Захаров Александр Анатольевич,
доктор технических наук, профессор,
заведующий кафедрой информационной безопасности
Тюменского государственного университета
Россия, г. Тюмень
E-mail: azaharov@utmn.ru

Оленников Евгений Александрович,
кандидат технических наук,
доцент кафедры информационной безопасности
Тюменского государственного университета
Россия, г. Тюмень
E-mail: olennikov@utmn.ru

Паюсова Татьяна Игоревна,
старший преподаватель
кафедры информационной безопасности
Тюменского государственного университета
Россия, г. Тюмень
E-mail: t.i.payusova@utmn.ru

Зулькарнеев Искандер Рашитович,
старший преподаватель
кафедры информационной безопасности,
Тюменского государственного университета
Россия, г. Тюмень
E-mail: i.r.zulkarneev@utmn.ru

Овчаренко Денис Игоревич,
студент направления «Информационная безопасность»
Тюменского государственного университета
Россия, г. Тюмень
E-mail: ovcharenkodenisutmn@gmail.com

ОПТИМИЗАЦИЯ ЗАТРАТ НА ЗАЩИТУ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ МЕДИЦИНСКИХ СИСТЕМАХ

В статье демонстрируются технологии, позволяющие значительно снизить затраты учреждений здравоохранения на обеспечение безопасности персональных данных в распределенных медицинских информационных системах. Рассматривается задача снижения расходов на защиту удаленного рабочего места, которое используется для автоматизации обработки и передачи медицинских данных. Показано как можно защитить рабочее места специалиста, занимающегося сбором медико-биологических данных для научных исследований. Описываются технологии обезличивания информации с помощью метода введения идентификаторов и метода декомпозиции.

Ключевые слова: персональные данные, информационные системы персональных данных, медицинская информационная система, оптимизация затрат, обезличивание, незащищенный канал связи, "сырые" данные, кардиограмма, медико-биологические научные исследования.

Введение

Защита персональных данных (ПДн) была и остается одним из важнейших вопросов информационной безопасности [1], так как любые несанкционированные действия в отношении ПДн касаются живых людей, и последствия таких действий могут нанести ущерб в экономическом, социальном, политическом и личном планах. Любая медицинская информационная система (МИС) работает со специальной категорией ПДн, составляющих врачебную тайну. Врачебная тайна охраняется законом [2], таким образом, любая медицинская организация и медицинские сотрудники должны соблюдать нормативно-правовые предписания для защиты информации, составляющей врачебную тайну, что, однако, может привести к существенной дополнительной финансовой нагрузке на учреждение.

Мероприятие по защите персональных данных

Обеспечение защиты ПДн является дорогостоящим мероприятием как с финансовой точки зрения, так и с точки зрения привлечения дополнительных кадровых ресурсов. Наибольшие затраты связаны с:

- аудитом безопасности ПДн;
- разработкой технического проекта на защиту ПДн;
- закупкой и внедрением средств защиты информации;
- разработкой документации по защите ПДн;
- проведением аттестационных мероприятий;
- обучением собственных специалистов;
- обновлением парка технических средств;
- ежегодным техническим сопровождением;
- внесением изменений в существующее программное обеспечение или закупкой нового.

Роскомнадзор, ФСТЭК России и ФСБ России в рамках своей зоны ответственности проводят плановые и внеплановые проверки соблюдения требований защиты ПДн, которые могут привести к весомым штрафам, убыткам в результате приостановления деятельности МИС, а также репутационным рискам. В 2017 году в Кодексе об административных правонарушениях был увеличен размер штрафов за нарушение данных требований [3].

Уменьшение расходов на защиту ПДн в первую очередь можно осуществить с помощью:

1) формирования единого подхода к защите ПДн в рамках региона. Ч.2 ст.4 ФЗ-152 позволяет принимать государственным органам в пределах своих полномочий нормативные правовые акты по отдельным вопросам, касающимся обработки ПДн [1];
2) грамотного планирования мероприятий по защите ПДн;
3) централизации ресурсов;
4) использования компенсирующих мер, например, обезличивания;
5) оптимизации технологического оснащения.

