ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2220-6469-2020-14-3-44-53
УДК 336.7(045)
JEL G21, L86, M15

Риски развития информационных технологий в банковском секторе

Н.Э. Соколинская[a], **Л.М. Куприянова**[b]
[a, b] Финансовый университет, Москва, Россия
[a] https://orcid.org/0000-0002-4731-722x; [b] https://orcid.org/0000-0002-9453-6425

АННОТАЦИЯ

Актуальность статьи обусловлена тем, что параллельно с процессами внедрения инноваций в сфере автоматизации и компьютеризации банковской системы возрастает количество видов банковских рисков, связанных с инновациями в сфере обслуживания клиентов онлайн и составления внутрибанковской отчетности, а также работы информационных систем. В процессе написания статьи были изучены последние законодательные акты Центрального банка России и обобщена практика отдельных кредитных организаций и банковского сектора в области рисков развития информационных технологий. Авторы отмечают, что в целях развития финансовых технологий в условиях цифровой экономики необходимо обсуждать появление новаций, а также рассмотреть возможность дальнейшего анализа имеющихся методических разработок с целью обмена передовым опытом. Построение эффективной системы управления рисками IT-безопасности — не одноразовый проект, важен комплексный процесс, ориентированный на минимизацию внешних и внутренних угроз, и учет ограничений на ресурсы и фактор времени.

Ключевые слова: финансовые технологии; хакерские риски; риски информационной безопасности; методы оценки рисков; организационная и правовая структура управления банковскими рисками; стандарт управления рисками информационной безопасности

Для цитирования: **Соколинская Н.Э., Куприянова Л.М. Риски развития информационных технологий в банковском секторе. *Мир новой экономики*. 2020;14(3):44-53. DOI: 10.26794/2220-6469-2020-14-3-44-53**

ORIGINAL PAPER

Information Technology Development Risks in the Banking Sector

N.E. Sokolinskaya[a], **L.M. Kupriyanova**[b]
[a, b] Financial University, Moscow, Russia
[a] https://orcid.org/0000-0002-4731-722x; [b] https://orcid.org/0000-0002-9453-6425

ABSTRACT

The relevance of the article is because in parallel with the processes of introduction of innovations in the field of automation and computerization of the banking system, the number of types of banking risks associated with innovations in the field of on-line customer service and internal Bank reporting, as well as information systems. As a result of this article, we have studied the latest legislative acts of the Central Bank of Russia as a mega-regulator and summarized the practice of both individual credit institutions and the banking sector in the field of information technology development risks in the banking sector. To strengthen the development of new financial technologies in the digital economy, it is necessary to regularly discuss the emergence of new phenomena and innovations; to consider the possibility of further analysis of existing methodological developments to exchange best practices of banks. Building an effective it security risk management system is not a one-time project. Still, a complex process is important, focused on minimizing external and internal threats and taking into account the limitations on resources and time factor.

Keywords: financial technologies; hacker risks; information security risks; risk assessment methods; organizational and legal structure of Bank risk management; a standard of information security risk management

For citation: **Sokolinskaya N.E., Kupriyanova L.M. Information technology development risks in the banking sector. *Mir novoi ekonomiki = The World of the New Economy*. 2020;14(3):44-53. DOI: 10.26794/2220-6469-2020-14-3-44-53**

В условиях развития современных информационных технологий важное место занимает интеллектуальная собственность. Поэтому появляются риски, препятствующие распространению инноваций, сопровождающие процесс внедрения результатов интеллектуальной деятельности в жизнь общества.

Банковский сектор является первым после военно-оборонного комплекса страны, внедрившим новые цифровые продукты, технологии, сервисы и информацию. В рамках стратегии инновационного развития и для поддержания конкуренции в банковском секторе кредитные организации регулярно разрабатывают новые инновационные продукты, процессы и технологии, а также совершенствуют уже существующие. Глобализация и интеграция в области интеллектуальной деятельности способствуют развитию и модернизации банковской системы России в целом, что, с одной стороны, отражается на функциональности и расширении возможных перспектив для дальнейшего развития кредитных организаций, а с другой — постоянно требует поисков путей минимизации возникающих рисков информационной безопасности (ИБ) коммерческих банков, связанной с развитием финтеха.

