Актуальные проблемы информационной защиты персональных данных в сфере здравоохранения

Topical issues of information security of personal data in the health sector

Ключевые слова: медицина – medicine; здравоохранение – health care; информационная защита – information security; базы данных – databases.

Информатизация общественных структур, активные реформы здравоохранения, призванные улучшить качество обслуживания населения, открывают все новые проблемы в медицине, требующие глубокого анализа. В данной статье рассмотрены особенности обеспечения безопасности персональных данных пациентов в условиях российского законодательства.

Informatization of public structures, active health care reform designed to improve the quality of public services, creates new problems in medicine that requires deep analysis. This article describes the features of the security of personal data of patients in the conditions of Russian law.

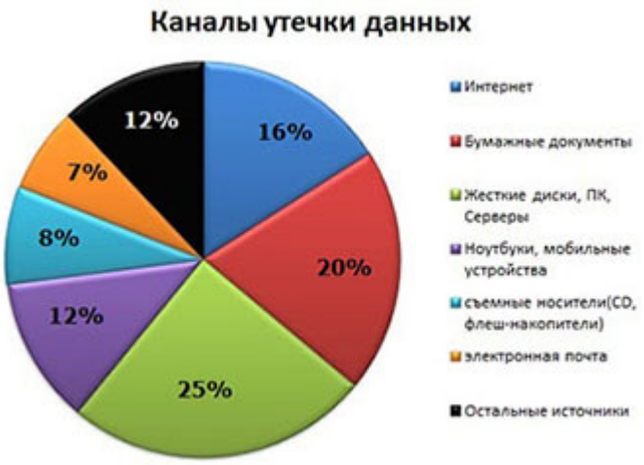
ТРИФОНОВ / TRIFONOV A.
Александр Александрович
(gilean@live.ru)
врач-интерн кафедры стоматологии детского возраста с курсом челюстно-лицевой хирургии СПбГМУ им. акад. И.П.Павлова,
магистрант кафедры геоинформационных систем НИУ ИТМО,
Санкт-Петербург

ИВАНОВА / IVANOVA E.
Евгения Анатольевна
(pipa0405@yandex.ru)
ассистент кафедры кафедры стоматологии детского возраста с курсом челюстно-лицевой хирургии СПбГМУ им. акад. И.П.Павлова,
магистрант кафедры геоинформационных систем НИУ ИТМО,
Санкт-Петербург

В наши дни во всем мире идет бурное развитие информационных технологий, что обуславливает эволюцию индустриального общества в новую формацию, получившую название «информационное общество». Здравоохранение, как важнейшая общественная структура, активно участвует в его становлении. Информатизация отрасли открывает широкие возможности для прямого и опосредованного повышения качества обслуживания пациентов. Этому способствует создание современных экспертных систем, мониторинга здоровья населения, а также систем делопроизводства, служащих для повышения эффективности использования ресурсов здравоохранения.

Более того, осуществление новых проектов, призванных произвести реформу государственных медицинских учреждений, невозможно без привлечения последних достижений в области информатики. В качестве примера можно привести постановление правительства Санкт-Петербурга от 25 октября 2011 г. №1472, в соответствии с которым был утвержден план мероприятий по профилактике основных стоматологических заболеваний и развитию детской стоматологической службы в Санкт-Петербурге на 2012-2014 годы. При всех достоинствах предложенных нововведений в области профилактики, критическим недостатком данного Плана является отсутствие какой-либо информационной поддержки, позволяющей в автоматизированном режиме проводить статистический анализ результатов, прогнозирование и планирование необходимых манипуляций. Большое количество государственных и частных стоматологических поликлиник, оказывающее помощь детскому населению Петербурга (по данным 2010г. более 650 тыс. чел.) обуславливает необходимость централизованного ведения статистики и хранения информации о пациентах. Исправить этот недостаток способна разработка специализированного программного комплекса, включающего в себя специализированную базу данных с удаленным доступом, а также системы статистической обработки и делопроизводства.

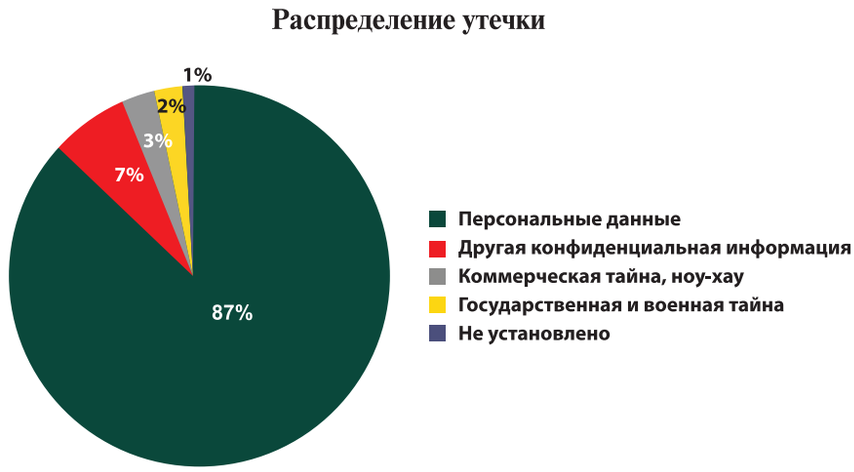
Но, к сожалению, помимо огромного количества преимуществ, которые дает внедрение информационных технологий в отрасль, открывается целый



спектр ранее не ведомых проблем. Централизованное хранение медицинских данных огромного количества пациентов делает их удобными для анализа, научных исследований, а также значительно снижает объем «бумажного» документооборота и нагрузку на административный сектор. Но это также делает подобные базы данных желанной и легкой целью для различного рода злоумышленников. В 2011 году удельный вес утечек медицинской информации, по данным аналитического центра компании Zecurion составил 19,1%, при этом цена одной такой записи на черном рынке в 50 раз превышает стоимость номера социального страхования. В США за последнее время произошло 364 случая похищения медицинской информации. Для России подобные случаи пока еще не были освещены в прессе, но это является лишь вопросом времени.

