

Раздел IV. Биотехнологии и медицинские информационные системы

УДК 681.3

Ю.М. Брумштейн, О.В. Сивер

АНАЛИЗ ФАКТОРОВ, МЕТОДОВ И МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ В ПРОЦЕССЕ ЖИЗНЕННОГО ЦИКЛА МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ*

Указаны особенности основных этапов жизненного цикла различных типов медицинских информационных систем (МИС), причины прекращения их эксплуатации. Рассмотрены риски, связанные с приобретением и использованием «встроенного» программного обеспечения отдельных единиц медицинского оборудования, обеспечением взаимосвязей этого оборудования с МИС масштаба медицинских учреждений. (МУ). Проанализированы принципы принятия решений о приобретении «готовой» или создании «собственной» МИС для МУ; состав лиц/организаций, принимающих и реализующих такие решения; источники и схемы (порядок) финансирования работ по покупке (созданию) и внедрению МИС. Подробно проанализирована структура рисков МУ для решений, связанных с самостоятельной разработкой и модернизацией МИС – с использованием собственных сотрудников и внешних организаций (аутсорсинг). Показано влияние конкуренции между разработчиками МИС на риски их создания и внедрения. Для различных типов МУ оценены риски, связанные с этапами внедрения МИС, их эксплуатации, прекращения использования. Рассмотрена организационная и технико-экономическая эффективность мер, направленных на уменьшение рисков.

Медицинские информационные системы; риски; разработка; эксплуатация; жизненный цикл.

Yu.M. Brumsteyn, O.V. Siver

SYSTEM ANALYSIS OF RISKS IN PROCESS OF MEDICAL INFORMATION SYSTEMS LIFE CYCLE

There are specified features of life cycle main stages various types of the medical information systems (MIS), the reasons of their operation termination. The risks, connected with acquisition and usage of the «built-in» software in separate units of medical equipment, by ensuring interrelations this equipment with MIS of medical institutions (MU) scale are considered. The principles of decision-making on acquisition «ready» or creation of «own» MIS for MU; structure of persons/organizations making and realizing such decisions; sources and schemes (order) of financing works on purchase (creation) and their MIS introduction are analyzed. The structure of MU risks for decisions, connected with independent development and MIS modernization - with use own employees and the external organizations (outsourcing) is analyzed in detail. Competition influence between MIS developers on risks of their creation and introduction is shown. For the various MU types are estimated the risks, connected with stages of MIS introduction, their operation, usage termination. Organizational, technical and economic efficiency of the measures, directed on risk reduction is considered.

Medical information systems; risks; development; operation; life cycle.

* Исследование выполнено при финансовой поддержке РФФИ (грант № 14-06-00279.)

Введение. Различным вопросам разработки и эксплуатации медицинских информационных систем (МИС) для медицинских учреждений (МУ) посвящено достаточно много работ (например, [1, 2, 3]). Однако вопросы, касающиеся управления рисками МИС в процессе их жизненного цикла (от принятия решения о приобретении/создании до прекращения эксплуатации) исследованы недостаточно полно. Поэтому в настоящей статье ставилась **цель** выполнить системный анализ этой проблематики и определить целесообразные приемы управления рисками в условиях неопределенности информации; различных видов ограничений.

Описание проблемы и методы решения. Термин «риск» (R_i) для i -го возможного неблагоприятного события (НС) ниже будем понимать как произведение вероятности его возникновения/реализации (P_i) на ущерб от реализации этого события (U_i):

$$R_i = P_i U_i. \quad (1)$$

В простейшем случае риски от отдельных НС ($i=1 \dots I$) в рамках оценки общего риска (R^*) предполагаются суммируемыми

$$R^* = N \sum_{i=1}^I R_i, \quad (2)$$

где I – общее количество видов НС; N – количество «периодов времени», для каждого из которых даются оценки рисков по формуле (1). Предполагается, что i -е НС может независимо реализовываться в каждом из N периодов. Учет эффектов «взаимодействия» рисков приводит к увеличению ущербов при сочетаниях НС.

$$R^{**} = N \left(\sum_{i=1}^I R_i + \sum_{i=1}^I \sum_{j=1(j \neq i)}^I P_i P_j U_{i,j}^* \right), \quad (3)$$

где $U_{i,j}^*$ – дополнительный ущерб от одновременной реализации в течение одного периода времени НС видов i и j . Использование МИС в МУ позволяет снизить ряд видов рисков для них, однако и сами процессы разработки, внедрения и эксплуатации МИС сопровождаются различными видами рисков.