Единый подход к защите ПДн в регионе может подразумевать:

1) разработку единой стратегии и концепции информационной безопасности, в том числе и для ПДн;
2) разработку единой типовой (или отраслевой) модели угроз безопасности ПДн с учетом специфики инфраструктуры региона и используемых технологий;
3) разработку пакета шаблонных документов по защите ПДн, в том числе по работе со средствами криптографической защиты информации;
4) организацию постоянной консультационной поддержки по вопросам защиты ПДн (методические материалы и рекомендации, запросы через сайт, call-центры, e-mail, взаимодействие со специалистами информационной безопасности напрямую);
5) организацию централизованного обучения и повышения квалификации ответственных сотрудников (организация тренингов и семинаров, касающихся защиты ПДн).

Данный подход поможет снизить затраты медицинских организаций на содержание штата специалистов в области защиты информации, сократить их количество за счет перераспределения задач на исполнительный орган государственной власти, а также их централизации.

Основные оптимизационные мероприятия по защите ПДн связаны с:

1) сегментированием информационных систем персональных данных, что позволяет разделить информационные системы для снижения уровня защищенности ПДн и соответственно снижению требований по их защите в соответствии с Постановлением 1119 [4];
2) выделением государственных информационных систем из всего множества информационных систем персональных данных, т.к. только государственные информационные системы требуют обязательной аттестации, а прочие информационные системы могут отчитаться перед Роскомнадзором с помощью декларации соответствия;
3) сокращением расходов на аудит (подготовкой и заполнением форм с информацией для оценки);

4) централизованным согласованием выбранных мер по защите ПДн, в частности, исключением навязывания ненужных мероприятий, а также предоставлением механизмов контроля и единого подхода к защите ПДн.

С применением подобных мероприятий (п.п. 2, 3, 4) возможно снижение затрат на услуги по защите информации (исключая внедрение средств защиты информации) до 30%. Стоимость внедрения средств защиты информации можно снизить до 15-20% (п.п. 1, 2, 4).

С технической точки зрения уменьшение расходов на защиту ПДн может быть связано с:

1) централизацией (размещение основных и общих информационных систем в ЦОДе, что дополнительно повышает отказоустойчивость МИС);
2) применением компенсирующих мер, в частности, обезличивания;
3) оптимизацией технического оснащения, например, за счет использования виртуализации.

Для распределенных МИС необходимо осуществить защиту как на стороне клиента, так и на стороне сервера, а также защитить каналы передачи ПДн.

На рисунке 1 представлена диаграмма, иллюстрирующая долю каждого типа средств защиты информации (СЗИ) от общей стоимости защиты одного клиента МИС (исходя из минимальной стоимости сертифицированных средств защиты информации, без защиты серверов и систем виртуализации).

Как видно из диаграммы, наиболее затратным является внедрение средств доверенной загрузки (46% стоимости), которые необходимы для обеспечения второго и выше уровня защищенности персональных данных [10]. В случае обеспечения безопасности удаленного рабочего места мы можем выделить его в отдельный сегмент защищаемой МИС. Количество записей о пациентах в данном сегменте, как правило, будет гораздо меньше 100 000. Если это не так, то следует исключить (если это возможно) те записи, которые не используются в повседневной работе (например, сохранить в отдельный архив на съемном носителе или передать на серверную часть МИС), чтобы количество записей о субъектах ПДн было меньше 100 000. Это позволит понизить требуемый уровень защищенности персональных данных в этом сегменте, что исключает необходимость внедрения средств доверенной загрузки.