В подавляющем большинстве случаев подобные инциденты являлись результатом халатности медицинских сотрудников и их абсолютной непросвещенности в вопросах информационной безопасности. Оставленные на видном месте записки с паролями или портативные жесткие диски с базами данных являются обычным делом. Если подобные случаи происходят в США, то что говорить о России? Пожилые доктора, имеющие огромный опыт медицинской практики, не разбираются в компьютерных технологиях, а у молодых специалистов, достаточно подкованных в области информатики, недостает клинического опыта. С внедрением компьютерной техники в промышленность меняются производственная среда и рабочее место человека, аналогичные процессы происходят и в лечебных учреждениях. В связи с этим, а также с отсутствием соответствующих учебных направлений в медицинских университетах, наблюдается недостаток инженеров-программистов, знакомых с проблемами здравоохранения, а также клиницистов, знакомых с процессами разработки и эксплуатации информационных систем. Особенно этот недостаток стал ощущаться после принятия закона о «Персональных данных» (ФЗ-152). В соответствии с текстом этого закона, обработка данных о состоянии здоровья разрешена только с наличием письменного согласия пациента. В качестве исключения выступает случай, когда обработкой данных занимается лицо, непосредственно занимающееся медицинской практикой и обязанное сохранять врачебную тайну (т.е. сам врач). В результате крайне затрудняется создание централизованных баз данных с удаленным доступом на основе облачных технологий, т.к. в данном случае определить круг лиц, имеющих доступ к персональным данным практически невозможно. Более того, поскольку в письменном соглашении, которое подписывает пациент, необходимо указать все цели, для которых может использоваться информация об его здоровье, а также указаны все лица, которые могут получить доступ к его личной информации, объем бюрократических процедур и бумажной документации не снижается, как предполагалось, а в лучшем случае остается на прежнем уровне.

Кроме того, нельзя обойти вниманием вопросы лицензирования. Создание средств защиты конфиденциальной информации без соответствующего разрешения, даже для личных нужд, расценивается как нарушение закона. При этом сам процесс получения лицензии является абсолютно недоступным для медицинских учреждений с государственным финансированием. Они просто не обладают соответствующим кадровым составом, регламентированным в требованиях, а привлечение сторонних организаций, обладающими необходимыми лицензиями, невозможно по материальным соображениям.



В чем же суть защиты персональных данных? Как и для всех информационных систем, сущность обеспечения комплексной защиты медицинской информации основывается на выполнении трех важнейших свойств защищенной системы:

1) Конфиденциальность. Пользователи медицинской системы должны получать доступ только к тем данным, для которых они имеют явное разрешение на доступ. Комплекс мер обеспечения конфиденциальности включает разработку и описания политик доступа, разработку и реализацию мер по обеспечению разграничения доступ, по обеспечению идентификации пользователей, а также мер криптографической защиты.

2) Целостность. Обеспечение защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки.

3) Доступность. Обеспечение возможности доступа авторизованных в системе пользователей в соответствии с принятой политикой доступа.

В медицинских системах происходит несколько видов информационных процессов, каждый из которых подвержен различным типам угроз. В большинстве случаев человек посещает лечебное учреждение достаточно редко, и именно тогда происходит большая часть процессов информационного обмена. В остальных случаях информация о пациенте располагается в архиве. Соответственно, необходимо обеспечить мероприятия по обеспечению безопасности архивных данных.

При обращении пациента к врачу происходит коррекция архивных данных и передача информации на АРМ врача. Меры защиты на данном этапе должны приниматься как на уровне АРМ, так и на уровне локальных сетей.

Не стоит забывать о том, что для передачи данных может использоваться сеть Интернет, что также представляет собой определенный риск.

При защите персональных данных очень эффективна процедура обезличивания. В основной базе данных совсем не обязательно хранить паспортные данные пациентов – их вполне могут заменить номера полисов обязательного медицинского страхования, а диагнозы – идентификаторы МКБ-10. Таким образом, ценность такой информации для потенциального злоумышленника резко снижается, а для того чтобы врач мог воспользоваться ей, ему достаточно иметь вторую часть базы на локальной машине, защитить которую намного проще.

Таким образом, единственным возможным выходом из этого положения является перекладывание ответственности за разработку информационных систем в области здравоохранения и систем защиты для них на рабочие группы, существующие на базах крупных научно-исследовательских университетов, которые обладают необходимыми ресурсами и лицензиями для осуществления данных проектов.

Литература

1. Сабанов В.И., Голубев А.Н., Комина Е.Р. Информационные системы в здравоохранении.//М., 2007.
2. Кустов В.Н., Петров С.В. Теория и практика применения электронной подписи.//Информационные технологии, связь и защита информации МВД России, 2011.
3. Ромашов И.Н., Середа С.Н. Правовые основы медицинской информатики//М., 2004.
4. Бабенко Л.К., Басан А.С, Журкин И.Г. Макаревич О.Г. Защита данных геонформационных систем //М.2011.
5. ГОСТ Р 52636-2006 Электронные истории болезни.
6. Федотов Н., Шабанов И. Глобальное исследование утечек персональных данных.//Лаборатория Касперского, 2010