Н. Ф. Князюк
(к.м.н., заведующая кафедрой менеджмента)
Байкальская международная бизнес-школа
Иркутского государственного университета

МЕНЕДЖМЕНТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ ТРЕБОВАНИЙ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27005:2011

Внедрение современных информационных технологий в медицинских организациях позволяет вывести их работу на качественно новый уровень, повысить эффективность работы врачей-специалистов и немедицинских служб, обеспечить лояльность медицинского персонала и рост удовлетворенности пациентов. Однако, одновременно с разработкой, внедрением и совершенствованием информационной системы необходимо предпринимать управленческие воздействия, направленные на выявление уязвимых мест системы, угроз и рисков. Правомерно задать следующий вопрос: какие же угрозы безопасности информации могут возникнуть? Прежде всего, это угрозы, создающие опасность конфиденциальности информации. Как известно, информация в зависи-

мости от категории доступа к ней подразделяется на общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [1]. Именно обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, передавать информацию другим лицам по договору или на ином установленном законом основании, а также ограничивать доступ к информации, если такая обязанность установлена федеральными законами. Особенно актуальной данная задача представляется в свете реализации закона №152-ФЗ «О персональных данных». Для обеспечения безопасности персональных данных пациентов медицинских организаций необходимы не только технические, но и организационные меры защиты. Особенность обработки персональных данных в медицинских организациях заключается также в том, что передача сведений, составляющих врачебную тайну, разрешена только с согласия пациента, за исключением случаев, предусмотренных статьей 61 «Основ законодательства РФ об охране здоровья граждан». Несмотря на то, что сегодня достаточно широко распространены такие угрозы, как «вирусы», «черви», спам и т. д., большой опасности для ИБ они уже не несут. Существующие на рынке средства достаточно эффективно защищают от них ИТ-инфраструктуру медицинской организации, необходимо только осознать важность их применения и выделить на их внедрение соответствующие ресурсы. Гораздо больший риск несут угрозы, исходящие изнутри самой организации. Существует масса каналов утечки данных, в первую очередь это, конечно же, Интернет и электронная почта. Далее — портативные накопители: «флешки», карты памяти, сотовые телефоны и т. д. Нужную информацию можно распечатать на принтере. Если медицинская организация будет отслеживать информацию, передаваемую по данным каналам, то риски в сфере ИБ можно свести к минимуму. Но эти действия, требующие больших затрат человеческих и временных ресурсов, с большой вероятностью обречены на провал. Для обеспечения ИБ в организации должны существовать корпоративные политики безопасности. А программные и аппаратные средства лишь призваны выполнять данные политики ИБ.

В связи с этим представляется необходимым определение руководством основных направлений разработки и внедрения системы менеджмента информационной безопасности, в основе которой — создание эффективной системы менеджмента информационной безопасности (СМИБ). Этот подход должен поддерживать менеджмент рисков для всей организации. Менеджмент рисков информационной безопасности (ИБ) должен быть неотъемлемой частью всех видов деятельности, связанных с менеджментом информационной безопасности, а также должен применяться для реализации и поддержки функционирования

СМИБ организации. Система менеджмента информационной безопасности (СМИБ) необходима любой медицинской организации и ее функционирование должно быть направлено на сохранение целостности, конфиденциальности и доступности ее информационных активов.

Нынешний год оказался революционным для российской организационной базы информационной безопасности — были приняты стандарты ГОСТ ИСО/МЭК 17799 и ГОСТ ИСО/МЭК 27001 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасности — Требования», являющиеся техническими переводами версий международных стандартов серии ISO 27000, в основе которых лежит авторитетный британский стандарт BS 7799, включающий в себя три составные части:

- BS 7799-1:2005. Information security management. Code of practice for information security management (Практические правила управления информационной безопасностью);
- BS 7799-2:2005. Information security management. Specification for information security management systems (Требования к системам управления информационной безопасностью);
- BS 7799-3:2006. Information security management systems. Guidelines for information security risk management (Руководство по управлению рисками информационной безопасности).