Средства защиты от несанкционированного доступа необходимы, т.к. на автоматизированном рабочем месте МИС происходит обработка и хранение персональных данных, к которым может получить доступ злоумышленник. Однако, если перестроить процесс обработки таким образом, чтобы сделать невозможным хранение данных на жестком диске, то можно исключить данный тип СЗИ и снизить затраты на 18%. Для этого, например, можно использовать специально защищенное внешнее устройство (USB-токен), на котором будет храниться в зашифрованном виде вся обрабатываемая информация. Работа всего программного обеспечения, обрабатывающее специальные ПДн, должна быть настроена таким образом, чтобы обработка (в том числе и запуск специализированного программного обеспечения) без данного токена была бы невозможна. Защищаемые должны храниться только на этом внешнем носителе и никогда не храниться на других машинных носителях информации. Сам носитель требуется хранить в специальном защищенном хранилище, например, сейфе.

Дополнительно снизить затраты при защите ПДн можно за счет правильного подбора СЗИ. Ввиду быстрого развития технологий и высокой конкуренции создаются универсальные сертифицированные средства защиты информации формата endpointprotection, которые включают функционал различных типов СЗИ в одном. Использование подобных СЗИ позволит существенно снизить затраты на закупку и облегчить процесс их внедрения, использования и сопровождения. Так, например, СЗИ DallasLock или SecretNetStudio предлагают функционал средств защиты от НСД, антивирусов, межсетевых экранов и др. за стоимость эквивалентную стоимости стандартного средства защиты от НСД, т.е. снижение расходов минимум на 13%.

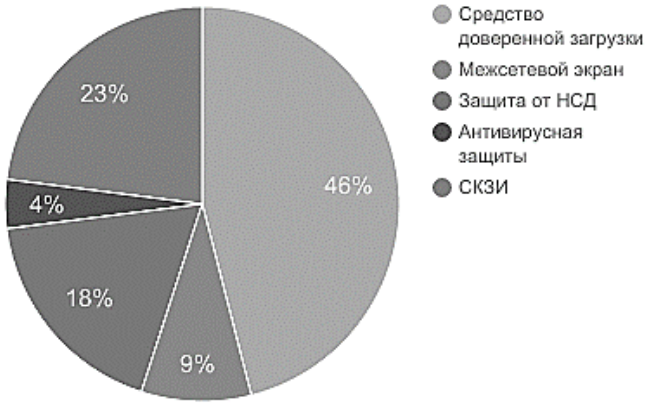

Рисунок 1. Распределение стоимости средств защиты информации при защите рабочего места

Применение компенсирующих мер, в частности, обезличивания, может являться альтернативой шифрованию - ГОСТ 28147-89 и ГОСТ Р 34.10-2012 [5, 6]. На текущий момент в расчете на одно рабочее место конечного пользователя распределенной МИС доля криптографических (шифровальных) средств защиты информации (СКЗИ) составляет порядка 23% от общей стоимости средств защиты информации. Применение обезличивания, если это позволяет сделать предметная область, сократит расходы за счет отсутствия необходимости в покупке, сопровождении и обслуживании сертифицированных программно-аппаратных криптосредств, таких как, VipNet Custom, КриптоПРО CSP, АПКШ «Континент», С-Терра и др.

Аспекты обезличивания регулируются Приказом Роскомнадзора №996 [7]. Согласно Приказу №996 можно применять обезличивание:

- методом введения идентификаторов;
- методом декомпозиции;
- методом изменения состава или семантики;
- метод перемешивания.

Метод введения идентификаторов предполагает замену значений атрибутов ПДн идентификаторами, декомпозиция разбивает исходную таблицу на подтаблицы таким образом, чтобы ни одна таблица по отдельности не смогла однозначно определить субъекта ПДн, изменение состава или семантики предполагает либо ликвидацию набора атрибутов, или изменение смысла значений атрибутов ПДн, например, с помощью обобщения. Перемешивание позволяет в соответствии с определенными перестановками переставлять значения в каждом атрибуте. Таким образом, все связи кортежа ПДн, теряются. Каждый из методов обладает своими достоинствами и недостатками, и каждый метод необходимо применять в зависимости от конкретных условий и требований.

