В.Л. Николаенко, А.А. Охрименко, В.И. Пачинин,
Г.В. Сечко, Т.Г. Таболич, И.И. Шпак

ЗАЩИТА ПЕРСОНИФИЦИРОВАННЫХ МЕДИЦИНСКИХ ДАННЫХ В БЕЛАРУСИ

Белорусский государственный университет информатики и радиоэлектроники

Анализируется терминология в области персональных данных пациента и предлагается именовать их персонифицированными медицинскими данными. Рассматриваются традиционные способы защиты персонифицированных медицинских данных и уровень защиты этими способами. Для повышения уровня защиты персонифицированных медицинских данных состоятельных пациентов предлагается использовать белорусские биометрические средств контроля доступа к рассматриваемым данным.

Ключевые слова: медицина, защита персональных данных пациентов, традиционные способы защиты персонифицированных медицинских данных, биометрические средств контроля доступа к данным.

Терминология: медицинские данные, персональные данные, персональные данные пациента, персонифицированные медицинские данные

Характер медицинской деятельности связан с использованием большого количества данных о здоровье пациента, истории его болезней, истории обращения к врачу и других данных. Перечисленные данные содержатся в медицинских документах, которые оформляются сотрудниками медицинских учреждений на каждого пациента. Медицинская документация - это документы установленной формы, предназначенные для регистрации результатов лечебных, диагностических, профилактических, реабилитационных, санитарно- гигиенических и других мероприятий. Примером медицинского документа является медицинская карта [1], которая позволяет обобщать и анализировать данную информацию. Медицинская документация является учетной и отчетной, её держателем выступают медицинские учреждения, следовательно, врачи медицинских учреждений несут ответственность за неправильное оформление соответствующих документов. Назовём все сведения о здоровье пациента, методах его лечения, медицинских назначениях и тому подобные данные *медицинскими данными.*

Однако, как следует из паспортной части, например, «Медицинской карты амбулаторного больного», в медицинских документах содержатся не только медицинские, но и персональные данные пациента. Согласно Федеральному закону Российской Федерации «О персональных данных» от 27.07.2006 N 152-ФЗ (статья 3, пункт 1) *персональные данные* - любая информация, относящаяся к прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных). Применительно к медицинским данным субъектом персональных данных является пациент, поэтому далее при упоминании о персональных данных речь будет идти только о *персональных данных пациента.* Следует отметить, что белорусский аналог российского закона N 152-ФЗ Национальное Собрание Республики Беларусь планирует рассматривать только в 2019 году.

Медицинская документация может содержать сведения о персональных данных пациента (например, рецепт [2], который содержит фамилию, имя и отчество больного, его возраст, адрес, номер его «Медицинской карты амбулаторного больного», назначения врача), но может и не содержать (например, отчетная медицинская документация, представляющая собой сводные статистические документы, содержащие сведения о состоянии и деятельности медицинских учреждений за определенный отрезок времени и т. д. [3]).

Каждый пациент, который попадает на приём в частную клинику, подписывает не только договор об оказании услуг, согласие на медицинское вмешательство, но и согласие на обработку своих персональных данных *совместно со своими медицинскими данными в* этом медицинском учреждении. Предыдущая фраза заимствована из ресурса [4], но в ней добавлен фрагмент, выделенный курсивом. Суть добавленного фрагмента состоит в том, что для похитителя персональных данных пациента важнее комплект этих данных вместе с медицинскими данными - без них сами по себе персональные данные похитителя мало интересуют в силу малой их привлекательности в части финансовых результатов хищения. Другое дело - описанная в ресурсе [5] утечка в Беларуси медицинских данных умерших пациентов. Их после вызова скорой помощи отвозят в морг специальные машины скорой помощи, именуемые в народе «труповозками». Рост конкуренции между похоронными бюро возрастает с каждым годом. Существует 3 категории людей, обладающих информацией об умерших: врачи скорой помощи, милиционеры и санитары, которые осуществляют перевозку умерших в морг [5]. Утечка информации также возможна на уровне диспетчеров скорой помощи. Медики или сотрудники правоохранительных органов либо сообщают агентам адрес квартиры покойного, после чего те связываются с родственниками умершего, либо прямо рекомендуют определенную похоронную организацию. Обычно сообщение срабатывает - родственникам покойного в состоянии сильнейшего стресса не хочется куда- то идти и разбираться.

