ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗДРАВООХРАНЕНИИ

[1] В.Б.Алюшкевич, [2] В.А.Дмитриев, [2] В.А.Лапицкий, [1] М.М.Сачек

[1] Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения, г. Минск, Республика Беларусь
[2] Объединенный институт проблем информатики Национальной академии наук Беларуси, г. Минск, Республика Беларусь

В статье приведены направления работы в области информационной безопасности при разработке, создании и эксплуатации медицинских информационных систем.

Ключевые слова: IT-технологии, надежность, информационная безопасность, уязвимость.

Переход на современные информационные технологии (IT-технологии) в медицине улучшает качество сервиса, сокращает время обследования, увеличивает точность диагностики, дает возможность проводить удаленные консультации, удаленную обработку первичной информации, долговременно хранить данные о пациенте в цифровой форме и при необходимости получить к ним доступ из любой точки мира.

Сегодня IT-инфраструктура организации здравоохранения (ОЗ) представляет собой разветвленную сеть, содержащую, как правило, три основных составляющих. Во-первых, это рабочие места сотрудников ОЗ – компьютеры врачей, регистраторов и т.д. Во-вторых, это медицинские информационные системы (МИС) – комплексные автоматизированные информационные системы, в которых объединены электронные медицинские записи о пациентах, данные медицинских исследований в цифровой форме, данные мониторинга состояния пациента с медицинских приборов, средства общения между сотрудниками, финансовая и административная информация. В-третьих, это медицинское оборудование (например, томографы), которое представляет собой медицинский прибор (или набор приборов), совмещенный с компьютером, на котором установлено специализированное программное обеспечение (ПО), и другими устройствами для передачи и вывода информации (например, принтером).

Главная особенность внедряемых МИС в том, что они хранят и обрабатывают конфиденциальную информацию, в том числе персональные данные пациентов, а также сведения, содержащие врачебную и коммерческую тайну. Более того, все МИС имеют жизненно важное значение независимо от того, обеспечивают ли они контроль за работой клинического и диагностического оборудования, учет и оплату лекарств и медицинских услуг или же поддержку принятия врачебных решений. Именно эти обстоятельства и диктуют самые жесткие требования к системам безопасности МИС и накладывают ограничения на доступ к информации.

В МИС не должно быть программных или аппаратных модулей, которые бы могли получить доступ к данным или программам МИС в обход системы безопасности.

Среди мер для повышения надежности систем безопасности МИС целесообразно использовать следующие основные методы и способы защиты:

- улучшение системы регистрации первичных медицинских данных;
- обязательное дублирование информации (лучше ежедневное), хранимой в базах данных различных уровней;
- периодическая (лучше ежедневная) актуализация всех баз данных в МИС (эта мера исключает возможность фальсификации медицинских сведений «задним числом»);
- обеспечение доступа к информации.

Реализация системы безопасности в МИС должна носить комплексный характер, она должна проводиться системно на всех этапах жизнедеятельности МИС: от проектирования и разработки до внедрении и эксплуатации, перекрывать все известные виды угроз безопасности, быть ориентированной на тактическое опережение угроз, соответствовать действующему законодательству и всем ведомственным актам системы здравоохранения, выдвигать только обоснованные ограничения на функциональные возможности и производительность МИС. С точки зрения архитектуры система безопасности должна функционировать на всех этапах обработки и передачи информации – сервере, каналах связи и конечных устройствах (компьютерах пользователей). При этом применяемые методы также должны быть реализованы на всей логической цепочке обеспечения безопасности: предупреждения, обнаружения, оповещения ответственных лиц, нейтрализации или блокирования, протоколирования, восстановления нормальной работы.

Современный опыт решения проблем информационной безопасности показывает, что для до-

стижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов.

Первым и наиболее важным является *принцип непрерывности совершенствования и развития системы информационной безопасности*: постоянный контроль функционирования системы, выявление ее слабых мест, возможных каналов утечки информации и несанкционированного доступа, обновление и дополнение механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, обоснование и реализация на этой основе наиболее рациональных методов, способов и путей защиты информации. Таким образом, обеспечение информационной безопасности не может быть разовым мероприятием.

Вторым является *принцип комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации*.

Комплексный характер защиты информации обусловлен действиями злоумышленников. Здесь правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения. Кроме того, наибольший эффект достигается в том случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – систему информационной безопасности. Только в этом случае появляются системные свойства, не присущие ни одному из отдельных элементов системы защиты, а также возможность управлять системой, перераспределять ее ресурсы и применять современные методы повышения эффективности ее функционирования.

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм представителей службы информационной безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами. Без соблюдения этих условий никакая система информационной безопасности не может обеспечить требуемого уровня защиты.

Важной разновидностью МИС являются медицинские приборно-компьютерные системы (МПКС). Основное отличие систем этого класса – работа в условиях непосредственного контакта с объектом исследования и в реальном режиме времени. Они представляют собой сложные программно-аппаратные комплексы. Для работы МПКС, помимо вычислительной техники, необходимы специальные медицинские приборы, оборудование, телетехника, средства связи. Опасность взлома этих систем представляет серьезную угрозу для организаций здравоохранения. Поскольку у многих медицинских приборов коммерчески доступные операционные системы, они столь же уязвимы для атак, как и обычные компьютеры. Но даже приборы со специализированными системами могут оказаться под ударом, часто – через механизм обновления программного обеспечения.