ИБ является одним из главных элементов совершенствования финтеха в банках, так как в кредитных организациях содержится много важной информации, в том числе касательно физических и юридических лиц, которая может оказаться у мошенников (хакеров, киберпреступников), что грозит банкам банкротством и потерей клиентов, а в масштабном плане — разрушением финансовой системы внутри страны.

Исследования показывают, что утечка 20% информации, которая является коммерческой тайной, как правило, приводит к разорению кредитной организации. Поэтому необходимо обеспечивать безопасность хранения данных, а также проводить контроль вероятности утечки информации.

Принципиально важны на этом этапе развития финтеха (особенно в банковской сфере) классификация рисков иформационной безопасности, методы оценки рисков информационной безопасности, организационная структура и принципы управления рисками ИБ, правовая основа и внутренние документы по рискам информационной безопасности, а также способы управления рисками и их минимизация.

Рассмотрим эти вопросы подробнее.

1. *Классификация рисков информационной безопасности*. Учитывая, что ежедневно банки осуществляют переводы в больших объемах (около 2 трлн долл.), важно обеспечивать их информационную безопасность. Иначе это может повлечь за собой финансовые потери и навредит имиджу банка (*рис. 1*).

Результаты исследований показали, что в последнее время потери от киберпреступности значительно увеличились. На *рис. 2* и *3* представлены типы атак, примененных злоумышленниками в 2017 г., а также типы событий, связанные с информационной безопасностью, зафиксированные специалистами Positive Technologies в 2017 г.

Активность хакерских и других атак с течением времени продолжает нарастать, хакеры изобретают все новые способы вмешательства в деятельность банков и краж средств с банковских карт и со счетов. Это вызывает обепокоенность банковского сообщества и повышенную заинтересованность кредитных организаций в увеличении технологий по информационной защите своих данных (*рис. 4*).

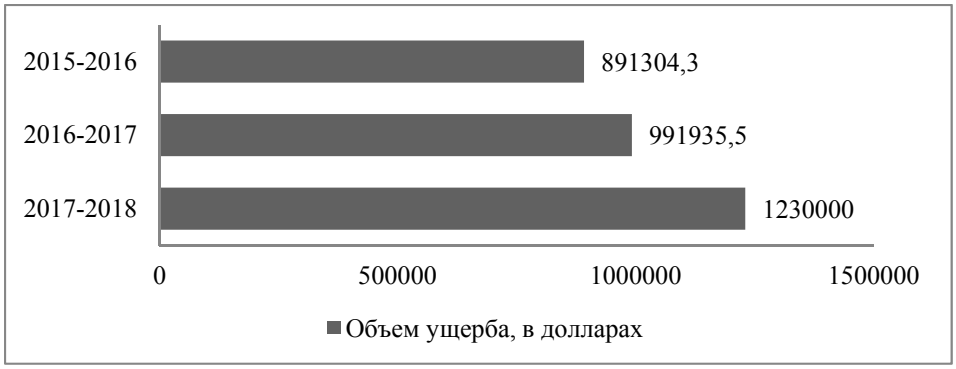

Рис. 1 / Fig. 1. **Утечка данных: убытки крупного бизнеса в области информационной безопасности / Data breach: losses of a large business in the field of information security**

Источник / Source: URL: http://www.tadviser.ru/index.php.

Рис. 2 / Fig. 2. **Виды атак в области информационной безопасности / Types of attacks in the field of information security**

Источник / Source: URL: https://www.ptsecurity.com/ru-ru/.

Рис. 3 / Fig. 3. **Типы событий, связанные с информационной безопасностью, зафиксированные специалистами Positive Technologies в 2017 г. / Types of events related to information security recorded by Positive Technologies specialists in 2017**

Источник / Source: URL: https://www.ptsecurity.com/ru-ru/.