Комплект персональных данных пациента вместе с его медицинскими данными будем именовать *персонифицированными медицинскими данными* (название «персональные данные пациента» - синоним»). Именно эти данные - клад для мошенников [4]. Как утверждают независимые эксперты, на чёрном рынке ценность медицинской информации в 10 раз выше финансовой. Полученные незаконным методом сведения о здоровье могут использоваться в ущерб пациентов. Это и обман пенсионеров, когда им пытаются продать препараты - пустышки за баснословные суммы, и желание выручить деньги с угрозами обнародования диагнозов у известных личностей, и другие случаи [4].

Традиционные способы защиты персонифицированных медицинских данных (ПМД) и уровень защиты информации этими способами

Общеизвестно, что самым простым способом защиты является полный переход от бумажного документооборота к безбумажному [6].

По состоянию на сегодня в Минске ПМД хранятся не только в элек-

тронном виде (файлы, папки и архивы в компьютерах сотрудников и на сервере лечебного учреждения), но и в бумажном виде - в регистратуре поликлиники («Медицинская карта амбулаторного больного»), в архиве больницы (истории болезни пациентов, переименованные недавно в «Медицинские карты стационарного больного»). В кожвендиспансерах аналогом карт амбулаторного или стационарного больного является форма № 065/у-07 «Медицинская карта амбулаторного больного инфекциями, передаваемыми половым путем» и похожие формы для других заболеваний № 065-1/у-07 и № 065-2/у-07. Эти формы также хранятся в регистратуре кожвендиспансера.

В начале февраля 2014 года появилась информация [7], что в Минске на базе 29-й поликлиники начали тестировать работу электронной медицинской карты (ЭМК), что давно сделано во многих регионах России [8-11]. По заверению главврача, оцифрованы были медицинские карты всех 39 тысяч пациентов 29-й поликлиники. Но регистратура с бумажными медицинскими картами существует до сих пор.

Если зафиксировать факт несанкционированного доступа к данным или попытки такого доступа в компьютере сотрудника медицинского учреждения технически несложно, то зафиксировать аналогичный факт в регистратуре этого учреждения или в его архиве практически невозможно. Более того, учитывая факт низкой зарплаты медрегистраторов в Беларуси (чуть больше 100 долларов), вероятность утечки ПМД из регистратуры медицинского учреждения или архива больницы очень велика. В настоящее время в белорусских медицинских учреждениях предусмотрены только меры административной ответственности виновных в утечке (если виновные будут найдены). На наш взгляд, этого недостаточно. Уровень защиты НМД при наличии бумажного документооборота нулевой.

При наличии в медицинском учреждении только безбумажного документооборота все ПМД учреждения циркулируют в локальной вычислительной сети (ЛВС) его и частично в Интернете (при обмене информацией из ЛВС данного учреждения с ЛВС других учреждений, в том числе вышестоящих). Способы защиты информации в Интернете общеизвестны, их рассматривать не будем.

Защиту информации в ЛВС медицинского учреждения общепринято осуществлять в программными, организационными и вспомогательными методами. К программным методам защиты относится в основном контроль и разграничение доступа к ПМД в ЛВС [6, 12], а также обеспечение безопасности ПМД с помощью криптосредств [13]. К организационным способам можно отнести издание и контроль за исполнением внутренних распорядительных документов и положений, а также политик в отношении обработки ПМД медицинского учреждения, образцы которых содержатся в [14], а полный перечень - в «Методических рекомендациях для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости [13]. Вспомогательными способами защиты ПМД могут быть обезличивание, абстрагирование и некоторые другие [13]. При этом под обезличиванием понимаются действия, в ре-

зультате которых невозможно определить принадлежность ПМД конкретному субъекту персональных данных [13].