Первые две части получили международное признание и представляют собой практические рекомендации по построению системы ИБ и оценочные требования (главным образом сертификационные) к системам управления ИБ (СУИБ). Третья часть британского стандарта ожидает получения международного статуса и посвящена анализу, оценке и управлению рисками.

Современные практики по управлению СМИБ базируются на международном стандарте ISO/IEC 27001 [2]. В данном стандарте определены основные цели и средства контроля, представляющие возможность устанавливать, применять, пересматривать, контролировать и поддерживать эффективную систему менеджмента информационной безопасности. Стандарт устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной системы менеджмента информационной безопасности в контексте существующих рисков организации. Менеджмент риска информационной безопасности должен быть непрерывным процессом и связан с анализом того, что может произойти, и какими могут быть возможные последствия, прежде чем выработать решение о том, что и когда должно быть сделано для снижения риска до приемлемого уровня. В этом контексте новый международный стандарт ISO/IEC 27005:2011 «Информационные технологии — Методы обеспечения безопасности — Управление рисками информационной

безопасности» может помочь медицинским организациям в повышении уровня управления рисками информационной безопасности. Новый стандарт описывает процесс управления рисками информационной безопасности и соответствующие действия и соответствует общим принципам, перечисленным в стандарте ISO/IEC 27001:2005. Недостаток отечественной нормативной базы ИБ состоит в отсутствии российского ГОСТа по рискам. Иначе говоря, отечественные организации по стандартизации перевели только две части британского стандарта BS 7799 из трех — это ГОСТ 17799 и ГОСТ 27001. Таким образом, имеется ГОСТ 27001, в котором заданы требования к СУИБ, и ГОСТ 17799, где имеются примеры по среде и системам ИБ, но нет руководства по оценке и управлению рисками. Вместе с тем именно в стандарте ISO 27005 представлено общее руководство по управлению рисками информационной безопасности. Он поддерживает общие концепции, изложенные в ISO/IEC 27001, и предназначен для «содействия адекватному обеспечению информационной безопасности на основе риск-ориентированного подхода». Риск информационной безопасности (Information security risk) определен в стандарте как потенциальная угроза эксплуатации уязвимости актива или группы ценных свойств, которые могут нанести вред организации. Стандарт применим ко всем видам организаций (в том числе и организациям, действующим в системе здравоохранения), планирующим управлять рисками информационной безопасности. Этот интернациональный стандарт обеспечивает рекомендации по управлению рисками информационной безопасности в организации, поддерживающей требования СМИБ (системы менеджмента информационной безопасности) согласно ISO/IEC 27001. Все действия менеджмента рисков информационной безопасности представлены как в разделе 6 стандарта, так и впоследствии описаны в следующих Разделах: установление состояния в Разделе 7, оценка риска в Разделе 8, обработка риска в Разделе 9, принятие риска в Разделе 10, перенос риска в Разделе 11, контроль и пересмотр рисков в Разделе 12. Порядок управления рисками по ISO 27005 представлен на рис. 1.

Рис. 1 иллюстрирует, что процессы менеджмента риска являются обычно цикличными для оценки риска и действиям по обработке рисков. Цикличный подход к проведению оценки риска может увеличить глубину и детали оценки при каждом новом цикле. Такой подход обеспечивает хорошее равновесие между уменьшением времени и усилием, гарантируя, что высокие риски оценены соответственно. В первую очередь устанавливается контекст рисков. После этого проводится оценка риска. Если предоставлено достаточно информации, чтобы определить эффективные действия, требуемые для изменения рисков до приемлемого уровня, тогда задача считается законченной и проводится обработка риска. Если информации будет недостаточно, то следует другой

цикл оценки риска с пересмотренным контекстом (например, критерии оценки риска). Эффективность обработки риска зависит от результатов оценки риска. Возможно, что обработка риска не будет немедленно приводить к приемлемому уровню остаточного риска. В этой ситуации другой цикл оценки риска с измененными контекстными параметрами (например, оценка риска, принятие риска или критерии воздействия), может в случае необходимости сопровождаться дальнейшей обработкой риска (рис. 1, вторая точка решения риска). Приемлемый уровень риска должен гарантировать, что остаточные риски приняты руководителями организации.

