БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 4 (115). – 66–83

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 005.342; 330.131.7 DOI: 10.17212/2782-2230-2024-4-66-83

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ И МЕТОДИК ОЦЕНКИ РИСКОВ, ПРИМЕНЯЕМЫХ ПРИ ПРОВЕДЕНИИ МОНИТОРИНГА И ВНУТРЕННЕГО КОНТРОЛЯ БИЗНЕС-ПРОЦЕССОВ*

Е.В. ВАЙЦ[1], Ю.В. ГРАЧЁВА[2], В.А. ВЛАДЫЧЕНСКАЯ[3], Б.С. ГАЛЬЦЕВ[4]

[1] *105005, РФ, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1, Московский государственный технический университет имени Н.Э. Баумана. E-mail: vev@bmstu.ru*
[2] *105005, РФ, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1, Московский государственный технический университет имени Н.Э. Баумана. E-mail: uvgracheva@bmstu.ru*
[3] *105005, РФ, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1, Московский государственный технический университет имени Н.Э. Баумана. E-mail: varvara_zi@mail.ru*
[4] *129090, г. Москва, ул. Мещанская, д. 9/14, стр. 1, Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет "Синергия"». E-mail: b.galtsev@gmail.com*

В статье проводится анализ существующих подходов и методик оценки рисков, которые применяются при мониторинге и внутреннем контроле бизнес-процессов. Авторы рассматривают различные методы оценки рисков и их применимость при мониторинге и внутреннем контроле. Актуальность темы обусловлена необходимостью разработки и внедрения эффективных методов оценки рисков в условиях постоянно меняющейся бизнес-среды. Результаты исследования могут быть полезны для специалистов по управлению рисками, внутреннему контролю и мониторингу бизнес-процессов.
В статье проводится анализ рисков, связанных с бизнес-процессом «Открытие, ведение и закрытие банковских счетов юридических и физических лиц». Рассматриваются основные виды рисков, которые могут возникнуть на каждом этапе этого процесса, а также методы их оценки и управления.

Ключевые слова: автоматизированная банковская система, дистанционное банковское обслуживание, оценка рисков, угроза, уязвимость, бизнес-процесс

* Статья получена 26 ноября 2024 г.
Работа выполнена в рамках госзадания Минобрнауки России (тема № FSFN-2024-0030).

ВВЕДЕНИЕ

Оценка рисков в обязательном порядке должна проводиться для объектов информационной инфраструктуры организации, а также при проведении мониторинга и внутреннего контроля бизнес-процессов, в том числе для банковских и кредитных организаций, – бизнес-процессов автоматизированных банковских систем и дистанционного банковского обслуживания (далее – АБС и ДБО соответственно).

Работники, проводящие оценку рисков, должны знать:

– законодательство Российской Федерации в данной области;

– международные и национальные стандарты в области оценки рисков и обеспечения информационной безопасности (далее – ИБ);

– нормативные акты регулирующих и надзорных органов в области оценки рисков и обеспечения ИБ;

– внутренние документы организации, регламентирующие деятельность в области оценки рисков и обеспечения ИБ;

– современные средства вычислительной и телекоммуникационной техники, операционные системы, системы управления базами данных, а также способы выполнения бизнес-процессов и обеспечения ИБ в них;

– возможные источники угроз ИБ, способы реализации угроз, частоту реализации угроз в прошлом;

– для банковских и кредитных организаций – знать способы обеспечения ИБ в платежных, информационных и телекоммуникационных системах организации, а также различные подходы к обеспечению ИБ, защитных мер и свойственных им ограничений.

1. ОЦЕНКА РИСКОВ НАРУШЕНИЯ ИБ

На основе общедоступных каталогов и справочников угроз, а также базовых отраслевых моделей угроз информационной безопасности в организации проводится идентификация угроз информационной безопасности, которые могут возникнуть в ходе эксплуатации объектов информационной инфраструктуры и выполнения бизнес-процессов.

После идентификации угроз осуществляется разработка механизмов обеспечения информационной безопасности, направленных на противодействие реализации применимых угроз.