Перечисленные традиционные способы защиты ПМД (программные, организационные и вспомогательные методы защиты информации в ЛВС) медицинского учреждения позволяют обеспечить некоторый уровень защиты ПМД, но достичь стопроцентной защиты с их помощью невозможно. Действительно, при назначении администратором сети медучреждения прав доступа к ПМД главврач медучреждения и его заместители, лечащие врачи, сам администратор и сотрудники, обрабатывающие ПМД, обязательно получат такие права. Естественно, что в этом случае стопроцентной гарантии исключения утечки данных для пациента через работников медучреждения нет.

Биометрические способы защиты ПМД

В соответствии с российским законодательством биометрические ПМД обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Существует также Постановление Правительства Российской Федерации от 06.07.2008 N 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Похожих правовых актов в Республике Беларусь нет, но предварительные научные исследования проводятся. Так, например, 8-9 декабря 2016 года Министерство здравоохранения Республики вместе с другими организациями провели в Минске международную научно-техническую конференцию «Медэлектроника-2016. Средства медицинской электроники и новые медицинские технологии». Большой интерес на конференции вызвал доклад доктора медицинских наук, профессора В. Н. Ростовцева и аспиранта А. А. Гивойно, опубликованный в [15]. В докладе для защиты ПМД была предложен архиватор, представляющий собой по российской классификации информационную систему класса 1 (К1) (информационные системы, для которых нарушение заданной характеристики безопасности ПМД, обрабатываемых в них, может привести к значительным негативным последствиям для пациентов). С помощью архиватора ПМД пациента упаковываются в архив, доступ к которому будет иметь только пациент. Архиватор состоит из аппаратной части (системы контроля доступа путем идентификации личности пациента по рисунку радужной оболочки глаза(радужки) Panasonic BM-ET500) и программного обеспечения NPack. Архиватор хорошо известен в Беларуси с 2013 года (дата первой публикации [16] в журнале о нём), опробован на ряде белорусских предприятий энергетической отрасли для передачи технико-экономических показателей теплоэлектроцентралей. Работы по модернизации архиватора продолжаются в части замены системы Panasonic BM-ET500 на более современную и дешёвую и активно публикуются [15-18],

Заложенная в архиваторе технология аутентификации личности пациента проста: полученное изображение радужки сравнивается с хранящимся в базе архиватора изображением. Уровень традиционные способы защиты

НМД пациента во много раз выше, чем у защиты традиционными способами (см. п. 2 выше), поскольку в этом случае полностью исключается утечка данных для пациента через работников медучреждения. Однако возникает вопрос: не слишком ли дорого стоит для пациента аутентификации его личности по радужке? Предварительные расчёты показывают, что при хранении в базе архиватора в течение трёх лет примерно 2000 изображений радужки стоимость аутентификации, включающая затраты на покупку и эксплуатацию архиватора, для одного пациента составит примерно 50 $.

Вывод

Чтобы минимально защитить конфиденциальные ПМД, нужно отказаться от всевозможных бумажных носителей медицинских данных и перейти на электронные. К сожалению, в части внедрения электронных медицинских карт Беларусь намного отстаёт от России. Отставание имеется и в части законодательства.

При исключении бумажной документации в медучреждении защиту ПМД в ЛВС медицинского учреждения традиционными методами (см. п. 2 выше) можно считать достаточной, а, главное, дешёвой. Естественно, однако, что в этом случае стопроцентной гарантии исключения утечки данных для пациента через работников медучреждения нет.

Наиболее материально обеспеченные пациенты могут достичь более высокого уровня защиты своих ПМД аутентификацией за умеренную плату своей личности по радужке с помощью описанного в [15] архиватора. Воспользоваться аутентификацией по радужке могут и менее обеспеченные пациенты, если нарушение заданной характеристики безопасности ПМД, обрабатываемых традиционными методами, может привести к значительным негативным последствиям для таких пациентов.