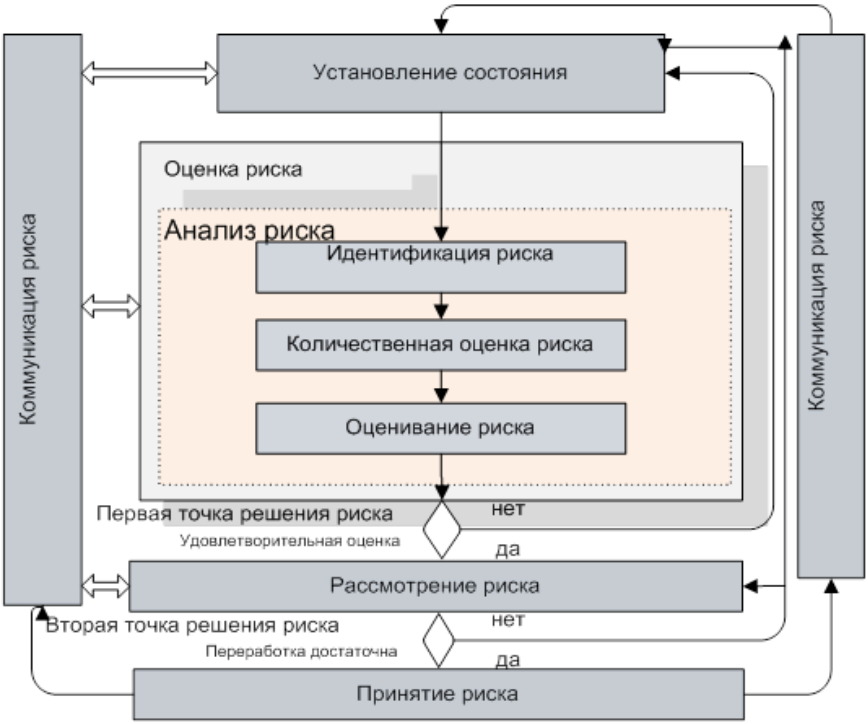

Рис. 1. Алгоритм управления рисками по ISO 27005 [3]

В СМИБ установление контекста, оценка риска, разработка плана обработки риска и принятие риска являются частью фазы «планирование».

В фазе «осуществление» СМИБ действия и средства контроля, требуемые для снижения риска до приемлемого уровня, реализуются в соответствии с планом обработки риска. Возможности современных

средств обеспечения ИБ очень широки: защита инфраструктуры организации, защита от атак, контроль поведения абонентов, защита периметра сети, мониторинг ИБ, защита от спама, отражение вирусов, применение политик, аутентификация почты, контроль приложений и аудит сетевой безопасности.

В фазе «проверка» СМИБ менеджеры определяют потребность в пересмотре обработки риска в свете инцидентов и изменений обстоятельств.

В фазе «действие» осуществляются любые необходимые работы, включая повторное инициирование процесса менеджмента риска ИБ. В таблице суммируются виды деятельности, связанной с менеджментом риска, значимые для четырех фаз процесса СМИБ.

Таблица 1

Соотношение СМИБ и процесса менеджмента рисков информационной безопасности

Процесс СМИБ	Процесс менеджмента рисков ИБ
Планирование	Установление контекста
	Оценка риска
	Планирование обработки риска
	Принятие риска
Осуществление	Реализация плана обработки риска
Проверка	Проведение непрерывного мониторинга и пересмотра рисков
Действие	Поддержка и усовершенствование процесса менеджмента рисков информационной безопасности

В общем виде деятельность по управлению рисками можно рассматривать в виде основных 7 этапов, представленных на рис. 2.