Эффективность затрат на приобретение, внедрение, эксплуатацию МИС определяется такими факторами: улучшение здоровья населения, возможностей использования его интеллектуального потенциала, трудоспособности; улучшением доступности и качества предлагаемых медицинских услуг и, как следствие, сохранением «лояльности» пациентов к МУ, привлечением новых клиентов; повышением эффективности работы персонала МУ, особенно высококвалифицированного; снижением нерациональных затрат рабочего времени на обработку информации; улучшением информационно-аналитической поддержки деятельности персонала; сокращением трудозатрат на получение медико-статистической отчетности и др.

В общем случае основными «направлениями» (объектами и субъектами) рисков, связанных с МИС, можно считать следующие: пациентов; медперсонал МУ; оборудование (прежде всего, компьютерное); каналы связи между компьютерным оборудованием; программное обеспечение (ПО) – специальное и общесистемное; сроки реализации работ в отношении разработки МИС и выполнения действий по ее использованию; качество выполнения работ и пр.

Для самих рисков их типология определяется, обычно, таким списком: кадровые риски; финансовые; юридические, организационные; инженерно-технические (техногенные); природные, нормативные, политические и пр.

В общем случае «контроль и управление рисками», связанными с МИС включает в себя такие компоненты: выявление общей структуры рисков; определение причин и источников рисков; анализ и оценка рисков (минимально – качественная); определение возможностей управления рисками; разработка и реализация мер по снижению рисков; анализ и оценка действий персонала по снижению рисков или их предотвращению – в т.ч. в рамках мер по «управлению качеством».

Важно отметить, что сейчас, как правило, решение об использовании (или модернизации) МИС в МУ принимается в условиях, когда какие-то «средства информатизации» уже применяются – это могут быть как полнофункциональные МИС, так и их отдельные подсистемы. Поэтому, в общем случае, выбор в отношении МИС возможен из числа следующих альтернатив: продолжение эксплуатации существующего ПО; модернизация уже эксплуатируемых разработок; создание программных «надстроек» обеспечивающих необходимую функциональность; разработка надстроек, позволяющих обеспечить для МИС «интерфейсы» с другими МИС, в т.ч. эксплуатируемыми вне МУ; прекращение эксплуатации существующих МИС и замена их другими разработками. В случае, если решение принимается для комплексной МИС (КМИС) региона, существует еще вариант разработки «стандартов и протоколов», потенциально обеспечивающих возможности «интеграции» [3] существующих (уже эксплуатируемых) разработок.

Выбор из этих альтернатив обычно осуществляется в условиях неопределенностей и рисков. Этот выбор могут осуществлять руководители отдельных МУ (прежде всего коммерческих); руководство органов управления здравоохранением регионов или ведомств и пр. Для снижения рисков неверных (неоптимальных) решений к процессам выбора могут подключать независимых экспертов.

Считается, что существует три основных подхода к созданию МИС.

(А) Закупка и внедрение «готовой» КМИС – возможно с некоторой ее адаптацией для конкретного МУ или региона [1, 2].

Для бюджетных МУ (и регионов) приобретение МИС по существующим правилам должно осуществляться с использованием «тендеров». Неточные или неполные формулировки в тендерной документации, а также малая известность информации об объявленных тендерах также должны рассматриваться как риски принятия не оптимальных решений по выбору поставщиков МИС.

При принятии решения учитываются такие факторы: стоимости предлагаемых МИС (поставки, услуги по внедрению; сопровождение в процессе эксплуатации); функциональность разработки [4]; возможности доработок МИС в процессе эксплуатации; масштабируемость МИС; требования к аппаратным средствам и ПО; требования к квалификации эксплуатантов МИС; длительность присутствия фирмы-разработчика МИС «на рынке»; количество успешных внедрений ею МИС; отзывы о надежности эксплуатации МИС (в т.ч. и в Интернете) и др.

Выбор в пользу достаточно крупных фирм-разработчиков, долгое время работающих на рынке, обуславливается снижением рисков того, что они «уйдут с рынка» в процессе эксплуатации МИС в МУ или в регионе [2]. При этом может быть утрачена возможность каких-либо доработок МИС, которые могут потребоваться по ходу их эксплуатации. Кроме того, крупные фирмы-разработчики обычно предлагают продукты со значительным опытом эксплуатации – это снижает риски наличия в МИС «неисправленных» ошибок.