На основе полученных результатов проводится оценка уровня рисков.

Выделим основные этапы качественной оценки рисков:

– оценка степени возможности реализации угроз;

– оценка степени тяжести последствий от реализации угроз;
– оценка уровня рисков.

1.1. ОЦЕНКА СТЕПЕНИ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ

Оценка степени возможности реализации (далее – СВР) угроз может принимать следующие значения: нереализуемая, минимальная, средняя, высокая, критическая.

Степень возможности реализации признается критической, если выполняются следующие условия:

– вероятность возникновения инцидента ИБ (реализации угрозы) чрезвычайно высокая (ожидания: 2 раза и более за полугодие);
– инциденты происходят практически с постоянной периодичностью;
– мотивация нарушителя чрезвычайно высокая;
– уязвимость может быть легко использована, или отсутствуют адекватные защитные меры.

Степень возможности реализации признается высокой, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– вероятность возникновения инцидента высокая (ожидания: не менее одного раза в год);
– возможность возникновения инцидента подтверждается данными за прошлый год;
– мотивация нарушителя высокая;
– уязвимость может быть легко использована, и существующие защитные меры не результативны.

Степень возможности реализации признается средней, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– вероятность возникновения инцидента средняя (ожидания: один раз в 2 года);
– подобные инциденты были зарегистрированы в прошлом;
– мотивация нарушителя средняя;
– уязвимость может быть использована, но есть определенные механизмы контроля.

Степень возможности реализации признается минимальной, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– вероятность возникновения инцидента низкая (ожидания: не менее одного раза в 5 лет);

– возможно, были подобные инциденты в прошлом;

– мотивация нарушителя низкая или отсутствует;

– использовать уязвимость сложно, и/или присутствуют достаточные механизмы контроля.

Степень возможности признается нереализуемой, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– вероятность возникновения инцидента очень низкая (ожидания: реже одного раза в 5 лет);

– подобных инцидентов в прошлом не было;

– мотивация нарушителя отсутствует;

– использовать уязвимость практически невозможно, и/или присутствуют результативные механизмы контроля.

В случае невозможности однозначного определения СВР осуществляется вычисление среднего значения СВР от оценок всех экспертов по оценке рисков нарушения ИБ.

1.2. ОЦЕНКА СТЕПЕНИ ТЯЖЕСТИ ПОСЛЕДСТВИЙ ОТ РЕАЛИЗАЦИИ УГРОЗ

Оценка степени тяжести последствий (далее – СТП) может принимать следующие значения: низкая, средняя, высокая, критическая.

Степень тяжести последствий оценивается как критическая, если выполняется хотя бы одно из следующих условий:

– реализация угрозы ведет к нарушению бизнес-процессов организации, приводящему к невозможности предоставления услуг клиентам организации (например, нарушение функционирования сегментов сети передачи данных или групп оборудования, возникшее вследствие форс-мажорных обстоятельств);

– прямые или косвенные финансовые потери от реализации угрозы превышают установленное в организации верхнее пороговое значение (далее – ВПР);

– реализация угрозы окажет критическое влияние на репутацию организации (например, общественные скандалы, негативные заявления в средствах массовой информации и т. п.). Практически невозможно восстановление репутации организации. Значительные усилия организации по восстановлению своей репутации не гарантируют положительных результатов.

Степень тяжести последствий оценивается как высокая, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– реализация угрозы приводит к нарушению бизнес-процессов организации, повлекшему за собой полное прекращение предоставления услуг клиенту или снижение качества предоставляемых услуг нескольким клиентам;

– прямые или косвенные финансовые потери от реализации угрозы будут находиться в диапазоне от установленного в организации среднего порогового значения (далее – СПР) до ВПР;

– реализация угрозы вызовет бурную негативную реакцию общественности и/или клиентов и, как следствие, ухудшение репутации организации на рынке. Организация должна приложить значительные усилия для восстановления своего имиджа.