Повсеместное использование глобальных информационных систем в медицине открывает качественно новые возможности:

- обеспечение взаимодействия региональных клиник с крупными медицинскими центрами;
- оперативное получение результатов последних научных исследований;
- подготовка и переподготовка кадров.

Перечисленные возможности можно охарактеризовать одним общим понятием – *телемедицина*, которая предусматривает дистанционное управление медицинской информацией.

Телемедицинские технологии находят все более широкое применение в практике клинической медицины при диагностике и лечении сложных случаев заболеваний.

Основное условие защиты медицинской информации при проведении телемедицинской консультации (ТМК) – обеспечение ее целостности, аутентичности, неизменности, сохранности и доступности. Обязательным требованием, с точки зрения законодательства, является обеспечение конфиденциальности персональной информации, в том числе, клинической информации о больном, составляющей предмет врачебной тайны.

Под целостностью медицинской информации в ходе ТМК понимается отсутствие ее потерь в процессе подготовки, преобразования, передачи, приема, обработки и предоставления информации. Это не означает, что информация не может разделяться на части, передаваемые или преобразуемые по отдельности. Целостность информации должна обеспечиваться протоколами передачи и преобразования данных и действиями всех участников ТМК.

Под аутентичностью медицинской информации в ходе ТМК понимается полное совпадение передаваемой и получаемой информации. В частности, аутентичность информации для аудио- и видеоинформации предполагает, что изображение и звук практически одинаковы на передающей и принимающей сторонах. Под аутентификацией (подлинностью) участников телеконсультации понимается взаимная доказуемая идентификация партнеров связи.

Под неизменностью медицинской информации понимается отсутствие искажений (преднамеренных или непреднамеренных) информации участниками ТМК или третьими лицами в ходе ТМК. Неизменность информации должна обеспечиваться протоколами передачи и преобразования дан-

ных и мерами по защите информации от несанкционированного доступа.

Под сохранностью медицинской информации понимается необходимость документирования (протоколирования) хода и результатов ТМК – всего комплекса представленных медицинских материалов, их обсуждения (устного при проведении видеоконференции или письменного при переписке по электронной почте) и заключения консультанта на соответствующих носителях, включая запись видеоконсультаций, представляющую собой ее синхронную копию.

Под доступностью медицинской информации при использовании ТМК понимается возможность для участников ТМК реально и своевременно получить доступ к медицинской информации, используемой в ходе телеконсультации, что может быть обеспечено только согласованными действиями всех участников ТМК.

Под конфиденциальностью понимается ограничение доступа к совокупности данных, являющихся предметом ТМК, включая ее результаты.

Информационная безопасность в ходе ТМК должна базироваться на использовании комплекса организационных и технических средств (регламентирующие документы, обучение персонала, программно-аппаратные решения, включая интероперабельность телемедицинских приложений), обеспечивающих конфиденциальность телеконсультации и защиту персонифицированной медицинской информации от несанкционированного доступа на различных этапах подготовки, обмена данными, сеанса дистанционного консультирования, промежуточного и последующего хранения документации с учетом ответственности (правовые аспекты) лиц, принимавших участие в проведении и поддержке ТМК.

Обеспечение сохранности информации (от подачи заявки до выдачи заключения) предусматривает: санкционированный доступ, аутентификацию и авторизацию пользователей (консультируемых и консультантов, технического персонала) при работе с телемедицинскими системами (ТМС) и базами данных (БД) консультированных пациентов (текущими и архивными). Авторизация доступа к ТМС и БД должна обеспечиваться программными и/или аппаратными средствами идентификации.

Комплексная защита информации при использовании для ТМК открытых каналов связи, включая Интернет, должна предусматривать:

- идентификацию и проверку подлинности (аутентификация) пользователей базы данных;
- защиту информации при передаче по каналам связи;
- управление целостностью данных (защита от несанкционированного изменения информации);
- применение обеими сторонами технологии электронной цифровой подписи.

Обучение персонала – основа информационной безопасности. Оно позволяет уменьшить негативные последствия атак на систему, приводящие к нарушению ее работоспособности и снизить потери информации, а также сократить время, необходимое для восстановления поврежденных данных.

Профессиональное обучение должно сформировать знания, необходимые при работе:

- с электронной почтой;
- с системами видеоконференцсвязи;
- с Интернет (Web-сервер);
- с базами данных;
- с программными средствами защиты информации.

Технические решения, направленные на обеспечение информационной безопасности при проведении ТМК, предусматривают:

- использование программно-аппаратных средств, удовлетворяющих условию аутентичности медицинской информации, передаваемой и получаемой в ходе ТМК;
- настройку оборудования;
- контроль наличия слабых мест (уязвимостей) в программном и техническом обеспечении;
- использование специальных программных и аппаратных средств обеспечения информационной безопасности, а именно:
- систем идентификации и аутентификации;
- систем управления разграничением доступа к информации;
- систем фильтрации, анализа трафика и его шифрования;
- систем обнаружения и предотвращения помех (атак) и уязвимостей;
- систем резервного копирования баз данных.

INFORMATION SAFETY ISSUES IN HEALTHCARE

[1]V.B.Alyushkevich, [2]V.A.Dmitriyev, [2]V.A.Lapitski, [1]M.M.Sachek

[1] Republican Scientific and Practical Centre of Medical Technologies, Informatization, Administration and Management of Health, Minsk, Republic of Belarus

[2] United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Republic of Belarus

The article presents aspects of work related to information safety when developing, creating and maintaining medical information systems.

Keywords: IT-technologies, reliability, information safety, vulnerability.

Поступила 01.08.2016 г.