В принципе возможна ориентация МУ (или регионов) и на «заказные МИС» (индивидуальные разработки). Однако при этом выше следующие виды рисков: не

выявленные ошибки в ПО – так как нет опыта массовой эксплуатации разработки; срыв плановых сроков разработки; недостаточно отработанная эксплуатационная документация для МИС; увольнение из фирм ключевых специалистов-разработчиков, в том числе и с переездом их на работу за рубеж; изменение требований к ПО в процессе выполнения разработки – в том числе исходя из новых требований нормативных документов, вышестоящих организаций и пр. Однако «заказные разработки» позволяют лучше (по сравнению с адаптацией существующего ПО) учесть особенности конкретного МУ или региона.

В случае «заказных» МИС для снижения рисков как «разработчика», так и «заказчика» применяются следующие меры: поэтапное финансирование работ, обычно исходя из принципа «достижения фиксированных рубежей»; страхование «профессиональных рисков» разработчиков в страховых фирмах и пр.

Основные недостатки подхода «А» следующие: обычно невозможность подключения к КМИС подсистем других разработчиков, предназначенных для решения специальных задач (как следствие возникает риск того, что поставщик КМИС сможет назначать «монопольные» цены на дополнительные разработки); сложности с синхронным внедрением подсистем КМИС в МУ или регионе; зависимость от «поддержки» разработчика при появлении новых операционных систем, другого общесистемного ПО, офисных программ.

(Б) Поэтапное внедрение покупных МИС (или их подсистем), обеспечивающих автоматизацию отдельных бизнес-процессов; их системная интеграция [3] на основе единых стандартов внутриучрежденческого обмена данными. Основные риски для этого варианта: программная несовместимость подсистем различных разработчиков МИС, а также встроенного ПО медоборудования и МИС; отказ фирмы-разработчика от ранее запланированного создания каких-то подсистем МИС (например, из-за малого спроса на них).

Преимущества варианта «Б» (по сравнению с «А») – снижение рисков, связанных с такими факторами: неполной совместимостью подсистем МИС друг с другом (они могут быть своевременно выявлены и, в ряде случаев, скорректированы); перегрузкой квалифицированного персонала на этапе внедрения и пр.

(В) Самостоятельная [1] (обычно – силами сотрудников МУ) поэтапная разработка и внедрение модулей МИС в МУ. При этом снижаются риски неполной адаптации (подгонки) МИС под требования конкретного МУ; значительно лучше «управляемость» разработчиков, т.к. это, обычно, штатные сотрудники МУ; выше «скорость реакции» на выявившиеся недочеты в разработках МИС и пр.

Недостатки варианта «В» связаны со следующими видами рисков: неверный выбор «платформы разработки», который может в последующем повлечь ограничения функциональности МИС, недостаточную скорость ее работы и пр.; увольнение ключевых разработчиков до завершения создания МИС (при этом ранее сделанная работа может оказаться просто «обесцененной»); увольнение после завершения разработки (при этом часто теряется возможность дальнейшего развития МИС); неверная оценка стоимости и/или продолжительности разработки МИС или их отдельных подсистем (особенно при отсутствии возможностей полноценно проанализировать опыт создания аналогичных разработок); неверный выбор приоритетов при разработке подсистем МИС в условиях ограниченных ресурсов разработчиков; неправильный выбор «соглашений об информационных связях» между разрабатываемыми подсистемами МИС (в последующем это может привести к необходимости переработки ПО, повторения процедур его тестирования и пр.); изменение в процессе создания МИС требований руководства МУ или вышестоящих организаций к функциональности МИС, ее надежности; принятие решений на «вышестоящем уровне» о внедрении в регионах «унифицированных» МИС; нали-

чие не выявленных ошибок в разработанных МИС, связанных с отсутствием опыта их массовой эксплуатации; относительно низкое (по сравнению с тиражируемыми МИС) отношение «результаты/затраты» и пр.

Отметим, что МУ (особенно бюджетные) часто не могут обеспечить ИТ-специалистам (включая разработчиков), конкурентоспособные зарплаты по сравнению с банковской сферой, крупными промышленными предприятиями и пр. – это приводит к «текучести» кадров. С другой стороны наем «внешних» специалистов (по договорам) обычно снижает «управляемость» коллективов разработчиков со стороны руководства МУ или его профильного ИТ-подразделения.

