ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саракуца И. М., Мальцева Е. С.

Бойправ О. В. – м.т.н.

В настоящее время активно создаются виртуальные инфраструктуры здравоохранения, объединяющие на базе единого информационного пространства (ЕИП) все составляющие элементы системы охраны здоровья населения. Создаваемые виртуальные инфраструктуры позволяют решить актуальную задачу дистанционного мониторинга состояния здоровья населения. При этом остро стоит вопрос с обеспечением информационной безопасности передаваемых физиологических данных.

Телемедицина – это отрасль медицины, которая использует телекоммуникационные и электронные информационные технологии для обеспечения медицинской помощи на расстоянии. Предмет телемедицины - передача посредством телекоммуникаций и компьютерных технологий всех видов медицинской информации между отдаленными друг от друга пунктами.

Телемедицину можно разделить на две части: локальная телемедицина (в рамках одного медицинского учреждения) и глобальная телемедицина (между различными медицинскими учреждениями). Локальная ТМ создаётся на базе уже действующей в клинике системы взаимоотношений между администрацией, врачами и пациентами. Глобальная ТМ создается при взаимодействии специалистов двух или нескольких медицинских учреждений.

В состав ТМ консультативно-диагностических системах входят следующие подсистемы:

- подсистема консультативно-диагностических пунктов (КДП);
- подсистема консультативно-диагностических центров (КДЦ);
- подсистема координационно-технического центра.

ТМКДС имеет структуру "клиент-сервер" и состоит из двух независимых частей - "клиента" и «сервера». В роли клиента выступают подсистема КДП и подсистема КДЦ. Приложение-сервер инициализируется при запуске и далее ожидает поступления запросов от клиентов: передачи телемедицинских запросов, ответов консультантов, информации о прохождении запроса и т. п.

Приложение-клиент посылает запрос на соединение с сервером, а также выполняет передачу телемедицинских запросов, ответов консультантов, информации о прохождении запроса и т.д. в зависимости от типа клиента (КДП или КДЦ).

Основная база данных ТМКДС находится на сервере. В БД хранятся консультационные запросы, полученные от удаленных пунктов, заключения консультантов, полученные от консультационных центров, информация о пользователях системы.

В качестве протокола обмена данными в системе используется TCP/IP, являющийся стандартным протоколом для обмена данными в сетях типа Интернет и интранет. В сетях на базе TCP/IP в наши дни наиболее широко используется интерфейс, основанный на сокетах.

В качестве структурной основы для хранения и передачи информации в системе используется распределенная БД. При этом клиент и сервер имеют независимые БД, информация в которых может дублироваться с целью сокращения трафика и повышения эффективности работы системы.

Связь между ТМ пунктами и ТМ центрами организуется по выделенным каналам связи или через Интернет. С экономической точки зрения наиболее выгодным является использование сети Интернет при условии, что провайдер обеспечит гарантированную пропускную способность, необходимую для удовлетворительной работы систем видеоконференцсвязи.

Как и у других телекоммуникационных систем, у телемедицинских систем имеется ряд нерешённых проблем, одной из которых является проблема защиты информации. Анализ ТМКДС позволяет представить их в обобщенном виде как совокупность КДП, КДЦ и узлов коммутации, соединенных между собой каналами связи.

При большом количестве пользователей необходима также защита и от пользователя-нарушителя, являющегося штатным сотрудником или законным абонентом ТМКДС. Кроме того, территориальное распределение средств КДП и КДЦ предполагает реализацию связи на дальние расстояния по кабелю, радиоканала и другим каналам, физически доступным для нарушителя, так как реализовать их охрану и контроль доступа к ним не представляется возможным. Поэтому вполне реальна возможность подключения нарушителя к каналам и линиям связи в виде шлюза, через который может происходить утечка информации, но и её модификация, разрушение, в результате чего могут подвергаться опасности системные отношения и связи между элементами ТМКДС.

Возможными каналами НСД для ТМКДС являются:

- штатные средства, при их использовании законными пользователями не по назначению и за пределами своих полномочий, а также посторонними лицами;
- технологические пульты и средства управления;
- побочное эми информации с аппаратуры технических средств;

- побочные наводки информации по сети электропитания, на вспомогательных и посторонних коммуникациях, сервисном оборудовании;
- изменение удаление, задержка, переупорядочивание, дублирование и посылка ложных сообщений;
- воспрепятствование передаче сообщений;
- осуществление ложных соединений;
- анализ трафика и id-ров абонентской сети;
- повторы сообщений, передача различного рода «информационного мусора» и т. д.

В зависимости от ожидаемой модели нарушителя этот перечень может быть до определённой степени сокращён. Нарушителем может быть человек: посторонний; законный пользователь или из числа лиц обслуживающего персонала. Квалификация его также может быть различной. Он может обладать или не обладать определенным набором технических средств, работать в комфортных условиях риска; быть единственным или в составе организованной группы. Круг доверенных лиц зависит от важности обрабатываемой информации и выполняемых задач. Такими лицами должны быть, по меньшей мере, администраторы, руководители работ и должностные лица службы безопасности.

Рекомендуемые средства защиты информации ТМКДС в соответствии с возможными несанкционированными действиями представлены в табл. 1.

Табл. 1 – Рекомендуемые средства защиты информации ТМКДС в соответствии с возможными несанкционированными действиями

№ п/п	Возможные несанкционированные действия	Средства защиты информации ТМКДС
1.	Устройства ввода-вывода информации	- Средства контроля и разграничения доступа в помещения. - Программа контроля и разграничения доступа к ПО и информации. - Антивирусные средства.
2.	Машинные носители информации	- Учет и разграничение доступа к носителям. - Электронная идентификация носителей. - Шифрование информации
3.	Носители ПО	-Учет, регистрация и разграничение доступа к носителям ПО. - Верификация и контроль целостности ПО. - Резервирование ПО с контролем доступа к его копии.
4.	Средства загрузки ПО	- Средства контроля и разграничения доступа в помещениях. - Антивирусные средства.
5.	Технологические пульты и органы управления, внутренний монтаж аппаратуры	- Средства контроля и разграничения доступа в помещения. - Система контроля вскрытия аппаратуры.
6.	Побочное электромагнитное излучение и наводки информации	- Средства снижения и зашумления уровня излучения и наводок информации на границе контролируемой зоны объекта автоматизации.
7.	Мусорная корзина	- Средства уничтожения носителей закрытой информации.
8.	Анализ трафика и идентификаторов получателей сообщений	- Специальные средства заполнения потока. - Линейное шифрование.
9.	Посылка ложного сообщения	- Цифровая подпись содержательной части сообщения.
10.	Задержка и удаление сообщений	- Подтверждение получения сообщений. - Введение контрольного интервала времени ответа. - Дублирование соединения или маршрута.
11.	Отказ отправителя от переданного, получателя – от принятого сообщения	- Центр контроля и управления безопасностью информации.

Список использованных источников:

1. Наумов В.Б., Савельев Д. А. Правовые аспекты телемедицины. – СПб.: Издательство "Анатолия", 2002. – 107 с.
2. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
3. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006. – 208 с.
4. Казаков В.Н., Климовицкий В.Г., Владзимирский А.В. Телемедицина. - Донецк: Типография ООО «Норд», 2002. – 100 с.