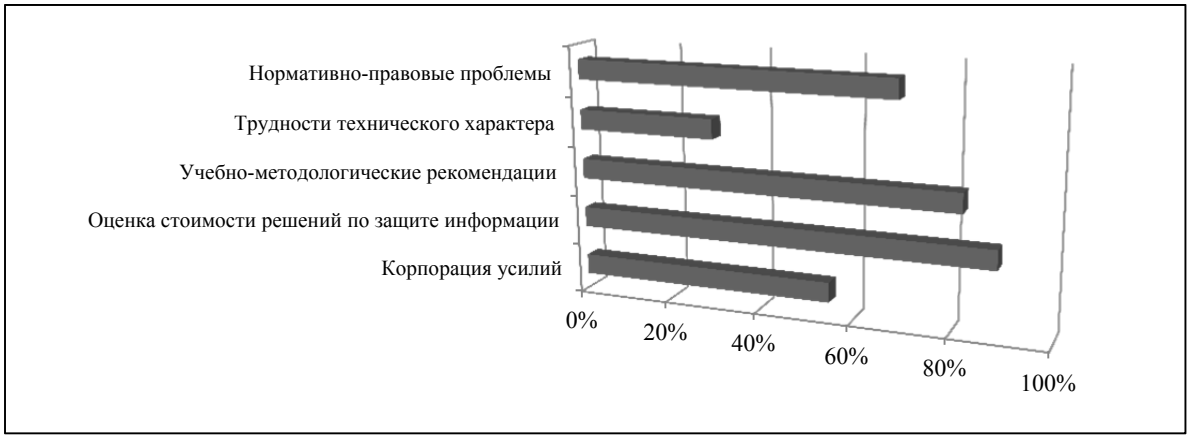

Рис. 4 / Fig. 4. **Заинтересованность коммерческих банков (практиков) в решении проблем ИБ (результаты опроса Ассоциации российских банков 200 респондентов) / The interest of commercial banks (practitioners) in solving information security problems (results of a survey of the Association of Russian Banks of 200 respondents)**

Источник / Source: URL: https://arb.ru/banks/analitycs.

Рис. 5 / Fig. 5. **Уязвимость банковских информационных систем в 2016–2017 гг. / The vulnerability of banking information systems in 2016–2017**

Источник / Source: URL: https://bankir.ru/dom/forum.

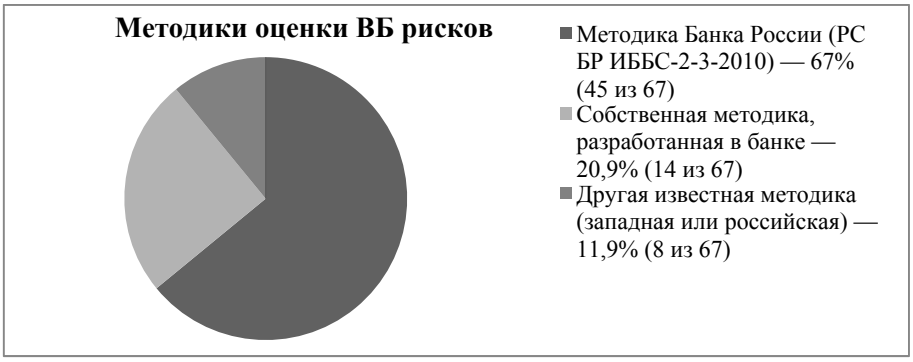

Рис. 6 / Fig. 6. **Опрос специалистов по информационной безопасности кредитных организаций за 2017 г. / Survey of information security specialists of credit institutions for 2017**

Источник / Source: http://www.tadviser.ru/index.php

Для предупреждения или минимизации рисков информационной безопасности необходимо их четко классифицировать в зависимости от различных критериальных признаков. Источниками рисков информационной безопасности являются:

- человеческий фактор;
- неправильный выбор использования интернет-программ и сетей;
- утечка информации различными путями (в том числе и через сотрудников кредитной организации);
- хакерские атаки на банк и его информационные ресурсы;
- несанкционированное отключение сетей;
- нарушения правил пользования информационными ресурсами.