Основными этапами «жизненного цикла» любых информационных систем считаются следующие: (1) выявление (оценка) целесообразности использования МИС в МУ; (2) оценка необходимой функциональности МИС; (3) принятие решения о необходимости использования МИС в МУ и сроках ее внедрения; (4) выбор между закупкой «готовой» МИС или ее самостоятельной разработкой, выбор поставщика готовой МИС – если выбрана закупка; (5) внедрение МИС; (6) эксплуатация МИС; (7) прекращение эксплуатации МИС. На всех этих этапах существуют определенные риски – как «управляемые» со стороны руководства МУ, так и не зависящие от их действий. Рассмотрим риски по этапам более подробно.

При выявлении целесообразности использования МИС в МУ (или модернизации существующей системы) учитываются следующие факторы: требования нормативных документов и вышестоящих инстанций (организаций); объективные потребности МУ в МИС с различной функциональностью; уровень «компьютерной квалификации» персонала; располагаемые финансовые ресурсы; имеющееся компьютерное оборудование, общесистемное ПО; перспективы развития аппаратно-программных средств в сфере информационных технологий; опыт внедрения/использования МИС в аналогичных организациях; вероятность и предполагаемые сроки того, что для бюджетных организаций будет осуществляться внедрение «унифицированных» МИС в централизованном порядке и пр.

В отношении всех этих факторов неточности оценок обуславливают риски принятия не оптимальных (как минимум!) решений. Снижение уровней этих рисков может быть обеспечено за счет следующих действий: тщательный анализ опыта работы других МУ; сбор информации о перспективах внедрения «унифицированных» МИС в других регионах по всем возможным источникам и пр.

«Откладывание» решения в отношении внедрения новой МИС или модернизации существующей также может рассматриваться как способ риск-менеджмента. В частности переход на новую МИС обычно не планируется на конец календарного года, когда необходима подготовка отчетных материалов по деятельности МУ.

Оценка необходимой функциональности МИС может определяться требованиями нормативных документов; мнениями сотрудников МУ; перспективами его деятельности, включая увеличение количества пациентов, изменение профиля Работы и пр. Риски, связанные с определением функциональности МИС могут быть снижены за счет привлечения «экспертов» (консультантов) извне МУ; изучения опыта работы с МИС аналогичных МУ и пр.

Принятие решения о необходимости использования МИС в МУ обычно требует документального оформления, влечет за собой ряд мер организационного, инженерно-технического, финансового и др. характера. Сама по себе совокупность работ, соответствующих закупке (или разработке) МИС и ее внедрению может рассматриваться как «проект». В качестве этапа проекта может выступать и «эксплуатация» МИС – если хотя бы приблизительно можно оценить ее продолжительность (учетом длительностей жизненного цикла аналогичных МИС и иных факторов). Ошибочные оценки стоимости разработки МИС; трудоемкости и продолжительности ее внедрения; вероятной продолжительности эксплуатации МИС;

баланса между «положительными» и «отрицательными» эффектами от внедрения новой МИС (или модернизации существующей) и продолжения эксплуатации существующей МИС [5] являются факторами риска для принимаемых решений.

Выбор между приобретением «готовой» МИС или ее самостоятельной разработкой актуален преимущественно либо для «уникальных» бюджетных МУ (например, связанных с оказанием специализированных видов высокотехнологичной медицинской помощи), либо для коммерческих МУ. В то же время бюджетные МУ (особенно небольшие) сейчас, обычно, вообще не могут принимать самостоятельные решения в отношении приобретения/использования МИС – такие решения принимает вышестоящее руководство.

Этап внедрения МИС принято делить на такие подэтапы: опробование МИС в МУ; опытная эксплуатация МИС; опытно-рабочая эксплуатация. Затем следует переход на этап рабочей «эксплуатации».

Основные риски для этапа внедрения МИС: неверная оценка необходимой функциональности МИС на предыдущих этапах; неправильная оценка трудоемкости работ по внедрению МИС, сроков таких работ; неполное выявление ошибок и недочетов МИС на этапе внедрения; «сопротивление» персонала МУ внедрению МИС – в том числе по психологическим причинам, из-за нежелания «переучиваться»; недостаток компьютерной квалификации эксплуатантов и системных администраторов, специалистов по информационной безопасности в МУ; неправильная оценка существующих «мощностей» имеющегося компьютерного оборудования, пропускной способности локальной компьютерной сети и иных сетей; различия в трактовке терминологии со стороны сотрудников МУ и разработчиков МИС; выявление недостаточной эксплуатационной надежности МИС – в том числе в условиях некачественного электропитания, перерывов в электроснабжении и пр.