Для проведения полного анализа информационных рисков, прежде всего, необходимо построить полную модель информационной системы с точки зрения ИБ. Эту задачу должны выполнять высококвалифицированные специалисты, учитывая сложность алгоритма анализа рисков, включающего по меньшей мере около ста параметров, который позволяет на выходе дать максимально точную оценку существующих в информационной системе рисков, основанную на глубоком анализе особенностей информационной системы.

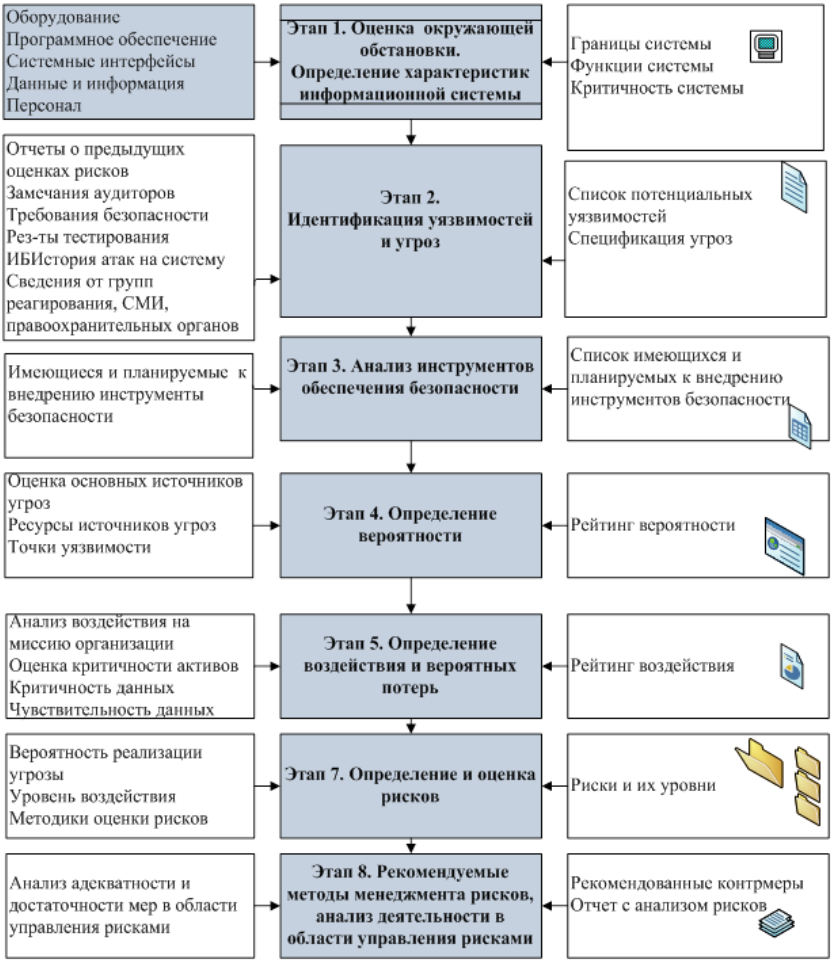

Рис 2. Этапы и структура управленческих воздействий в области управления рисками

Далее производится анализ угроз безопасности и уязвимостей. Исходные данные для оценки угроз и уязвимостей аудитор получает от уполномоченных представителей организации в ходе соответствующих интервью. Для проведения интервью используются специализированные опросники. Вопросы связаны с различными категориями ресурсов. Допускается корректировка вопросов, исключение или добавление новых. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффективности внедрения средств защиты. Необходи-

мо идентифицировать все виды информации, представляющей ценность для медицинской организации. Идентифицируются все активы, задействованные в функционировании бизнес-процессов и имеющие влияние на ценную для организации информацию. Данные активы включают:

- человеческие ресурсы;
- информационные ресурсы (как в электронном, так и в бумажном виде);
- оборудование;
- программное обеспечение;
- услуги, оказываемые внутренним и внешним заказчикам.