Пример реализации

При проведении совместных медико-биологических научных исследований требуется обеспечить безопасность передаваемых данных, в частности: истории болезней, результаты анализов, анамнезы, диагнозы, назначенные лечения, данные фармакологических исследований, инновационные формулы и методики и т.д. В качестве компенсирующей меры в данном случае можно использовать обезличивание персональных данных (ПДн) пациентов.

Но обезличивание ПДн не является универсальным решением по защите медицинских данных. Например, важную информацию как с точки зрения ПДн, так и с точки зрения защиты данных медико-биологических научных исследований, могут содержать графические материалы: рентгеновские снимки, томограммы, электрокардиограммы и пр. В связи с этим также необходимо автоматизировать “зачистку” разнородных медицинских данных от потенциально критичной информации.

Одним из примеров задач, требующих организации централизованного защищенного сбора информации и автоматизированной “зачистки” графических материалов, является задача информационной поддержки скринингового исследования распространенности сердечно-сосудистых заболеваний (ССЗ) в Тюменской области. В контексте поставленной задачи метод декомпозиции является наиболее подходящим решением, поскольку позволяет свободно передавать по незащищенным каналам обезличенные данные, а процесс деобезличивания осуществлять на стороне клиента с помощью заранее сгенерированных идентификаторов.

Архитектура системы представлена на рисунке 2.

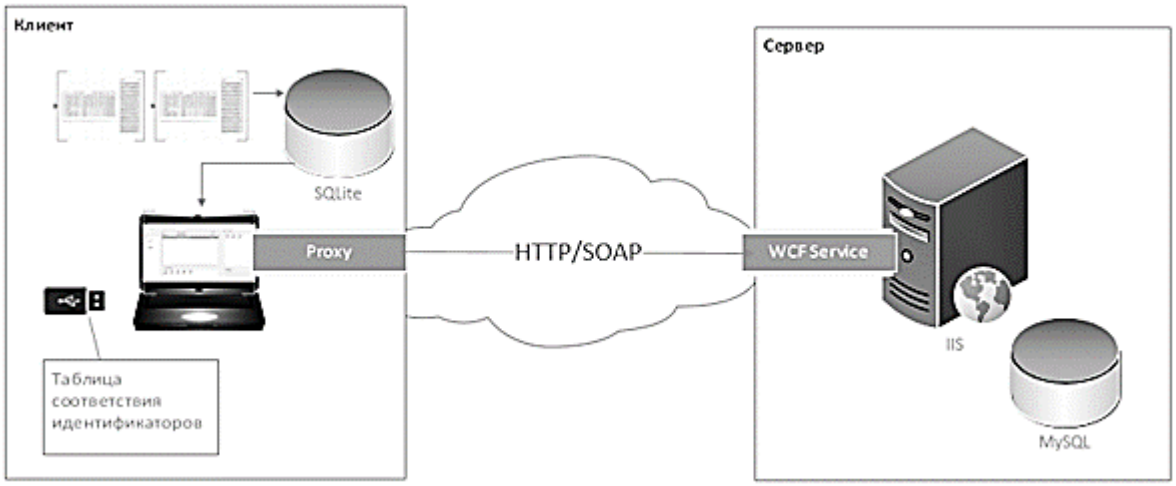

Рисунок 2. Архитектура клиент-серверного приложения

Первоначальная кардиограмма содержит ПДн пациента: ФИО пациента и дату рождения пациента (рисунок 3). На рисунке 3 приведен пример кардиограммы, в связи с этим данные реального пациента отсутствуют. Т.к. графические материалы скрининга содержат ПДн пациента, необходимо автоматизировать «зачистку» кардиограммы от нижнего блока данных (рисунок 3 - нижний блок). Преобразованная кардиограмма будет содержать только данные, полученные с кардиографа, и не будет однозначно указывать на конкретного пациента исследования (рисунок 4). Автоматизированная обработка кардиограмм осуществляется с помощью специальной библиотеки.