На этапе эксплуатации для МУ наиболее актуальны следующие риски: угрозы информационной безопасности МИС в том числе связанные с разрушением баз данных (БД) – эти риски обычно уменьшают за счет систематического резервного копирования БД, использования RAID-массивов и пр.; нарушением нормативных требований в отношении обеспечения безопасности персональных данных пациентов [6, 7, 8]; значительное превышение запланированных ранее расходов на эксплуатацию МИС (особенно – в отношении «заказных разработок»); неумышленными ошибками эксплуатантов МИС (в этом случае могут быть полезны специальные подсистемы контроля их действий [9]); внесением в МИС неполной, искаженной или ошибочной информации (средства автоматизации контроля вносимых данных могут выявить лишь часть таких ошибок); появлением необходимости наращивания (модернизации) функциональности МИС – в том числе из-за изменений условий деятельности МУ (включая нормативные требования), появлением дополнительных требований со стороны руководства органов управления здравоохранением региона и пр.; сменой руководства МУ или региона (новое руководство может предъявить новые требования); появлением требований со стороны вышестоящей организации о переходе на «унифицированные» КМИС (например, в масштабе региона); неработоспособности (несовместимости) МИС с вновь появляющимися операционными системами, другим общесистемным ПО; внесение разработчиками поправок в МИС без их последующего тестирования на работоспособность (практика показывает, что при таких изменениях возможны «побочные эффекты», в т.ч. такие, которые выявляются не сразу) [10].

Повторим, что увольнение штатных разработчиков МИС (или их подсистем) из МУ часто приводит к «блокированию» возможностей дальнейшего развития эксплуатируемых МИС, а иногда и к невозможности их полноценной эксплуатации. Основные причины такого положения: чаще всего ПО МИС пишется без дос-

таточного количества комментариев, которые дали бы возможность разобраться в логике программы другим программистам; «интерфейсы» между отдельными модулями МИС часто оказываются документированными в недостаточной степени и др. При этом, как правило, программисты-разработчики, нашедшие себе новое место работы с лучшими условиями, обычно не склонны сотрудничать с «прежним работодателем» (МУ) на договорных условиях – из-за нехватки времени, по соображениям экономической невыгодности и пр.

В то же время увольнение «системных администраторов» в МУ обычно не является критичным в отношении продолжения эксплуатации МИС.

При прекращении эксплуатации МИС также возможны определенные риски: меньшая функциональность новых программных разработок по сравнению с теми, которые снимаются с эксплуатации; наличие «программных надстроек» к снимаемой с эксплуатации МИС, которые не могут работать «автономно»; проблемы при конвертировании накопленных БД для использования их в новой МИС; необходимость некоторое время эксплуатировать старую и новую МИС «параллельно» – что может приводить к различиям во введенных данных и пр.

Рассмотрим математическую модель оптимального выбора набора решений (НР) по управлению рисками (УР), в которой необходимые значения коэффициентов могут быть определены по нормативным документам, существующим расценкам или экспертно. Примем, что возможны «М» НР по УР. Для каждого из них величины снижения отдельных видов рисков для одного периода времени определяются матрицей $[Q_{i,m}]_{i=1..I;m=1..M}$, а объемы ресурсов, используемых для УР – матрицей $[S_{k,m}]_{k=1..K;m=1..M}$, где K – количество видов ресурсов, которые можно использовать. Затраты на использование ресурсов задаются матрицей $[Z_{k,m}]_{k=1..K;m=1..M}$. Ее элементы можно вычислить по формуле

$$Z_{k,m} = a_k S_{k,m}, \quad (4)$$

где a_k – затраты на использование единицы k -ого ресурса. Тогда затраты, соответствующие M вариантам НР – это вектор $\{\omega_m\}_{m=1..M}$, где

$$\omega_m = \sum_{k=1}^K Z_{k,m}. \quad (5)$$

Оптимальное решение по УР будет соответствовать

$$\max_m \{E_m - \omega_m\}. \quad (6)$$

где E_m – положительный эффект от снижения рисков по m -му варианту НР

$$E_m = \sum_{i=1}^I Q_{i,m}. \quad (7)$$

Для (6) должны выполняться ограничения по отдельным ресурсам $\{S_k^*\}_{k=1..K}$ и суммарным затратам (Ω)

$$\{S_{k,m} \leq S_k^*\}_{k=1..K}; \omega_m \leq \Omega. \quad (8)$$

Заключение. Итак, сделаем **выводы**. 1) риски существуют на всех этапах жизненного цикла МИС – от начала их создания, до прекращения эксплуатации; 2) целесообразно различать риски МИС, связанные с деятельностью их разработчиков, эксплуатантов, пациентов; органов управления здравоохранением; 3) Для этих групп