Введенные группы ценной информации должны быть размещены пользователем на объектах хранения информации (серверах, рабочих станциях и т. д.). Заключительная фаза — указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

Одним из значимых этапов является определение и оценка рисков (risk assessment) . В рамках анализа проводится инвентаризация и категоризация защищаемых ресурсов, выясняются нормативные, технические, договорные требования к ресурсам в сфере ИБ, а затем с учетом этих требований определяется стоимость ресурсов. В стоимость входят все потенциальные затраты, связанные с возможными воздействиями на защищаемые ресурсы. Следующим этапом анализа рисков является составление перечня значимых угроз и уязвимостей для каждого ресурса, а затем вычисляется вероятность их реализации. Стандарт допускает двоякое толкование понятия угрозы ИБ: как условие реализации уязвимости ресурса (в этом случае уязвимости и угрозы идентифицируются отдельно) и как общее потенциальное событие, способное привести к компрометации ресурса (когда наличие возможности реализации уязвимости и есть угроза). Не возбраняется разделение угроз ИБ на угрозы целостности, доступности и конфиденциальности.

Оценивание риска проводится путем его вычисления и сопоставления с заданной шкалой. Анализ риска может быть осуществлен с различной степенью детализации в зависимости от критичности активов, распространенности известных уязвимостей и прежних инцидентов, касавшихся организации. Методология измерения может быть качественной или количественной, или их комбинацией, в зависимости от обстоятельств. На практике качественная оценка часто используется первой для получения общих сведений об уровне риска и выявления основных значений рисков. Позднее может возникнуть необходимость в осуществлении более специфичного или количественного анализа основных значений рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и менее затратным.

В стандарте подробно описываются детали методологии оценки:

а) Качественная оценка использует шкалу квалификации атрибутов для описания величины возможных последствий (например, низкий, средний и высокий) и вероятности возникновения этих последствий. Преимущество качественной оценки заключается в простоте ее понимания всем соответствующим персоналом, а недостатком является зависимость от субъективного выбора шкалы.

Такие шкалы могут быть адаптированы или скорректированы таким образом, чтобы удовлетворять требованиям обстоятельств, а для разных рисков могут использоваться разные описания. Качественная оценка может использоваться:

- как начальная деятельность по тщательной проверке для идентификации рисков, требующих более детального анализа;
- там, где этот вид анализа является соответствующим для принятия решения;
- там, где числовые данные или ресурсы являются неадекватными для количественной оценки.

б) Количественная оценка использует шкалу с числовыми значениями (а не описательные шкалы, используемые в качественной оценке) последствий и вероятностей, включающую данные из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев количественная оценка использует фактические данные за прошлый период, обеспечивая преимущество в том, что она может быть напрямую связана с целями информационной безопасности и проблемами организации. Недостатки количественного подхода могут иметь место тогда, когда фактические проверяемые данные недоступны, поэтому создается иллюзия ценности и точности оценки риска.

BS 7799-3 допускает использование как количественных, так и качественных методов оценки рисков, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ. Приложение к стандарту содержит единственный пример, который условно можно отнести к качественному методу оценки. Данный пример использует трех- и пятибалльные оценочные шкалы:

1. Оцениваются уровни стоимости идентифицированного ресурса по пятибалльной шкале: «незначительный», «низкий», «средний», «высокий», «очень высокий».
2. Оцениваются уровни вероятности угрозы по трехбалльной шкале: «низкий», «средний», «высокий».
3. Оцениваются уровни вероятности уязвимости: «низкий», «средний», «высокий».
4. По заданной таблице рассчитываются уровни риска.

5. Проводится ранжирование инцидентов по уровню риска.