В условиях цифровой экономики потери от рисков информационной безопасности кредитных организаций постоянно растут, а к уже известным их видам (таким как риски утечки информации, недоступности данных, искажения информации, неправильной эксплуатации оборудования) прибавляются новые, связанные, например, со скрытым вмешательством в работу информационных систем.

Следует отметить высокую уязвимость банковских информационных систем (*рис. 5*). Поэтому так важно владеть современными методами оценки и предупреждения рисков информационной безопасности.

В то же время на сегодняшний день нет достаточного количества методик оценки рисков информационной безопасности. Их выбор ограничен, что подтверждается данными опроса 67% кредитных организаций (*рис. 6*).

Как видно из *рис. 6*, разброс применяемых в банковском секторе методик оценки рисков информационной безопасности недостаточно велик. Поэтому так важен вопрос о применяемых методах оценки рисков информационной безопасности, которые позволили бы своевременно и качественно принимать необходимые меры по их минимизации.

2. *Методы оценки рисков информационной безопасности.* Все современные методы оценки рисков

Таблица 1 / Table 1

Условный пример расчета информационных рисков автоматизированной банковской системы / Example of calculating information risks of an automated banking system

№	Показатель: сумма затрат на предупреждение рисков за анализируемый период (у.е.), оценка возможного риска	Балльная оценка возможного риска экспертами по рангу ожидаемого риска или информационных угроз			Итого: сумма ожидаемых потерь (у.е.)
		1	2	3	
1	Риск утечки информации — 800	1	–	–	80
2	Риск недоступности данных — 1000	–	2	–	200
3	Риск искажения информации — 200	–	–	3	60
4	Риск неправильной эксплуатации оборудования — 100	1	–	–	10
5	Риск скрытого вмешательства в работу информационных систем — 700	–	–	3	21
6	Синтетический коэффициент риска — 2800	–	–	–	371

Источник / Source: составлено авторами / compiled by the authors.

информационной безопасности условно можно подразделить на несколько групп (*рис. 6*):

• экспертные оценки с использованием автоматизированных программных средств (явные или скрытые). Недостатком этого способа является зависимость от квалификации / компетенции эксперта;

• статистика вероятности уязвимости и ущерба. Недостатком является необходимость иметь большой объем статистических данных и невозможность точной оценки данных под влиянием быстроменяющейся обстановки (в отдельных случаях — для отдельных угроз — отсутствие данных);

• аналитический подход, основанный на построении графиков по используемым статистическим и математическим моделям.

Кроме перечисленных методов оценки рисков информационной безопасности при построении методики их оценки следует учитывать возможности *количественной и качественной оценки*:

1) количественная оценка рисков ИБ проводится в ситуациях, когда исследуемые угрозы и риски можно сопоставить с количественными конечными значениями, выраженными в денежном эквиваленте, процентах, определенном времени, человекоресурсах и др. [1].

Количественная оценка предусматривает присвоение всем элементам оценки рисков конкретных и реальных количественных значений. Алгоритм оценки и полученных данных должен обеспечивать наглядность и понятность. Объектом оценки может быть ценность актива в денежном выражении, вероятность угрозы, ущерб от реализации угрозы, а также стоимость защитных мер и др. На сегодняшний день четкая методика количественного расчета величин рисков информационной безопасности не разработана. Это связано с отсутствием достаточного объема статистической инфрмации о вероятности реализации какой-либо угрозы в банке, так как информация конфеденциальна и индивидуальна для каждого конкретного банка;

2) качественный метод отличается сложностью получения конкретной оценки объекта из-за неопределенности получаемых показателей. Чаще всего при этом производится балльная оценка выбранных банком для своей индивидуальной методики показателей при обязательном участии экспертов. Качественный метод не использует данные в денежном выражении для объекта оценки. Для сбора данных применяется опрос, интервьирование, анкетирование, личные встречи. Такой анализ рисков проводится с привлечением сотрудников, имеющих опыт и компетенции в области

рассматриваемой угрозы. При этом используется общий подход к оценке риска, сформулированный Базелем 2 и 3, включающий размер возможных потерь, умноженных на вероятность риска (http://www.cbr.ru). При использовании такой методики целесообразно учесть шкалу увеличения показателя риска в разрезе каждого вида информационных рисков для выведения синтетического коэффициента риска (*табл. 1*).