юридических лиц возможны различные меры по управлению рисками, в том числе в условиях как совпадающих, так и различающихся интересов сторон; 4) при принятии решений, связанных с внедрением МИС риски могут быть значительно снижены за счет объективного анализа опыта, накопленного другими МУ при эксплуатации МИС; 5) эксплуатационные риски МИС могут быть уменьшены за счет рационального распределения усилий (и финансовых средств) для борьбы с различными видами внутренних и внешних угроз. Принятие соответствующих решений должно включать в себя динамическое накопление информации об угрозах и анализ этой информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Борисов А.Г.* МИС: промышленное решение или внутренняя разработка // *Врач и информационные технологии.* – 2009. – № 3. – С. 49-53.
2. *Брумштейн Ю.М., Чернов С.В.* Анализ вопросов обеспечения информационной безопасности МИС в учреждениях, оказывающих высокотехнологичную медицинскую помощь // *Известия ЮФУ. Технические науки.* – 2010. – № 9 (110). – С. 179-184.
3. *Брумштейн Ю.М., Захаров Д.А., Акишкин В.Г.* Риски информационной безопасности медучреждений, их специалистов и пациентов // *Информационная безопасность регионов.* – 2013. – № 1. – С. 13-21.
4. *Брумштейн Ю.М., Тарков Д.А., Дюдиков И.А.* Анализ моделей и методов выбора оптимальных совокупностей решений для задач планирования в условиях ресурсных ограничений и рисков // *Прикаспийский журнал: управление и высокие технологии.* – 2013. – № 3. – С. 169-179.
5. *Гусев А.В.* Обзор рынка комплексных медицинских информационных систем // *Врач и информационные технологии.* – 2009. – № 6. – С. 4-17.
6. *Князюк Н.Ф., Кицул И.С.* Проектирование системы менеджмента рисков информационной безопасности на основе требований международного стандарта ISO/IEC 27005:2011 // *Врач и информационные технологии.* – 2012. – № 1. – С. 39-47.
7. *Козадой Ю.В.* Исследование типовых процессов интеграции в медицинских информационных системах // *Программные продукты и системы.* – 2009. – № 2. – С. 55.
8. *Космачева И.М.* Анализ проблемы эффективной организации контроля за действиями пользователей в медицинских информационных системах // *Вестник Астраханского государственного технического университета.* – 2008. – № 1. – С. 74-76.
9. *Мухин Ю.Ю., Лебедев Г.С.* Подходы к параметрической оценке и сопоставлению функций медицинских информационных систем // *Информационно-измерительные и управляющие системы.* – 2013. – Т. 11, № 10. – С. 19-30.
10. *Пономарева М.Г.* Вопросы информационной безопасности при модернизации медицинских информационных систем // *Научные труды Вольного экономического общества России.* – 2013. – Т. 179. – С. 617-623.

REFERENCES

1. *Borisov A.G.* MIS: promyshlennoe reshenie ili vnutrennyaya razrabotka [MIS: industrial solution or internal development], *Vrach i informatsionnye tekhnologii* [The doctor and information technology], 2009, No. 3, pp. 49-53.
2. *Brumshteyn Yu.M., Chernov S.V.* Analiz voprosov obespecheniya informatsionnoy bezopasnosti MIS v uchrezhdeniyakh, okazyvayushchikh vysokotekhnologichnuyu meditsinskuyu pomoshch' [The analysis of information safety MIS maintenance questions in the establishments, rendering hi-tech medical aid], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2010, No. 9 (110), pp. 179-184.
3. *Brumshteyn Yu.M., Zakharov D.A., Akishkin V.G.* Riski informatsionnoy bezopasnosti meduchrezhdeniy, ikh spetsialistov i patsientov [The information security risks of hospitals, specialists and patients], *Informatsionnaya bezopasnost' regionov* [Information security regions], 2013, No. 1, pp. 13-21.
4. *Brumshteyn Yu.M., Tarkov D.A., Dyudikov I.A.* Analiz modeley i metodov vybora optimal'nykh sovokupnostey resheniy dlya zadach planirovaniya v usloviyakh resursnykh ogranicheniy i riskov [Information security regions], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian journal: management and technology], 2013, No. 3, pp. 169-179.