Степень тяжести последствий оценивается как средняя, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– реализация угрозы приводит к значительному нарушению бизнес-процессов организации, повлекшему за собой частичное исчезновение услуги или замедление работы;

– прямые или косвенные финансовые потери от реализации угрозы будут находиться в диапазоне от установленного в организации низкого порогового значения (далее – НПР) до СПР;

– реализация угрозы вызовет негативную реакцию общественности и/или клиентов и, как следствие, ухудшение репутации организации на рынке. Организация должна приложить усилия для восстановления своего имиджа.

Степень тяжести последствий оценивается как низкая, если не выполнено ни одно из вышеописанных условий, но выполняется хотя бы одно из следующих:

– реализация угрозы приводит к небольшому нарушению бизнес-процессов организации, которое не окажет существенного влияния на предоставляемые клиентам услуги;

– прямые или косвенные финансовые потери от реализации угрозы составят менее установленного НПР;

– реализация угрозы практически не влияет на репутацию организации, но возможна негативная реакция со стороны некоторой части клиентов или контрагентов организации. Организация должна приложить некоторые усилия для восстановления своего имиджа.

В случае невозможности однозначного определения СТП осуществляется вычисление среднего значения СТП от оценок всех экспертов по оценке рисков нарушения.

1.3. ОЦЕНКА УРОВНЯ РИСКОВ

Уровень риска определяется на основе значений СТП и СВР с помощью табл. 1.

Таблица 1

СВР	СТП			
	Минимальная	Средняя	Высокая	Критическая
	Риск			
Нереализуемая	Незначительный	Незначительный	Незначительный	Умеренный
Минимальная	Незначительный	Незначительный	Умеренный	Умеренный
Средняя	Незначительный	Умеренный	Умеренный	Высокий
Высокая	Умеренный	Умеренный	Высокий	Высокий
Критическая	Умеренный	Высокий	Высокий	Высокий

Для ранжирования и наглядности представления результатов оценки рисков шкала рангов риска подразделяется на три группы риска.

1. Высокий риск. В общем случае риски этой группы являются недопустимыми и требуют обработки. Принятие таких рисков допустимо только в исключительных случаях и должно быть утверждено руководством организации после детального анализа возможностей обработки.

2. Умеренный риск. Риски этой группы являются нежелательными. Решение о принятии таких рисков принимает руководство организации. В качестве критерия принятия рисков, относящихся к данной категории, служит оценка стоимости внедрения защитных мер для снижения рисков. Если стоимость внедрения не оправдывает получаемого эффекта, риск может приниматься.

3. Незначительный риск. В применении механизмов контроля для минимизации рисков этой группы необходимости нет, так как усилия по управлению таких рисков не будут играть важной роли в связи с незначительным уровнем самого риска.

Таблица 2

Уровень риска	Допустимость риска	Принятие риска	Необходимость в обработке
Незначительный	Риски этой группы являются **допустимыми**	Риски принимаются руководством без рассмотрения	В обработке риска нет необходимости
Умеренный	Риски этой группы являются **нежелательными**	Руководство принимает без детального рассмотрения, в качестве критериев принятия риска выступает неприемлемая стоимость защитных мер на снижение данного риска	Риски подвергаются обработке в случае соответствия стоимости защитных мер возможным потерям
Высокий	Риски этой группы являются **недопустимыми**	Принятие рисков руководством возможно после тщательного анализа и в качестве исключения, например, в случаях отсутствия мер защиты от такого риска или их чрезвычайной дороговизны	Риски подвергаются обработке

На основе результатов оценки рисков организация должна принять решение относительно минимизации выявленных рисков.

2. ОСНОВНЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ БИЗНЕС-ПРОЦЕССОВ

Существует масса подходов и методик по оценке рисков, однако не все они применимы в той или иной прикладной сфере. Ниже представлен перечень наиболее применимых подходов и методик по оценке рисков бизнес-процессов организаций.

1. Качественная оценка рисков (Qualitative Risk Assessment)

Метод, основанный на экспертных оценках и качественных показателях, таких как вероятность возникновения риска и его потенциальное воздействие. Риски, как правило, классифицируются по уровням (высокий, средний, низкий).