После того как риск оценен, должно быть принято решение относительно его обработки (risk treatment) — точнее, выбора и реализации мер и средств по минимизации риска. Помимо оцененного уровня риска, при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др. Предлагается одна из четырех мер обработки риска:

6. Уменьшение риска. Риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие меры и средства безопасности.

7. Передача риска. Риск считается неприемлемым и на определённых условиях (например, в рамках страхования, поставки или аутсорсинга) переадресуется сторонней организации.

8. Принятие риска. Риск в конкретном случае считается осознанно допустимым — организация должна смириться с возможными последствиями. Обычно это означает, что стоимость контрмер значительно превосходит финансовые потери в случае реализации угрозы либо организация не может найти подходящие меры и средства безопасности.

9. Отказ от риска. Отказ от бизнес-процессов организации, являющихся причиной риска. Например, отказ от электронных платежей по Сети.

В результате обработки риска остается так называемый остаточный риск, относительно которого принимается решение о завершении этапа обработки риска. Раздел 7 BS 7799-3 «Непрерывная деятельность по управлению рисками» затрагивает следующие две фазы менеджмента системы: контроль риска и оптимизация риска.

Для контроля риска рекомендуются технические меры (мониторинг, анализ системных журналов и выполнения проверок), анализ со стороны руководства, независимые внутренние аудиты ИБ.

Фаза оптимизации риска содержит переоценку риска и, соответственно, пересмотр политик, руководств по управлению рисками, корректировку и обновление механизмов безопасности. Процедуры контроля рисков и оптимизации — включая использование политик, мер и средств безопасности, идентификацию ресурсов, угроз и уязвимостей, документирование — гармонизированы с ISO 27001 и 27002.

В стандарте в качестве приложений приведены примеры оценки основных элементов оценки уязвимостей, угроз, рисков, приведен вариант методики количественной и качественной оценки рисков и др. Результатом работ по анализу рисков информационной безопасности, как правило, является:

- описание обследованных автоматизированных систем и сервисов, применяемых административных, организационных мер, программно-технических средств обеспечения ИБ;
- карта рисков информационной безопасности;
- план обработки рисков, который включает комплекс внедряемых административных, организационных мер и программно-технических средств, направленных на снижение уровня рисков информационной безопасности, оценку стоимости внедрения, а также график мероприятий по внедрению мер обеспечения ИБ (а в некоторых случаях полученные данные могут быть представлены в виде эскизного проекта реализации системы информационной безопасности ИС организации).

В конечном итоге решение о внедрении в систему новых инструментов и механизмов информационной безопасности и усовершенствовании имеющихся принимает руководство медицинской организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для деятельности. Использование международного стандарта ISO/IEC 27005:2011 позволяет руководству организовать данную деятельность на системной основе и защитить организацию от потери каких-либо ресурсов, а самое главное — потери деловой репутации.

Термины и определения

Риск — комбинация вероятности события и его последствий.

Управление риском (Risk Management) — скоординированные действия по управлению и контролю организации в отношении риска. Обычно включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске.

Оценка риска (Risk Assessment) — общий процесс анализа и оценивания риска.

Анализ риска (Risk Analysis) — систематическое использование информации для идентификации источников и оценки величины риска.

Оценивание риска (Risk Evaluation) — процесс сравнения оценочной величины риска с установленным критерием риска с целью определения уровня значимости риска.

Обработка риска (Risk Treatment) — процесс выбора и реализации мер по модификации риска. Меры по обработке риска могут включать в себя избежание, оптимизацию, передачу или сохранение риска.

Список литературы

1. Марков А. С., Цирлов В. Л. Управление рисками — нормативный вакуум / А. С. Марков, В. Л. Цирлов // Открытые системы. СУБД. — 2007. — №8. — с. 63-67.

2. URL: http://www.itsec.ru/articles2/pravo/o_vnedreniya_17799

3. URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742.