Раздел V. Информационно-психологическая безопасность человека

УДК 002.56:681.5

Ю.М. Брумштейн, С.В. Чернов

АНАЛИЗ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИС В УЧРЕЖДЕНИЯХ, ОКАЗЫВАЮЩИХ ВЫСОКОТЕХНОЛОГИЧНУЮ МЕДИЦИНСКУЮ ПОМОЩЬ

Рассмотрена структура информационных ресурсов и МИС в учреждениях высокотехнологичной медпомощи. Проанализирована совокупность угроз для МИС в отношении информационной безопасности, возможные подходы к ее обеспечению.

Информационная безопасность; медицинские информационные системы; высокотехнологичная медпомощь.

Yu.M. Brumshteyn, S.V. Chernov

THE ANALYSIS OF INFORMATION SAFETY MIS MAINTENANCE QUESTIONS IN THE ESTABLISHMENTS, RENDERING HI-TECH MEDICAL AID

The information resources and MIS structure in hi-tech medical service establishments is considered. Set of threats for MIS, concerning information safety, possible approaches to its maintenance is analysed.

Information safety; medical information systems (MIS); hi-tech medical service.

Строительство и эксплуатация организаций высокотехнологичной медицинской помощи (ВТМ) является сейчас одним из важных направлений повышения качества и доступности медпомощи для населения России, обеспечения «качества человеческого капитала» регионов и страны. Организации ВТМ (ОВТМ) – это, в основном, бюджетные учреждения. Однако элементы ВТМ начинают все шире использоваться и в коммерческих медучреждениях, что повышает их конкурентоспособность на рынке платных медуслуг. Традиционно отнесение организаций к ОВТМ осуществляется исходя из их оснащенности современным медоборудованием и состава оказываемых медуслуг. Отметим, что в ОВТМ объемы получаемой, хранимой, обрабатываемой информации (как правило, в цифровой форме) значительно выше, чем в «обычных» медучреждениях. Поэтому для ОВТМ вопросы работы с информацией и, в частности, безопасности использования медицинских информационных систем (МИС), играют ключевую роль. Это в полной мере относится и к ФГУ федеральный центр сердечно-сосудистой хирургии (ФЦССХ) в г. Астрахань, Министерства здравоохранения и социального развития Российской Федерации. Данная статья подготовлена с учетом опыта создания/эксплуатации МИС в данном ФЦССХ. Центр построен в рамках федеральной программы обеспечения населения ВТМ и бесплатно обслуживает жителей ряда южных регионов России (в рамках выделенных для этих регионов квот). Цели данной статьи: системный анализ вопросов информационной бесопасности (ИБ) для МИС ОВТМ;

разработка методов оценки качества ИБ (КИБ); формализация подходов к оценке эффективности расходов на ИБ; анализ опыта обеспечения ИБ на материале ФЦССХ. В дальнейшем это позволит построить модели для динамической оптимизации затрат по отдельным направлениям обеспечения ИБ – с учетом накапливаемых данных по реализации угроз и ресурсным ограничениям.

Сам по себе термин МИС традициионно понимается двояко: как МИС предназначенные для целей управления медучреждениями; МИС, обрабатывающие/отображающие данные, поступающие непосредственно с медоборудования – в последнем случае соответствующие программные средства (ПС) могут быть «встроенными» в оборудование. Для МИС ОВТМ фактически происходит интеграция этих двух «видов», так как результаты диагностики, лечения, мониторинга пациентов и прочие включаются в базы данных (БД) общей МИС организации и используются для принятия оперативных решений, планирования деятельности и т.д. Для ФЦССХ г. Астрахани объем добавляемой в МИС информации растет по мере увеличения функциональности МИС [2] и на 01.05.2010 г. составляет, порядка 18 Гб/сутки, а общий объем информационных ресурсов (ИР) в цифровой форме, относящихся к одному «пролеченному пациенту» – 2:-5 Гб (при двух- и более кратном «пролечивании» пациента в ФЦССХ показатели, естественно, выше).

Третьим компонентом интегрированных МИС ОВТМ в перспективе может стать телемедицинская информация (ТМИ), в том числе связанная с видеозаписью хода операций, телеконсультированием, мониторингом состояния пациентов и пр. В случае фиксации и хранения ТМИ в МИС темпы роста ИР ОВТМ (и, в частности, ФЦССХ) могут значительно возрасти.

В целом для МИС ОВТМ характерны: непосредственное влияние качества их функционирования на большинство технологических цепочек работы с пациентами; большие объемы персональной медицинской информации (ПМИ); в перспективе – интенсивный информационный обмен с другими медучреждениями, в том числе ТМИ. Поэтому для МИС ОВТМ вопросы ИБ играют важнейшую роль, с позиций обеспечения информационно-психологической безопасности пациентов, их родственников, персонала медучреждений и пр.

