительные сертифицированные средства защиты от НСД, что так же в конечном итоге удорожает стоимость автоматизации ЛПУ.

Отдельно встает вопрос защиты информации от побочных электромагнитных излучений и физическая охрана помещений. Это так же дополнительные затраты.

Представьте электромагнитный томограф рядом с которым стоит генератор шума для подавления излучения монитора и специальный аппаратный комплекс технической разведки, который стоит за окном и пытается его перехватить.

Или пациента, которого нельзя оставить одного в палате, т.к. там установлен ПК, подключенный в информационной системе. Т.к. пациент потенциально может установить закладку в ПК.

Однако при этом, ни учет медицинских карт, их выдача и ознакомление, транспортировка по ЛПУ производится без охраны. Любой сотрудник регистратуры может свободно ознакомиться с содержанием медицинской карты больного. Тогда с какой целью тратятся дополнительные средства ?

В нашей системе используется 2 типа разграничения доступа к данным уровне:

- Самой МИС;
- СУБД.

Если первый механизм мы можем сертифицировать, т.к. разработчики мы его программного обеспечения, то Firebird мы не можем сертифицировать. А его разработчики не будут этого делать. Т.к. это открытый и бесплатный проект.

Применение подобного подхода делает невозможным использование бесплатного программного обеспечения в России, т.к. разработчики бесплатных и открытых систем не заинтересованы в трате ограниченных финансовых средств на проведение сертификации.

Следовательно, наша компания, возможно, перейдет на платный коммерческий аналог Firebird – СУБД Interbase компании Borland, в случае если он будет сертифицирован, т.к. это станет необходимым для продаж в России. В настоящее время лицензии на использование данной СУБД сопоставимы со стоимостью нашей информационной системы. А следовательно, стоимость нашей информационной системы для заказчика удваивается, т.к. параллельно необходимо приобретение лицензий компании Borland. В этом случае так же увеличивается стоимость владения, т.к. в случае Firebird обновление СУБД на следующие версии не требует финансовых затрат, использование же Interbase требует оплаты последующих версий СУБД.

4.3. Длительность и высокая стоимость сертификации информационных систем

В настоящее время все потенциальные заказчики нашей МИС уделяют повышенное внимание вопросам соответствия информационной системы требованиям законодательства «О персональных данных».

Основным критерием при выборе информационной системы становится наличие сертификатов на соответствие требованиям по уровню защищенности систем.

Таким образом, для прохождения процедуры сертификации наша компания обратилась в соответствующую организацию.

В ходе консультаций было установлено, что для осуществления сертификации необходимо:

- оборудование специального помещения для ведения разработки ПО, которое будет проходить сертификацию (установка железных дверей, защита от побочных электро-магнитных ислучений);
- создание аттестованных рабочих мест для программистов, осуществляющих разработку МИС исключающих вход в Интернет;
- подготовка необходимой для сертификации документации;
- предоставление исходного кода МИС для проведения проверки на недекларированные и программные закладки.

Данные требования вызывают целый ряд вопросов.

С какой целью создается охраняемое помещение с защитой от электромагнитных излучений, если обработка персональных данных на ПК программистов не проводится а исходный код приложения не является секретным? Он действительно представляет большую ценность для нашей компании, как разработчика, но не потенциального злоумышленника.

Для чего осуществляется аттестация персональных компьютеров программистов? Для проверки, что иностранные спецслужбы не заложили спец. закладки в ПК? В таком случае один из программистов может быть

агентом иностранных специальных служб и аттестация персональных компьютеров не обеспечит безопасности.

Предоставление исходного кода приложения понятно, т.к. действительно мы, как разработчик МИС можем оставить дыры в системе безопасности нашей МИС. Однако может ли данная организация проверить исходный код? И сколько это будет длиться?.

Так наша информационная система разрабатывалась достаточно длительное время. По примерным оценкам это около 15 человек\лет. Естественно исключая ошибочные решения, время потраченное на исправление ошибок, постановку задач и т.д. это будет меньше. Пусть мы даже сузим этот срок до 3 лет. Для проверки исходного кода программисты сертифицирующей организации должны иметь уровень знаний аналогичный разработчикам нашей компании. Способны ли они провести проверку исходного кода системы в адекватные сроки?