Далее сумму ожидаемых потерь следует умножить на оценку их вероятности, исходя из подобного ранжирования. Можно сделать это отдельно по каждой угрозе или рассчитать обобщающий показатель с выходом на общую сумму потерь от реализации оцененных информационных рисков.

3. *Организационная структура и принципы управления рисками ИБ.* В условиях цифровой экономики и возрастания рисков информационной банковской деятельности требуется перестройка организационной структуры кредитных организаций. Значит, должно появиться специальное подразделение в банке, которое отвечает непосредственно за оценку и минимизацию рисков. Эта деятельность требует создания и разработки специальной политики, задач, принципов и методик оценки и управления информационными рисками, наличия квалификационных и этических требований к работникам, занимающимся этим видом деятельности. Они должны уметь в каждый момент оценивать уровень незащищенности информационных систем банка и на основании анализа вырабатывать необходимые меры для предупреждения рисков или безболезненной ликвидации их последствий.

Особенностью такой работы по управлению рисками информационной безопасности является то, что она охватывает не только работников специального подразделения в банке, но и весь коллектив — от руководителей, служб внутреннего контроля и аудита до рядовых работников бухгалтерии. Поэтому во внутренних документах кредитной организации, в том числе во всех должностных инструкциях, должны быть отражены обязанности, связанные с информационной безопасностью банка и степень ответственности за ее нарушение. Каждый работник кредитной организации должен опираться на внутренние документы банка по рискам информационной безопасности и имеющуюся правовую базу.

4. *Правовая основа и внутренние документы по рискам информационной безопасности.* На сегодняшний день создана основная правовая основа, помогающая регулировать риски информационной безопасности (*табл. 2*).

Из *табл. 2* видно, что список существующих на сегодняшний день правовых основ регулирования рисков информационной безопасности нуждается в расширении для опоры кредитных организаций при создании своих собственных внутрибанковских документов и методик.

Как видно из *рис. 7*, существуют 3 уровня защиты информации, для каждого из которых требование выполняется указанным способом:

«Н» — реализация является необязательной;

«О» — реализация путем применения организационной меры;

«Т» — реализация путем применения технической меры.

После определения необходимого контура применяемой защиты ИБ кредитной организации следует выявить достоинства и недостатки каждого способа управления рисками информационной безопасности.

5. *Способы управления рисками и их минимизация.* Самым известным методом управления рисками информационной безопасности является метод COBIT for Risk. Этот метод основан на утверждении, что риски информационной безопасности являются неотъемлемым составным элементом общей системы банковских рисков. Особенно ярко эта связь проявляется в отношении операционных рисков, поэтому способы и методы управления ими во многом аналогичны уже известным кредитной организации. Однако при этом нельзя забывать про технические моменты их реализации, которым в условиях цифровизации следует уделять особое внимание (*рис. 8*).

Реализации функции управления рисками базируется на анализе и оценке информационной безопасности в организации по разработанному сценарию. Методология рискового сценария представляет собой описание событий, при возникновении которых возможны неопределенные (позитивные и негативные) воздействия на эффективность деятельности организации. Методологией предусматривается разработка более 100 сценариев, характеризующих определенную степень воздействия к определенному типу рисков — стратегические, проектные, риск-менеджмент и др. (*табл. 3*).

Практическое применение методологии COBIT for Risk позволяет выделить следующие достоинства (*табл. 4*) и недостатки (*табл. 5*).