В ОВТМ помимо МИС используются и другие ПС, включая следующие направления: бухгалтерский учет; кадровая информация; учет продуктов для пищеблока и пр. Новым для России фактором является дистанционный контроль через Интернет условий работы высокотехнологичного медоборудования в ОВТМ непосредственно фирмами-производителями или их сервисными центрами. Это, безусловно, влияет и на уровень ИБ ОВТМ.

Процессы информатизации в сфере здравоохранения России по сравнению с развитыми странами следует считать находящимися на начальной стадии. Частично признанием этого факта является выделение по программе дополнительного финансирования здравоохранения на 2011–2012 гг. суммы в 24 млрд руб. (из 460 млрд) специально на цели «информатизации» – в основном для создания общероссийской базы электронных полисов обязательного медицинского страхования [1]. Это даст возможность пользоваться ими на всей территории России, а не только в том регионе, в котором они были выданы (что сейчас фактически имеет место из-за «*сложной системы взаиморачетов между регионами*» [1]).

Разработок ПС для организаций системы здравоохранения существует уже достаточно много. Их функциональное назначение – от информатизации отдельных кабинетов и амбулаторных медучреждений до комплексной информатизации регионов. При этом: стоимость разработок ПС «профессионального класса» достаточно высока; службы сервисной поддержки пользователей (ССПП) ПС в регионах обычно отсутствуют; многие медучреждения в рамках информатизации разра-

батывают и эксплуатируют собственные ПС, в том числе даже рассчитанные на использование DOS-овского интерфейса; в сфере информатизации здравоохранения ПС МИС централизованно не сертифицируются в отношении стандартов хранения/передачи данных. Это приводит к взаимной несовместимости ПС и, как следствие, к затруднениям в создания единого информационного пространства лечебно-диагностических медучреждений, органов управления здравохранением, аптек и пр. даже в пределах отдельных регионов. Для ОВТМ, обслуживающих несколько регионов, этот вопрос особенно актуален. Сравним: все ПС бухучета в России подлежат обязательной сертификации Минфином; количество оставшихся на рынке фирм-разработчиков ПС бухучета очень невелико; все они обладают развитой сетью ССПП. Аналогичная ситуация имеет место и по сметным программам для строительства и многих (если не большинства) других ПС массового применения.

Сектор ПС МИС для ОВТМ на рынке является неразвитым, а имеющиеся предложения очень дороги и плохо учитывают конкретные потребности отдельных ОВТМ, в том числе ФЦССХ. Кроме того, с позиций ИБ ориентация на ПС сторонних разработчиков (кроме централизованных поставок от Минздравсоцразвития), достаточно «рискованна» из-за: отсутствия гарантий, что фирма-разработчик не «исчезнет» с рынка; предстоящих перемен в сфере информатизации здравоохранения и др. Поэтому руководством ФЦССХ г. Астрахань было принято решение о формировании собственной группы разработчиков и создании комплекса ПС.

В настоящее время в ФЦССХ успешно функционируют следующие подсистемы: «IMS: Врач стационара», «IMS: Врач поликлиники», «IMS: База данных». В стадии разработки находятся модули медицинской и экномической статистик, складского учета, госпитализации. Для автоматизации учета «движения» расходных материалов внедряется система, основанная на использовании штрих-кодов. Отметим, что комплексная информатизация ФЦССХ вообще говоря требует интеграции с МИС еще систем: кадрового учета; расчета зарплаты сотрудников; вывода графической информации по отдельным уникальным операциям, проведенным в центре; управления сайтом организации в Интернете и пр. Этапность разработок подсистем определяется: их приоритетами для руководства ФЦССХ; объемами трудозатрат на сопровождение уже эксплуатируемых подсистем; имеющимися трудовыми ресурсами ИТ-специалистов ФЦССХ.

Обычно обеспечение ИБ связывается [4] с защитой ИР от несанкционированного доступа, передачи, повреждения, уничтожения. Применительно к МИС ОВТМ этот перечень по-нашему мнению необходимо, дополнить еще направлениями защиты, связанными с: отказами оборудования, обеспечивающего съем медицинской информации с пациентов, ее анализ/отображение, ввод в БД МИС; отказами аппаратных средств ПЭВМ и серверов, входящих в МИС; временной утратой или замедлением доступа к ИР по различным причинам; нарушением работоспособности внутренних и/или внешних коммуникационных каналов; утратой работоспособности МИС при отключениях электроэнергии и пр.

В связи с введением в действие Закона «О персональных данных» [6], предусматривается обязательное лицензирование медучреждений, включая и ОВТМ, в отношении ИБ ПМИ. В то же время, возможности, предусмотренные Законом «Об электронной цифровой подписи» [7], пока в медучреждениях практически не используются – ни для внутреннего «документооборота» медицинских данных, ни при информационном обмене с внешней средой. Постепенно начинает применяться шифрование данных с ПМИ, передаваемых в другие медучреждения.