Подходы

- SWOT-анализ – оценка рисков на основе сильных и слабых сторон, возможностей и угроз.
- Матрица вероятности и воздействия (Risk Impact/Probability Matrix) – визуализация рисков с учетом вероятности их наступления и возможного воздействия.

2. Количественная оценка рисков (Quantitative Risk Assessment)

Используются числовые данные и модели для оценки рисков, что позволяет рассчитать вероятности и финансовые последствия рисков.

Подходы

- Анализ дерева решений (Decision Tree Analysis) – метод, позволяющий оценить последствия различных решений и связанных с ними рисков.
- Монте-Карло (Monte Carlo Simulation) – использование компьютерных моделей для прогнозирования и оценки возможных исходов рисков.
- Финансовое моделирование (Financial Modeling) – оценка финансовых рисков с использованием данных о вероятности и последствиях различных сценариев.

3. Анализ сценариев (Scenario Analysis)

Метод, предполагающий рассмотрение различных сценариев – как положительных, так и негативных – с целью оценки их влияния на бизнес-процессы.

Подходы

- Стресс-тестирование (Stress Testing) – проверка устойчивости бизнес-процессов при самых неблагоприятных сценариях.
- Анализ «что если» (What-If Analysis) – анализ различных гипотетических ситуаций и их последствий для бизнеса.

4. Анализ исторических данных (Historical Data Analysis)

Оценка рисков на основе анализа данных о прошлых инцидентах и ситуациях.

Подходы

- Регрессионный анализ (Regression Analysis) – использование статистических методов для выявления зависимостей и прогнозирования рисков.
- Анализ трендов (Trend Analysis) – оценка рисков на основе анализа изменений в исторических данных.

5. Анализ отказов и их последствий (Failure Mode and Effects Analysis – FMEA)

Метод, фокусирующийся на идентификации потенциальных точек отказа и оценке их последствий.

Подходы

- Оценка вероятности и тяжести отказа – анализ вероятности возникновения отказов и серьезности их последствий.
- Разработка планов по минимизации последствий – разработка стратегий для минимизации воздействия отказов.

6. Анализ рисков с использованием ключевых показателей риска (Key Risk Indicators – KRI)

Использование определенных показателей для мониторинга рисков и выявления их на ранних стадиях.

Подходы

- Установка пороговых значений KRI – определение допустимых значений ключевых показателей риска и мониторинг их изменений.
- Регулярный мониторинг и отчетность – постоянное отслеживание KRI и создание отчетов для своевременного реагирования на риски.

7. Комплексная оценка рисков (Integrated Risk Assessment)

Интегрированный подход, который объединяет различные методы оценки рисков, чтобы дать целостную картину.

Подходы

- Взаимодействие с различными подразделениями – включение различных подразделений для всесторонней оценки рисков.
- Использование программного обеспечения для интегрированной оценки – применение специализированных программ для объединения и анализа данных по рискам.

3. ПРИМЕНЕНИЕ МЕТОДОВ ОЦЕНКИ РИСКОВ БИЗНЕС-ПРОЦЕССОВ

Рассмотрим в качестве примера применение методов оценки рисков по отношению к бизнес-процессу банковской организации «Открытие, ведение и закрытие банковских счетов юридических и физических лиц».

Бизнес-процесс «Открытие, ведение и закрытие банковских счетов юридических и физических лиц» представим в виде раздельных схем, составленных в соответствии с нотацией BPMN v.2.0: схема открытия лицевого счета (рис. 1), схема ведения лицевого счета (рис. 2), схема закрытия лицевого счета (рис. 3).