Таблица 2 / Table 2

Законодательная база в области регулирования рисков информационной безопасности / The legal framework in the field of regulation of information security risks

№	Документы (по убыванию важности)	Содержание
1	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Закон регулирует отношения, связанные с использованием различных видов финансовых информационных технологий, возникающих при информационных рисках и мерах по защите кредитных организаций и их клиентов от технических и информационных сбоев и нарушений, а также от утечки информации
2	Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»	Закон регулирует отношения, возникающие при: – формировании нормативной и методологической базы для внедрения электронной подписи в системы документооборота властных структур; – предоставлении административных услуг в электронной форме; – создании юридической базы для проведения государственных и муниципальных закупок посредством электронных торгов; – урегулировании электронного банкинга, в том числе по схеме «клиент-банк»; – усовершенствовании процедур подачи электронной отчетности в налоговые и другие контролирующие инстанции
3	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Закон регулирует отношения, возникающие при взаимодействии кредитной организации с клиентами, способные нанести ущерб пользователю из-за утечки его личной информации, которой могут воспользоваться мошенники, владеющие цифровыми технологиями
4	Письмо Банка России от 24.04.2014 № 49-т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»	Письмо регулирует отношения, возникающие при применении средств защиты от вредоносного кода. В нем даются рекомендации банкам по повышению компетенций работников для применения средств защиты по направлениям и способам выявления вредоносного кода, методам и способам защиты при применении инновационных финансовых технологий в кредитных организациях
5.	ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»	Стандарт регулирует отношения, возникающие при установлении уровня защиты информации (рис. 7)

Источник / Source: составлено авторами / compiled by the authors.

ВЫВОДЫ

Следует отметить, что в связи с развитием информационных технологий растут риски, связанные с их использованием и появляются новые угрозы.

Реализация бессистемных мероприятий, ориентированных на повышение уровня информационной безопасности, сегодня не может обеспечить требуемый уровень защиты. Для понимания приоритетности мероприятий, направленных на повышение уровня информационной безопасности, необходимо разработать и применить механизм управления рисками ИТ-безопасности. Такой эффективный риск-менеджмент позволит сконцентрировать усилия и направить их на защиту банка от опасных угроз с минимальными затратами.

Построение эффективной системы управления рисками ИТ-безопасности — не одноразовый проект, важен комплексный процесс, ориентированный на минимизацию внешних и внутренних угроз, и учет ограничений на ресурсы и фактор времени (https://icc.moscow/upload/doc/ICC_reports_RU.pdf). В этой связи целесообразно использовать метод CRAMM, разработанный Службой безопасности Великобритании (UK Securiti Service) по заказу британского правительства и признанный государственным стандартом построения системы управления рисками IT-безопасности. Система управления рисками как экономически обоснованная стратегия позволит минимизировать внешние и внутренние угрозы, а также издержки и неоправданные расходы.