Ущербы, связанные с нарушением ИБ (в приведенном расширенном толковании), могут в конечном счете наноситься: пациентам и иным лицам, с которыми

работают ОВТМ; самим ОВТМ как юрлицам; другим медучреждениям; персоналу медучреждений, в том числе ОВТМ и пр. Большинство из этих направлений ущерба в практическом плане нуждаются в дальнейшей расшифровке.

Управление КИБ ОВТМ (в том числе и КИБ МИС) осуществляется в условиях вероятностного характера угроз и различных ограничений (нормативных; финансовых; кадровых, организационного характера и пр.), часть которых носит «барьерный» характер, т.е. не должна нарушаться. Типичными постановками задач управления КИБ МИС могут быть: обеспечение формального соблюдения требований к защите ПМИ при минимальных затратах на ресурсы (МЗНР); постоянное поддержание КИБ на уровне не хуже требуемого при условии МЗНР; использование всех ресурсов (в том числе замены оборудования, разработки/совершенствования ПС и пр.) для достижения наилучшего КИБ и др.

В общем случае возможны различные подходы к оценкам КИБ МИС.

(**А**) Сравнение фактических и необходимых значений показателей (НЗП) для КИБ. При этом НЗП могут быть нормативными или устанавливаться руководством конкретного ОВТМ с учетом его специфики. Простейший вариант оценки – «бинарный», т.е. обеспечиваются ли все НЗП по ИБ или нет.

(**Б**) Если часть НЗП не обеспечивается, то возможна оценка КИБ в виде

$$Q_1 = K_+ / (K_+ + K_-), \tag{1}$$

где K_+, K_- – количества показателей, для которых НЗП соответственно выполняются и не выполняются.

(**В**) Обобщением формулы (1) с учетом важности показателей может быть

$$Q_2 = (\sum_{i=1}^{I} W_i \lambda_i) / \sum_{i=1}^{I} W_i, \tag{2}$$

где I – количество принимаемых во внимание показателей ИБ; $\lambda_i = 0$, если НЗП не выполняется и $\lambda_i = 1$, если НЗП выполняется; весовые коэффициенты для показателей (W_i) могут быть определены, например, экспертно.

(**Г**) При количественном учете отличий фактических значений показателей от НЗП в сочетании с использованием весовых коэффициентов V_i имеем

$$Q_3 = (\sum_{i=1}^{I} V_i \left| Z_i^{(f)} - Z_i^{(n)} \right|) / \sum_{i=1}^{I} V_i, \tag{3}$$

где $Z_i^{(f)}, Z_i^{(n)}$ – фактическое и необходимое значение **i**-го показателя КИБ. Возможные обобщения (3): с несимметричными весовыми коэффициентами для отклонений показателей в б*о*льшую и меньшую стороны; переход от НЗП к «интервалам» значений показателей; учет долей времени, когда нарушаются НЗП.

(**Д**) Использование для КИБ величины, обратно пропорциональной вероятному суммарному ущербу для МИС от всех видов угроз за определенный период:

$$Q_4 = 1 / U_\Sigma = 1 / (\sum_{j=1}^{J} U_j); \tag{4}$$

$$U_j = \sum_{k=1}^{K} A_{j,k} U_{j,k}, \quad (5)$$

где J – количество учитываемых видов угроз; K – количество классов объектов, которым угрозы могут наносить ущерб; $A_{j,k}, U_{j,k}$ – вероятности реализации и ущербы для МИС ОВТМ при реализации **j**-й угрозы в отношении **k**-го класса объектов. Формула (5): определяет модель линейно-независимых ущербов от отдельных видов угроз (что выполняется не всегда); может быть обобщена на случай вероятностного распределения величин ущербов по диапазонам значений. Рентабельность затрат на обеспечение ИБ МИС ОВТМ обычно может быть оценена исходя из величин предотвращаемых вероятных ущербов (P):

$$R_1 = 100\% * ((P - E) / E), \quad (6)$$

где E – величина затрат на обеспечение ИБ. Подчеркнем, что E фактически имеет две компоненты: текущие затраты, направленные в основном на поддержание КИБ (в т.ч. с учетом роста объемов ИР и трафиков с внешней информационной средой); перспективные, которые будут давать положительный эффект в отношении КИБ с запаздыванием. Поэтому в общем случае может быть целесообразным модифицировать (6) с введением дисконтирующих коэффициентов (учитывающих инфляционные процессы) для предотвращаемых ущербов и затрат

$$R_2 = 100\% \cdot (\sum_{l=1}^{L} (D_l * (P_l - E_l))) / (\sum_{l=1}^{L} (D_l * E_l)). \quad (7)$$

При этом: эффективность конкретных затрат на ИБ в ОВТМ определяется не только сиюминутными эффектами, но и долговременными; эффективность принятых мер ИБ со временем обычно снижается (вплоть «до нуля»), поэтому произведенные затраты должны быть отнесены к ограниченному периоду времени; один вид затрат может снижать вероятности реализации угроз и/или ущербов от них сразу для нескольких видов угроз и/или классов объектов (причем в разной степени). Объем затрат на ИБ серьезно зависит от календарного времени, за которое необходимо получить нужный результат; требуемого КИБ МИС ОВТМ.