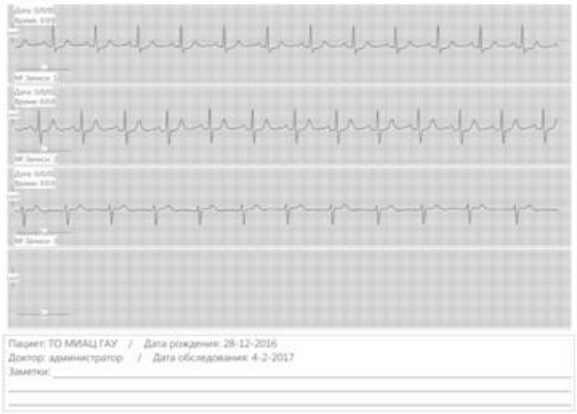

Рисунок 3. Пример кардиограммы, полученной с кардиографа CaRe

Рисунок 4. Пример преобразованной кардиограммы, не содержащей ПДн пациента

Каждому блоку данных, полученных с различных устройств, будет присвоен уникальный идентификатор после зачистки. На серверной части заранее генерируются пул уникальных идентификаторов пациентов для каждой клиентской системы, обеспечивая их уникальность в пределах всей распределенной системы. Эти данные передаются клиенту системы. Идентификатор пациента присваивается каждому пациенту (по его ФИО), обезличивая его персональные данные методом введения идентификаторов. Далее происходит соотнесение идентификатора пациента и идентификаторов блоков данных с устройств по принципу один ко многим в специальной таблице. В итоге, по незащищенному каналу будет передаваться блок данных с уникальными идентификатором, кардиограмма, а также результаты анализов. Обезличивание и деобезличивание по таблице соотнесения идентификаторов происходит в специальной программе клиента системы. Отметим, что такой метод применим для любых данных, полученных с диагностических медицинских устройств.

Заключение

Снизить стоимость затрат на защиту персональной информации в распределенной МИС более чем на 80% можно за счет применения описанных технологий, которые позволят исключить закупки и обновления, сертифицированных СЗИ для клиентской и серверной частей, а также использования дешевых незащищенных каналов передачи данных.

Отметим, что при этом отпадает необходимость разработки пакета документации в соответствии с требованиями законодательства по защите информации и не требуется специальное обучение персонала для работы со средствами защиты информации.

Список литературы

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) [Электронный ресурс] / Официальный сайт компании “КонсультантПлюс”. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 16.04.2017);
2. Федеральный закон "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 N 323-ФЗ (последняя редакция) [Электронный ресурс] / Официальный сайт компании “КонсультантПлюс”. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения 16.04.2017);
3. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 03.04.2017) [Электронный ресурс] / Официальный сайт компании “КонсультантПлюс”. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения 16.04.2017);
4. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс] / Официальный сайт компании “КонсультантПлюс”. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 16.04.2017);
5. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. [Электронный ресурс] / Федеральное агентство по техническому регулированию и метрологии. Режим доступа: http://protect.gost.ru/v.aspx?control=7&id=139177 (дата обращения 16.04.2017);
6. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. [Электронный ресурс] / Федеральное агентство по техническому регулированию и метрологии. Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения 16.04.2017);
7. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных" [Электронный ресурс] / Официальный сайт компании “КонсультантПлюс”. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_151882/ (дата обращения 16.04.2017);
8. Дистанционная передача ЭКГ. Индивидуальный электрокардиограф CaRe 1.0 [Электронный ресурс] / Медицинский информационно-аналитический центр. Режим доступа: http://miac-tmn.ru/wp-content/uploads/2016/08/CaRe-1.0-Distantsionnaya-peredacha-EKG-19.08.2016.pdf (дата обращения 16.04.2017);
9. ЭКГ по Небу [Электронный ресурс] / «МедОблако». Клиники, анализы, врачи, сравнение цен и запись. Режим доступа: https://medoblako.ru/uslugi/ekg-po-nebu/ (дата обращения 16.04.2017);
10. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». [Электронный ресурс] / ФСТЭК России. Режим доступа:http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 01.04.2017)
11. Интеллектуальный модуль анализа данных в информационных системах с помощью искусственных нейронных сетей. Захаров А.А., Оленников