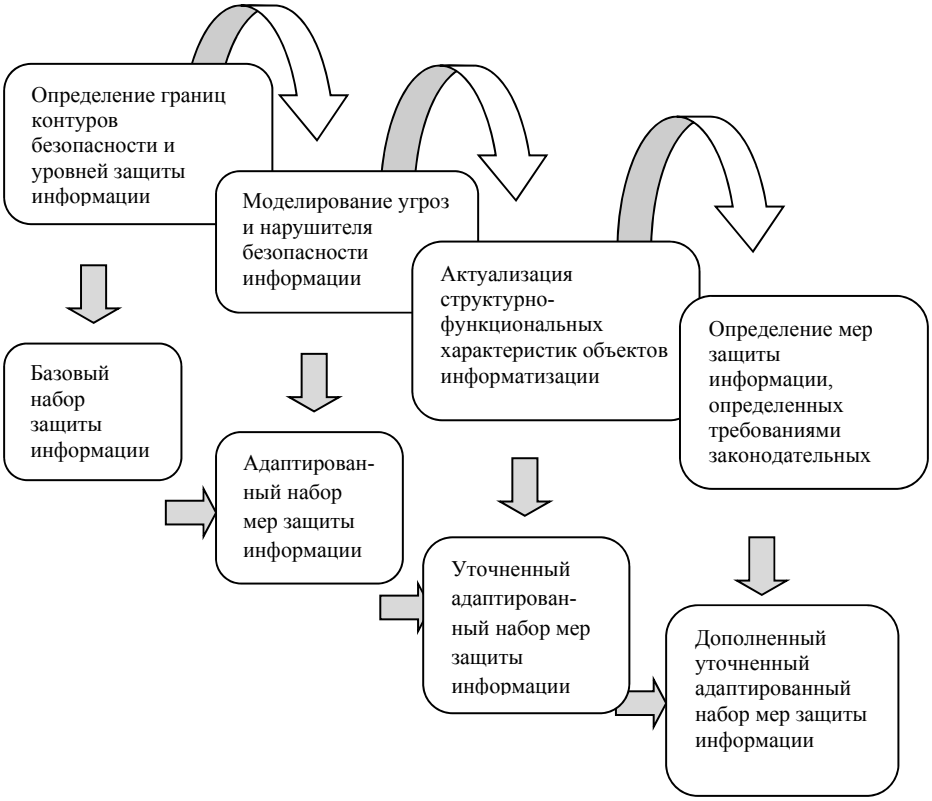

Рис. 7 / Fig. 7. **Определение уровня защиты ИБ / Determination of the IS protection level**

Источник / Source: [2].

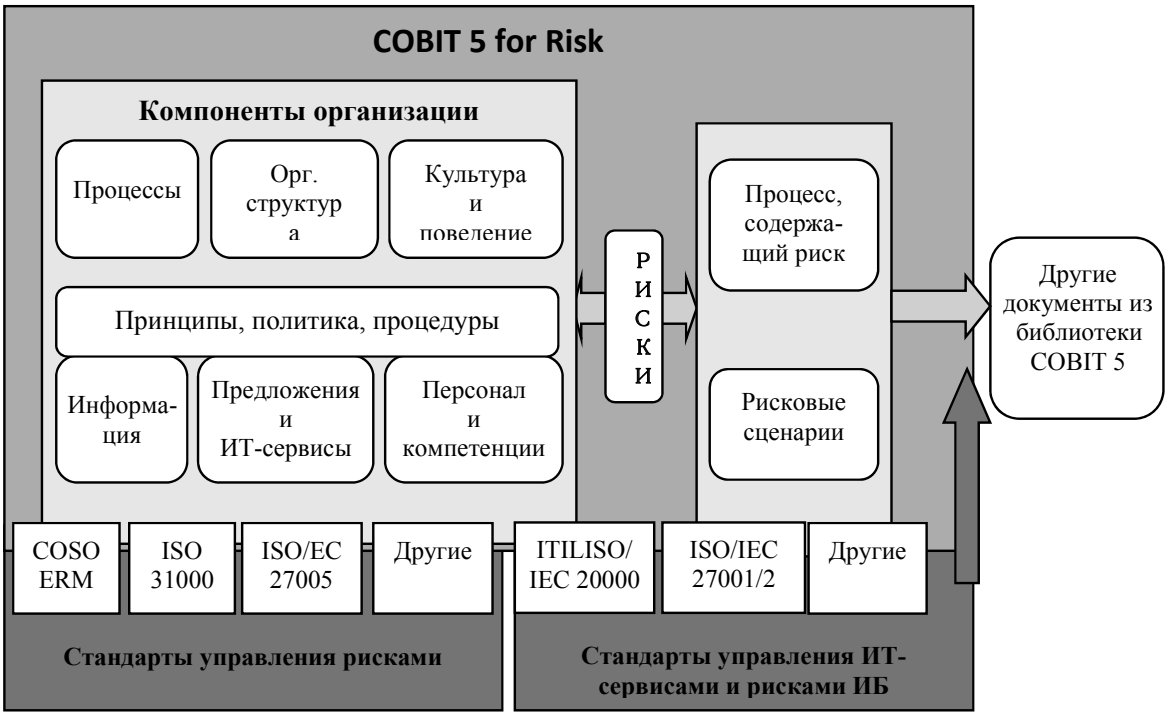

Рис. 8 / Fig. 8. **Схематизация рисков по методу COBIT for Risk ИБ / Risk schematization using the COBIT for Risk information security method**

Источник / Source: [3].