Конкретно по ФЦССХ структура затрат на ИБ включает: обеспечение мер физической защиты МИС в отношении доступа посторонних лиц к ПЭВМ и серверам; защиту оборудования от неблагоприятных температурных режимов, перерывов энергопитания, скачков напряжения и пр.; разработка собственных ПС и закупка готовых ПС, включая антивирусные средства; использование средств разграничения доступа к ИР [3]; повышение общей «компьютерной квалификации» персонала ФЦССХ и др. Оптимальное распределение затрат по этим направлениям относится к области задач теории принятия решений в нечетких условиях [5].

В качестве перспективного технического решения, позволяющего повысить КИБ МИС, рассматривается возможность замены в ФЦССХ части ПЭВМ пользователей на бездисковые терминальные комплексы («тонкие клиенты»), что значительно упростит вопросы администрирования компьютерной сети. Кроме того, предполагается разделение сети на две подсети – «защищенную» часть (не имеющую выхода в Интернет) и «незащищенную» – в которой такой выход будет иметься. Связь этих подсетей предполагается организовать через специализированное серверное оборудование, обеспечивающее адекватные меры ИБ.

Итак, сделаем **выводы**. 1. В рамках процессов информатизации организаций здравоохранения (и, особенно, ОВТМ) необходимо уделять особое внимание во-

просам ИБ, в том числе в отношении ПМИ. 2. Целесообразно создание МИС ОВТМ, учитывающих специфику работы этих организаций, в том числе очень большие объемы ИР и активное взаимодействие с внешней информационной средой. 3. Эффективность затрат, связанных с ИБ, целесообразно определять с учетом как текущих положительных эффектов, так и долговременных. 4. Модели для оценки эффективности затрат на ИБ нуждаются в дальнейшей разработке, в т.ч. в отношении учета стохастических факторов. 5. Целесообразно формирование координирующих механизмов, обеспечивающих взаимоувязку информатизации ОВТМ (чаще всего это федеральные структуры) и местных медучреждений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Батенёва Т.* Здравоохранение идет на поправку. За два года больницы и поликлиники страны получат 460 млрд. рублей на перевооружение и модернизацию // Известия. – № 71/28086 от 22.04.2010. – С. 1-2.
2. *Брумштейн Ю.М., Чернов С.В., Королев М.Е.* Использование телемедицинских технологий и информационная безопасность корпоративных информационных систем медучреждений // Теория, методы проектирования, программно-техническая платформа корпоративных информационных систем: Материалы VII Междунар. науч.-практ. конф. – Новочеркасск, 25.05.2009. – С. 47-50.
3. *Девянин П.Н.* Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005. – 144 с.
4. *Партыка Т.Л., Попов И.И.* Информационная безопасность. – М.: ФОРУМ: ИНФРА-М, 2005. – 368 с.
5. *Черноруцкий И.Г.* Методы принятия решений. – СПб.: БХВ-Петербург, 2005. – 416 с.
6. Федеральный Закон «*О персональных данных*» – от 27.07.2006г. № 152-ФЗ (с изменениями от 25 ноября 2009 г.).
7. Федеральный Закон «*Об электронной цифровой подписи*» – от 10.01.2002 г. № 1-ФЗ.

Брумштейн Юрий Моисеевич
Астраханский государственный университет.
E-mail: brum2003@mail.ru.
414040, г. Астрахань, пл. Карла Маркса, д. 21, кв. 34.
Тел.: 88512257120.

Чернов Сергей Владимирович
Федеральное государственное учреждение «Федеральный центр сердечно-сосудистой хирургии» Министерства здравоохранения и социального развития Российской Федерации.
E-mail: chernov_serzh@mail.ru.
414045, г. Астрахань, ул. Бэра, 55, кв. 53.
Тел.: +79054800777.

Brumshteyn Yurij Moiseevich
Astrakhan State University.
E-mail: brum2003@mail.ru.
Flat 34, home 21, Square Karla Marksa, 414040, Russia.
Phone: +78512257120.

Chernov Sergei Vladimirovich
Federal state establishment «Federal centre of cardiovascular surgery» for health and social development Ministry of the Russian Federation.
E-mail: chernov_serzh@mail.ru.
Sq. 53, 55 Bera street, Astrakhan, 414045, Russia.
Phone.: +79054800777.