Библиографический список

1. Электронная медицинская карта (ЭМК) [Электронный ресурс]. - Режим доступа: swan-it.ru/elektronnoe_zdravoohranenie/elektronnaya_meditsinskaya_karta.- Дата доступа 25.12.2017.

2. Рецепт — Википедия [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/PeuenT. - Дата доступа 25.12.2017.

3. Медицинская документация отчетная - это... Что такое ... [Электронный ресурс]. — Режим доступа: https://dic.academic.ru/dic.nsf/medic2/26580. - Дата доступа 25.12.2017.

4. Защита персональных данных в медицинских учреждениях [Электронный ресурс]. - Режим доступа: www.bit-medic.ru/articles/zashita-personalnyh-dannyh/. - Дата доступа 25.12.2017.

5. О чём молчат сотрудники похоронных бюро? Беларусюянавшы - [Электронный ресурс]. - Режим доступа: www.newsby.org/by/2011/08/1 l/text20890.htm. - Дата доступа: 25.12.2017.

6. Защита персональных медицинских данных в автоматизированных

медицинских системах лечебно-профилактических учреждений / В. Д. Зыков, Р. В. Мещеряков, К. О. Беляков // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2009. - № 1 (19). - Часть 2 (июнь). -С. 67-70.

7. Электронная медицинская карта. Введение в картотеку « e-Gov.by ... [Электронный ресурс]. - Режим доступа: e-gov.by/stroitelstvo-e-gov/elektronnaya-medicinskaya-karta-wedenie- v-kartoteku. - Дата доступа 25.12.2017.

8. Электронная медицинская карта (ЭМК) [Электронный ресурс]. - Режим доступа: swan-it.ru/eektronnoe_zdravoohranenie/elektronnaya_medtsinskaya _karta. - Дата доступа 25.12.2017.

9. РИАМС «ПроМед [Электронный ресурс]. - Режим доступа: swan-it.ru/elektronnoe_zdravoohranenie/riams_promed. - Дата доступа 25.12.2017.

10.Что представляет собой RobomedNetwork? [Электронный ресурс]. Режим доступа: https://robomed.io/ru/. - Дата доступа 25.12.2017.

11. Электронная медицинская карта пациента, амбулаторного ... [Электронный ресурс]. - Режим доступа: https://robomed.com/articles/elektronnaya-meditsinskaya-karta/. - Дата доступа 25.12.2017.

12. Введение - StudFiles.net [Электронныйресурс]. - Режим доступа: https://studfiles.net/preview/6006132/.-Дата доступа 25.12.2017.

13. Методические рекомендации [Электронный ресурс]. - Режимдоступа: www.mz26.ru/netcat_files/ 140/195/h 3ff46872330d31a54a05al 1434a0f613. - Дата доступа 25.12.2017.

14. Образцы организационно-распорядительных документов ... [Электронный ресурс]. -Режим доступа: https://miacso.ru/Documents/images/Site/ObrazidokpoORD3.doc- Дата доступа 25.12.2017.

15. Гивойно, А.А. Защита медицинских данных пациентов / А. А. Гивойно, В. Н. Ростовцев // Доклады БГУИР. - 2016. - № 7 (101). - С. 79-83.

16. Безопасное архивирование данных с помощью биометрических технологий / А. А. Гивойно, С. В. Нестерович, Г. В. Сечко, Т. Г. // Весшксувязь - 2013. - № 6 (122). - С. 25-28.

17. Повышение информационной безопасности заархивированной информации / А. А. Гивойно, Г. В. Сечко, Т. Г. // Актуальные вопросы образования и науки: научный журнал. - М,- Архангельск: Архангельский институт управления, 2013. - № 3-4 (37-38). - С. 80-83.

18. Сравнение алгоритмов работы архиватора, использующего различные способы идентификации личности по радужке / А. А. Гивойно, Г. В. Сечко, Т. Г.// Материалы XXI МНТК «Информационные системы и технологии» (ИСТ-2015), Нижний Новгород (17 апреля 2015 г.). - Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2015. - С. 308.