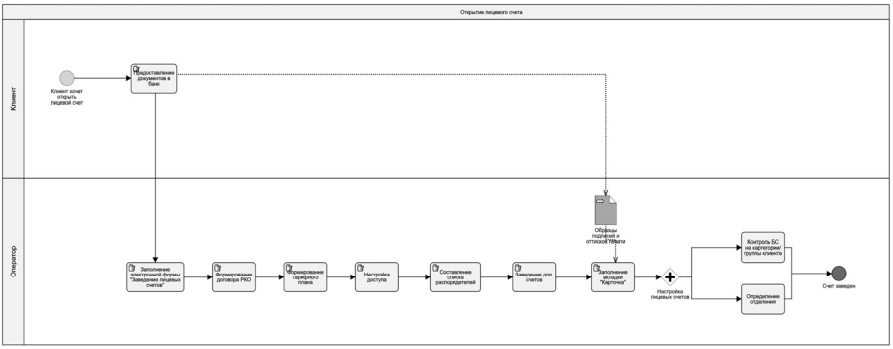

Рис. 1. Бизнес-процесс открытия лицевого счета

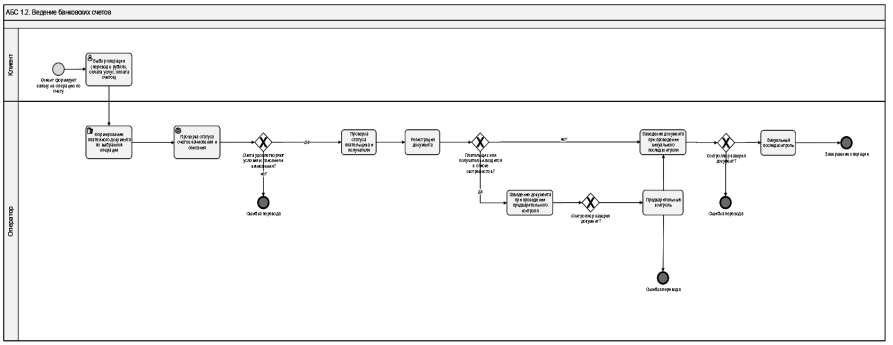

Рис. 2. Бизнес-процесс ведения лицевого счета

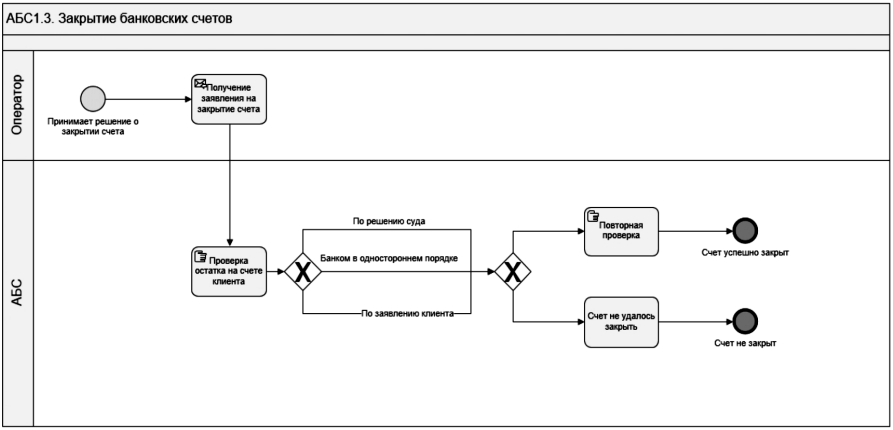

Рис. 3. Бизнес-процесс закрытия лицевого счета

Возможные риски бизнес-процесса «Открытие, ведение и закрытие банковских счетов юридических и физических лиц»:

– риски несоответствия законодательным и регуляторным требованиям;
– операционные риски;
– риски мошенничества;
– репутационные риски;
– риски снижения качества обслуживания;
– риски потери данных или утечек информации.

Подходы оценки рисков

1. Риски несоответствия законодательным и регуляторным требованиям

Процесс открытия и ведения счетов напрямую регулируется законодательством, включая требования по ПОД/ФТ. Несоответствие может привести к штрафам, санкциям и утрате лицензии.

Применяемые методы

• Качественная оценка рисков (матрица вероятности и воздействия). Позволяет классифицировать риски нарушения требований и разработать меры по их снижению, например, через усиление контроля за документами клиентов.