5. Gusev A.V. Obzor rynka kompleksnykh meditsinskikh informatsionnykh sistem [Market review complex medical information systems], *Vrach i informatsionnye tekhnologii* [The doctor and information technology], 2009, No. 6, pp. 4-17.
6. Knyazyuk N.F., Kitsul I.S. Proektirovanie sistemy menedzhmenta riskov informatsionnoy bezopasnosti na osnove trebovaniy mezhdunarodnogo standarta ISO/IEC 27005:2011 [Design management system information security risks based on the requirements of international standard ISO/IEC 27005:2011], *Vrach i informatsionnye tekhnologii* [The doctor and information technology], 2012, No. 1, pp. 39-47.
7. Kozadov Yu.V. Issledovanie tipovykh protsessov integratsii v meditsinskikh informatsionnykh sistemakh [Study of typical processes of integration in health information systems], *Programmnye produkty i sistemy* [Software products and systems], 2009, No. 2, pp. 55.
8. Kosmacheva I.M. Analiz problemy effektivnoy organizatsii kontrolya za deystviyami pol'zovateley v meditsinskikh informatsionnykh sistemakh [The analysis of the problem of effective control over the actions of users in medical information systems], *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta* [Vestnik of Astrakhan state technical University], 2008, No. 1, pp. 74-76.
9. Mukhin Yu.Yu., Lebedev G.S. Podkhody k parametricheskoy otsenke i sopostavleniyu funktsiy meditsinskikh informatsionnykh sistem [Approaches to parametric evaluation and comparison of functions of the medical information systems], *Informatsionno-izmeritel'nye i upravlyayushchie sistemy* [Information-measuring and control systems], 2013, Vol. 11, No. 10, pp. 19-30.
10. Ponomareva M.G. Voprosy informatsionnoy bezopasnosti pri modernizatsii meditsinskikh informatsionnykh sistem [Information security issues when upgrading health information systems], *Nauchnye trudy Vol'nogo ekonomicheskogo obshchestva Rossii* [Scientific works of the Free economic society of Russia], 2013, Vol. 179, pp. 617-623.

Статью рекомендовал к опубликованию д.т.н. Г.А. Попов.

Брумштейн Юрий Моисеевич – Астраханский государственный университет; e-mail: brum2003@mail.ru; 414040, г. Астрахань, пл. Карла Маркса, 21, кв. 34; тел.: 88512610843; кафедра управления качеством; к.т.н.; доцент.

Сивер Ольга Викторовна – e-mail: s_o_v69@mail.ru; 414057, г. Астрахань, ул. Кубанская, 5; тел.: 88512777588; магистрантка; начальник информационно-аналитического отдела НУЗ «МСЧ».

Brumshteyn Uuri Moiseevich – Astrakhan State University; e-mail: brum2003@mail.ru; 21, Square Karla Marksa, fl. 34, Astrakhan, 414040, Russia; phone: +78512610843; the department of quality control; cand. of eng. sc.; associate professor.

Siver Olga Viktorovna – e-mail: s_o_v69@mail.ru; 5, Kubanskaya street, Astrakhan, 414057, Russia; phone: +78512777588; magistrant; head of information and analysis department of NUZ "MSCh" (Astrakhan).

УДК 615.471:616-073.97:616.831:681.3.06

В.Ю. Вишневецкий, Т.П. Строчан

ВЫБОР МЕТОДА ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТА ДЛЯ ПЬЕЗОКВАРЦЕВОГО БИОСЕНСОРА

Автоматические методы химического анализа, тесно связаны со средствами аналитической и микропроцессорной техники. Приборы должны быть пригодны для автоматического выполнения важнейших стадий аналитического определения, в том числе и для большого объема измерений. Биосенсоры, представляют собой комбинацию селективного биохимического элемента с электронным датчиком, позволяют провести анализ воды в режиме реального времени и обнаружить различные загрязнители и их смеси, исключают