УДК 004.9

ИТ-БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНЕ

Горбунова Т.В.,
научный руководитель канд. техн. наук Колокольникова А. И.
Кузбасский государственный технический университет им. Т. Ф. Горбачева

Медицина активно работает с наиболее важными персональными демографическими, медицинскими и финансовыми данными, которые требуют защиты. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное положение, образование, профессия, доходы и т. д., являются персональными данными. Такие сведения в лечебно-профилактических учреждениях (ЛПУ) сосредоточены в электронных картах и системах, обеспечивающих решение задач обязательного и добровольного медицинского страхования.

Согласно отчетам компании Gartner, именно ИТ- безопасность возглавляет список технологических приоритетов организаций, а затраты на финансирование проектов ИТ- безопасности ежегодно возрастают по всему миру. Аналитики Gartner прогнозируют рост потребности в компьютеризированных системах медицинских записей (computer-based patient records systems).

Опыт коммерческих и ведомственных клиник, государственные программы по информатизации системы здравоохранения влияют на появление медицинских информационных систем, в том числе и тех, которые требуют защиты персональных данных. Защите подлежит любая зафиксированная информация, неправомерное обращение с которой может нанести ущерб ее владельцу - физическому лицу.

Организации системы здравоохранения являются операторами персональных данных и адаптируют свои информационные системы персональных данных (ИСПДн) к требованиям госрегуляторов, Министерство здравоохранения и социального развития инициировало процесс согласования требований Федерального закона «О персональных данных» № 152-ФЗ с одним из регуляторов - ФСТЭК, чтобы выполнить требования закона, но не израсходовать слишком много бюджетных денег. Сертификацией в ФСТЭК подтверждается соответствие мер по защите персональных данных тем мерам, которые определены законодательством. При исполнении требований законодательства разрабатывается комплекс документов, которые регламентируют защиту данных, на основе комплексного аудита информационных систем внедряются средства защиты, которые и предотвращают утечку важных персональных сведений. В отраслевых рекомендациях Минздравсоцразвития для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости определены основные обязанности учреждений здравоохранения, работающих с ИСПДн.

Подходы к построению системы защиты персональных данных везде стандартны и практически всегда включает стадии обследования, классификации ИСПДн, формирования требований к системе защиты ИСПДн, проектирования, ввода в действие (внедрения) средств защиты, аттестации (на данный момент добровольной). Отраслевые особенности влияют на характер проектов и на конфигурацию системы защиты персональных данных, которая получается в итоге. Недостаточный уровень автоматизации медицинских учреждений отражается на характере проектов по защите персональных данных. Особенности информационных систем персональных данных лечеб-

ных учреждений - обработка сведений о состоянии здоровья большого числа субъектов, территориальная распределенность ЛПУ.

Защита персональных данных в медицинских учреждениях имеет несколько особенностей. Во-первых, необходим более детальный анализ бизнес-процессов учреждения на предмет выявления наличия или отсутствия признаков обработки персональных данных. Более половины форм учетно-отчетных документов типового ЛПУ, а в здравоохранении их более 300, содержат персональные данные. При создании системы защиты персональных данных (СЗПДн) необходимо выявлять места обработки/хранения персональных данных: информация во многих учреждениях может храниться на бумажных носителях; в Microsoft Word, при передаче данных по страховым программам до сих пор используется Excel, в клиниках могут использоваться самописные программы. Необходимо детально проанализировать функциональную структуру ЛПУ, схемы взаимодействия её подразделений, интеграцию с другими ИС ЛПУ - кадровой, бухгалтерскими системами, взаимодействие с внешними организациями, в том числе с ФОМС. При реализации проектов по защите персональных данных должны регламентироваться все процессы взаимодействия, применяться средства обеспечения безопасности при передаче данных.

Во-вторых, сертификация ИСПДн на отсутствие недекларированных возможностей, что сильно сужает круг возможных внедряемых средств. К специальным информационным системам, которые обрабатывают медицинские данные, предъявляют особое требование по разработке Модели угроз. Модель угроз медицинской системы ЛПУ предусматривает описание характеристик информационной системы, нарушителей, объектов и целей, каналов и способов реализации угроз, пользователей, типов, защищенности, вероятности реализации угроз, оценку их опасности и актуальности. При правильном подходе разработка модели угроз может позволить произвести корректировку требований к СЗПДн, чтобы оставить только актуальные для лечебно-профилактического учреждения угрозы.

Для минимизации затрат на построение системы защиты персональных данных предлагаются методы:

- обезличивания персональных данных за счет присвоения пациентам специальных идентификаторов с использованием для кодирования диагнозов справочника, хранящегося в регистратуре или в отдельной информационной системе;
- абстрагирования: «размывания» точных данных о пациентах, то есть вместо прямого указания диагноза можно просто внести пациента в группу риска или группу для прохождения определенной процедуры;
- разделения пациентов по участкам: вместо точного адреса пациента поликлиника может сохранять в базе лишь номер участка, а точный адрес хранить либо в регистрационной карточке пациента на бумаге, либо в отдельной, хорошо защищенной информационной системе;
- сегментации - разделения общей базы, где хранится вся информация обо всех пациентах, на несколько специализированных, в каждой из которых класс хранимых персональных данных будет ниже, чем в исходной;
- разделения данных - для уменьшения размера базы данных сведения обо всех пациентах стоит разделить на несколько баз данных, например, по участкам или по отделениям, чтобы снизить уровень необходимых средств защиты, а также уменьшить требования к масштабированию всей информационной системы учреждения.

При обезличивании скрывается идентификационная информация пациентов, а при абстрагировании - сведения о здоровье. Перехват данных в канале связи не позволит идентифицировать по этим данным конкретное лицо - что даст возможность снять достаточно серьезные (затратные) требования по криптографической защите.

Работы по сегментации можно провести с помощью соответствующей настройки существующих в учреждении сертифицированных межсетевых экранов. Минимизация затрат на построение системы защиты персональных данных в медицинских учреждениях достигается за счет дифференциации требований, которая означает управление доступом к регистрационным, финансовым, медицинским данным пациентов. Защиту персональных данных обеспечивает использование встроенных в прикладные информационные системы средств, для реализации этого подхода необходимо обращаться к поставщикам и разработчикам ИС для приобретения сертифицированных версий программных продуктов и выполнения требований ФСТЭК к подсистемам управления доступом; регистрации и учета; контроля целостности.

Пользуясь введенной Gartner терминологией 5-ти поколений систем (Collector, Documenter, Helper, Colleague и Mentor), можно сказать, что ведущие современные медицинские системы находятся на уровне 2-3 поколения, лишь некоторые обладают элементами 4-го поколения, характеризующимися поддержкой принятия решений, клинических потоков работ, продвинутых аналитических возможностей. Появление систем 5-го поколения, которые будут выделяться наличием возможности подсказывать врачам возможные пути лечения и диагностики пациентов, прогнозируется не ранее 2015 года.