• Анализ сценариев (стресс-тестирование). Применяется для моделирования ситуаций, когда происходит резкое изменение регуляторных требований, чтобы оценить готовность банка к таким изменениям и адаптировать процессы.

2. Операционные риски

В процессе «Открытие, ведение и закрытие банковских счетов юридических и физических лиц» высок риск ошибок и сбоев, связанных с человеческим фактором или системными сбоями, которые могут повлиять на корректность ведения счетов и безопасность данных клиентов.

Применяемые методы

- FMEA (анализ отказов и их последствий). Идентифицирует возможные точки отказа в процессах, таких как неправильно введенные данные клиента или системные сбои, и разрабатывает план действий для их предотвращения.
- Анализ исторических данных. Используется для выявления повторяющихся ошибок или проблем, таких как частые сбои в работе системы, что помогает разработать меры по их устранению.

3. Риски мошенничества

Процессы открытия и ведения счетов подвержены рискам мошеннических действий, включая использование поддельных документов и незаконных транзакций. Это требует эффективных методов оценки и мониторинга рисков.

Применяемые методы

- Количественная оценка рисков (метод Монте-Карло). Помогает моделировать и оценивать вероятность финансовых потерь в результате мошенничества, а также разработать меры по предотвращению таких ситуаций, например, через усиление проверки документов.
- Анализ рисков с использованием KRI (ключевые показатели риска) – внедрение показателей, которые будут отслеживать потенциальные аномалии в транзакциях, что позволит быстро выявлять и блокировать подозрительные операции.

4. Репутационные риски

Ошибки в процессе открытия и ведения счетов могут негативно повлиять на доверие клиентов и репутацию банка. Эффективное управление этими рисками помогает сохранить и укрепить репутацию.

Применяемые методы

- Анализ сценариев («что если») – оценка последствий потенциальных репутационных рисков, таких как массовое закрытие счетов или утечка данных, и разработка мер реагирования.

• Анализ трендов. Мониторинг изменений в клиентском поведении или внешней среде позволяет заранее выявить потенциальные репутационные риски и адаптировать процессы для их минимизации.

5. Риски снижения качества обслуживания

Важно управлять рисками, связанными с идентификацией клиентов, обработкой их данных и качеством обслуживания, чтобы обеспечить их безопасность.

Применяемые методы

• Комплексная оценка рисков – использование нескольких методов (например, SWOT-анализ и FMEA) для оценки рисков на каждом этапе взаимодействия с клиентами, от открытия счета до его закрытия.

• Мониторинг KRI – постоянное отслеживание ключевых показателей, которые могут указывать на ухудшение качества обслуживания или возникновение проблем, связанных с обработкой данных клиентов.

6. Риски потери данных или утечек информации

Процессы открытия и ведения счетов подвержены рискам несанкционированного доступа, утечки или потери конфиденциальных данных клиентов, что может привести к финансовым убыткам и репутационным потерям для банка.

Применяемые методы

• Шифрование данных – использование современных методов шифрования для защиты данных клиентов как при хранении, так и при передаче, что снижает риск утечек.

• Многофакторная аутентификация (MFA) – внедрение многофакторной аутентификации для обеспечения дополнительного уровня защиты доступа к системам, содержащим данные клиентов.

• Мониторинг активности – постоянный мониторинг и анализ активности в системе для выявления подозрительных действий или попыток несанкционированного доступа.

Вывод

Эти методы оценки рисков целесообразно применять в данном бизнес-процессе для обеспечения его устойчивости, соответствия требованиям законодательства и повышения надежности операций. Это помогает минимизировать как операционные и финансовые риски, так и репутационные, что в конечном итоге способствует укреплению доверия клиентов и улучшению качества обслуживания.

Описанные выше методы и подходы помогут всесторонне оценить риски, связанные с бизнес-процессом «Открытие, ведение и закрытие банковских счетов юридических и физических лиц».