Е.А., Паюсова Т.И. Вестник Тюменского государственного университета. Физико-математическое моделирование. Нефть, газ, энергетика. 2015. Т.1. № 4 (4). С. 102-111.
12. Интернет-сервис для доказательной медицины Захаров А.А., Захарова И.Г., Оленников Е.А., Паюсова Т.И., Бойко А.В. В сборнике: Научный сервис в сети Интернет труды XVIII Всероссийской научной конференции. ИПМ им. М.В. Келдыша РАН. 2016. С. 128-134.
13. Захаров А.А., Оленников Е.А., Петухов А.С. Информационная модель электронной истории болезни пациента // Вестник ТюмГУ. 2007, №5. С. 97-101.
14. Захаров А.А., Оленников Е.А., Петухов А.С. Математические методы оценки результатов исследований в диагностической подсистеме в составе электронной истории болезни пациента // Вестник ТюмГУ. 2008, №6. С. 145-152.
15. Захаров А.А., Нестерова О.А., Оленников Е.А. Проблемы информационного поиска для научных исследований в медицинских информационных системах // Вестник Тюменского государственного университета – Тюмень, 2009 - №6. С. 215-219.
16. Захаров А.А., Нестерова О.А., Оленников Е.А. Алгоритм информационного поиска в медицинских архивах на основе контекстно-временной онтологии // Вестник ТюмГУ. 2010, №6. С. 177-182.
17. Научный анализ данных в медицинской информационной системе (на примере определения факторов, влияющих на уровень с-реактивного белка, с помощью нейронных сетей) Захаров А.А., Оленников Е.А., Паюсова Т.И., Петелина Т.И., Мусихина Н.А., Гапон Л.И., Осипова И.В., Такканд А.Г., Белослудцева О.Е. Вестник Тюменского государственного университета. Физико-математическое моделирование. Нефть, газ, энергетика. 2014. № 7. С. 251-257.
18. Николаева А.А. Единый подход к системе медицинского образования в странах азиатско-тихоокеанского региона посредством процессно-ориентированного управления// Инновационное развитие экономики. Научно-практический и теоретический журнал№2 (32) 2016 март-апрель. С. 279-284.
19. Парфенова Е.Н., Симоненко Н.В. Проблемы развития инновационной инфраструктуры в российских регионах// Инновационноеразвитие экономики. Научно-практический и теоретический журнал№ 1 (37) – 2017, январь-февраль. С. 38-44.
20. Петухов А.С., Оленников Е.А., Захаров А.А. Модели и методы вывода в многоуровневой компонентной советующей подсистеме в составе электронной истории болезни. // «Известия ОрелГТУ» - Орел, 2008. С. 153-158.
21. Cloud service for data analysis in medical information systems using artificial neural networks Zakharov A.A., Olennikov E.A., Payusova T.I., Silnov D.S. International Journal of Applied Engineering Research. 2016. Т. 11. № 4. С. 2917-2920.
22. Scientific data analysis using neural networks as exemplified in defining the factors impacting the c-reactive protein level Zakharov A.A., Olennikov E.A., Payusova T.I., Petelina T.I., Musikhina N.A., Gapon L.I. Biology and Medicine. 2016. Т. 8. № 6. С. 329.