В настоящее время программирование в основном осуществляется с использованием языков высокого уровня. В частности наша МИС разрабатывается с использованием DELHI это объектно-ориентированный язык. Наши программисты используют многие компоненты других разработчиков. Проверка исходного кода на DELPHI не даст представления о наличии недекларированных возможностей, т.к. они могут быть встроены в сторонние используемые компоненты. А их исходные коды не предоставляются. Разработчики сторонних компонент в свою очередь используют другие языки программирования и компоненты. Неужели сотрудники данного учреждения будут проверять их все? Или они декомпилируют программу и будут ее анализировать?

Сколько будет стоить анализ исходного кода программы непосредственно на разработку которой было потрачено 3 года? Если средняя заработная плата программиста в г. Москве составляет 40 000 рублей ?

Каковы гарантии того, что исходный код приложения не будет передан третьим лицам?

Предположим, что проверка выполнима. И может быть выполнена в течении полугода. И стоимость ее невелика. Однако программное обеспечение не стоит на месте. Нашей компанией 1 раз в 2 месяца выпускаются версии системы с дополненным и расширенным функционалом, а так же исправлением допущенных ошибок, которые не были выявлены в ходе тестирования. Это могут быть как лишь незначительные изменения, а могут быть целые новые модули для автоматизации тех или иных потребностей ЛПУ. В результате каждый раз исходный код программы должен целиком проверяться на наличие недекларируемых возможностей. Таки образом любые изменения будут попадать к заказчику с опозданием. А следовательно реализации функционала будет существенно отставать от современных особенностей бизнес-процессов заказчика.

Выпуск исправлений для ошибок в версии в подобных условиях невозможен.

4.4. Существенные затраты на аттестацию рабочих мест пользователей со стороны заказчика МИС

В настоящее время стоимость 1 аттестованного для работы с персональными данными рабочего места составляет от 80 тысяч рублей. В ходе аттестации осуществляется установка дополнительных средств защиты в связи с отсутствием сертифицированных операционных систем и баз данных, а так же требованиям по защите от аппаратных закладок и побочных электро-магнитных излучений.

Для сравнения, стоимость простой версии нашей информационной системы для стоматологической клиники составляет 60000 рублей. Таким образом, в случае оборудования 1 рабочего места необходимо затратить больше средств, чем на приобретение программного обеспечения. На последующие рабочие места стоимость МИС составляет 6000 рублей, а затраты на защиту остаются на прежнем уровне в 80000 рублей.

В условиях свободного обращения информации содержащей персональные данные вне информационных систем, данные затраты не представляются обоснованными.

5. Пример простого расчета затрат в связи с новыми требованиями нормативных документов по защите персональных данных.

Затраты разработчика на примере нашей компании:

№ п.п.	Наименование	Цена, ед	Кол-во	Стоимость
1.	Оборудование специального помещения	150000	1	150000
2.	Аттестованное рабочее место программиста	120000	8	960000
3.	Обучение специалистов по обеспечению безопасности информации внутри компании	40 000	2	80000
4.	Сертификация новых версий ПО, 6 раз в год (ориентировочная стоимость)	1000000	6	6000000

Затраты заказчика МИС, использующего полный функционал МИС. Персональные данные 1 категории из расчета установки МИС на 100 ПК:

№ п.п.	Наименование	Цена, ед	Кол-во	Стоимость
1.	Дооборудование помещений в соответствии с требованиями нормативных документов	Нет данных		
2.	Установка сетевых средств защиты	Нет данных		
3.	Организация аттестованного рабочего места	120000	100	12000000
4.	Приобретение средств криптографической защиты	Нет данных		

6. Заключение

Принятие закона «О персональных данных» безусловно является положительным событием, т.к. обращает внимание руководителей всех уровней на необходимость обеспечения сохранности информации.

Что дает гражданам дополнительную уверенность в том, что их персональные данные будут использоваться по прямому назначению.

Однако нормативные документы регламентирующие порядок выполнения требований закона «О персональных данных» устанавливают необоснованно высокий уровень защиты данных.

В условиях отсутствия доступных сертифицированных операционных систем, систем управления базами данных, средств разработки, выполнение требований нормативных документов влечет значительные финансовые затраты как со стороны разработчиков ПО, так и со стороны заказчиков информационных систем, что создает препятствия для развития и внедрения программных комплексов. А существующие процедуры сертификации слишком продолжительны, дорогостоящи и не дают гарантий безопасности данных.