Таблица 3 / Table 3

Типы рисков и характеристика воздействия / Types of risks and exposure characteristics

Типы рисков	Характеристика воздействия
Стратегические риски	Риски, связанные с упущенной возможностью использования ИТ-технологий, ориентированных на повышение эффективности деятельности организации
Проектные риски	Риски влияния ИТ-технологий на создание и развитие действующих технологических процессов
Риски управления и предоставления ИТ-сервисов	Риски, связанные с учетом пожеланий клиентов кредитной организации по использованию ИТ-сервисов

Источник / Source: [3].

Таблица 4 / Table 4

Достоинства применения методологии COBIT for Risk / Benefits of using COBIT for Risk methodology

Достоинство	Характеристика
Связана с общей библиотекой COBIT и «ИТ-контроль» (меры по снижению рисков)	Позволяет рассматривать и оценивать риски информационной безопасности и меры по снижению рисков, воздействующие на бизнес-процессы
Признается международными институтами	Метод, по которому накоплены значительные профессиональные компетенции и имеются хорошие результаты
Наличие понятного формализованного описания методологии	Описание методологии сделано просто и доходчиво, что позволяет избежать многих недоразумений, возникающих при ее использовании
Простота требований к специальным знаниям и компетенциям	Анализ и управление рисками становятся понятны исполнителям и не требуют дополнительных компетенций
Снижение трудозатрат	Применяется внутренними и внешними аудиторами, что не требует составления специальных материалов, дополняющих отчетность банка

Источник / Source: составлено авторами / compiled by the authors.

Таблица 5 / Table 5

Недостатки применения методологии COBIT for Risk / Disadvantages of using COBIT for Risk methodology

Недостаток	Характеристика
Высокая сложность и трудоемкость сбора исходных данных	Требуется вести большую постоянную базу данных
Вовлеченность большого количества заинтересованных лиц	Затрудняет работу в команде, создает условия для возникновения ошибок и просчетов из-за длительного согласования полученных результатов
Отсутствие возможности оценки рисков в денежном выражении	Делает невозможным своевременную оценку необходимых затрат для минимизации рисков или исправления недочетов и ошибок в информационной системе банка

Источник / Source: составлено авторами / compiled by the authors.

СПИСОК ИСТОЧНИКОВ

1. Зинкевич В., Штатов Д. Информационные риски: количественная оценка. *Бухгалтерия и банки*. 2007;(2):50–53.
2. Соколинская Н.Э. Банковские информационные системы и технологии. М.: Кнорус; 2020.
3. Гамза В.А., Ткачук И.В., Жилкин И.М. Безопасность банковской деятельности. 3-е изд. М.: ЮРАЙТ; 2015.

REFERENCES

1. Zinkevich V., Shtatov D. Information risks: Quantitative assessment. *Bukhgalteriya i banki*. 2007;(2):50–53. (In Russ.).
2. Sokolinskaya N.E. Banking information systems and technologies. Moscow: Knorus; 2020. (In Russ.).
3. Gamza V.A., Tkachuk I.V., Zhilkin I.M. Banking security. 3rd ed. Moscow: URAYT; 2015. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Наталия Эвальдовна Соколинская — кандидат экономических наук, профессор Департамента финансовых рынков и банков, Финансовый университет, Москва, Россия
Nsokolinskaya@fa.ru
Людмила Михайловна Куприянова — кандидат экономических наук, доцент Департамента учета, анализа и аудита, заместитель заведующего кафедрой «Экономика интеллектуальной собственности», Финансовый университет, Москва, Россия
kuprianovalm@yandex.ru

ABOUT THE AUTHORS

Natalia E. Sokolinskaya — Cand. Sci. (Econ.), Professor, Department of Financial Markets and Banks, Financial University, Moscow, Russia
Nsokolinskaya@fa.ru
Lyudmila M. Kupriyanova — Cand. Sci. (Econ.), Associate Professor, Department of Accounting, Analysis and Audit, Deputy Head of "Economics of intellectual property" faculty, Financial University, Moscow, Russia
kuprianovalm@yandex.ru

Статья поступила 25.01.2020; принята к публикации 10.06.2020.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was received on 25.01.2020; accepted for publication on 10.06.2020.
The authors read and approved the final version of the manuscript.