ЗАКЛЮЧЕНИЕ

В настоящее время существует множество методов и инструментов для оценки рисков в различных областях деятельности. Однако выбор наиболее подходящего подхода и методики зависит от специфики конкретного бизнес-процесса, его сложности и особенностей.

Анализ показал, что наиболее эффективными являются комплексные подходы, которые учитывают как количественные, так и качественные аспекты рисков. Также важно использовать современные технические и программные средства, такие как системы управления рисками, аналитические платформы и инструменты для моделирования и прогнозирования.

Результаты исследования могут быть полезны для организаций, стремящихся улучшить свои процессы мониторинга и контроля рисков. Они позволяют выбрать наиболее подходящие методы, а также разработать более эффективные стратегии управления рисками.

Дальнейшие исследования в этой области могут быть направлены на разработку новых подходов и методик, учитывающих специфику конкретных отраслей и типов бизнес-процессов, а также подходов и методик по поиску уязвимостей в бизнес-процессах (бизнес-логике) организаций, что позволит создать более точные и надежные инструменты оценки рисков и повысить эффективность управления ими.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51897–2011. Менеджмент риска. Термины и определения. – М.: Стандартинформ, 2012.

2. ГОСТ Р ИСО 31000–2019. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2019.

3. ГОСТ Р МЭК 61160–2006. Менеджмент риска. Формальный анализ проекта. – М.: Стандартинформ, 2006.

4. *Балдин К.В., Передеряев И.И., Голов Р.С.* Управление рисками в предпринимательстве. – М.: Дашков и К°, 2017.

5. *Вяткин В.Н., Гамза В.А., Маевский Ф.В.* Риск-менеджмент. – М.: Юрайт, 2023.

6. *Домащенко Д.В., Финогенова Ю.Ю.* Управление рисками в условиях финансовой нестабильности. – М.: Магистр: Инфра-М, 2010.

7. *Качалов Р.М.* Управление экономическим риском: теоретические основы и приложения. – СПб.: Нестор-История, 2012.

8. *Когденко В.Г.* Анализ финансовых рисков в рамках фундаментального анализа компании // Финансовая аналитика: проблемы и решения. – 2015. – Т. 8, вып. 34. – С. 2–14.

9. Риск-менеджмент в коммерческом банке / под ред. И.В. Ларионовой. – М.: КноРус, 2014. – 454 с. – ISBN 978-5-406-02907-7.

10. *Мамаева Л.Н.* Управление рисками. – М.: Дашков и К°, 2013.

11. *Плошкин В.В.* Оценка и управление рисками на предприятиях. – Старый Оскол: ТНТ, 2014.

12. *Рыхтикова Н.А.* Анализ и управление рисками организации. – М.: Форум, 2012.

13. *Уродовских В.Н.* Управление рисками предприятия. – М.: Вузовский учебник: Инфра-М, 2011.

14. *Шапкин А.С., Шапкин В.А.* Теория риска и моделирование рисковых ситуаций. – М.: Дашков и К°, 2019.

15. Энциклопедия финансового риск-менеджмента / под ред. А.А. Лобанова, А.В. Чугунова. – М.: Альпина Паблишер, 2003.

Вайц Екатерина Викторовна, кандидат технических наук, доцент кафедры «Защита информации» Московского государственного технического университета имени Н.Э. Баумана. E-mail: vev@bmstu.ru

Грачёва Юлия Викторовна, старший преподаватель кафедры «Защита информации» Московского государственного технического университета имени Н.Э. Баумана. E-mail: uvgracheva@bmstu.ru

Владыченская Варвара Александровна, старший преподаватель кафедры «Защита информации» Московского государственного технического университета имени Н.Э. Баумана. E-mail: varvara_zi@mail.ru

Гальцев Борис Сергеевич, аспирант Московского финансово-промышленного университета «Синергия». E-mail: b.galtsev@gmail.com

DOI: 10.17212/2782-2230-2024-4-66-83

Analysis of existing approaches and methods for risk assessment used in monitoring and internal control of business processes *

E.V. Vaitc[1], Y.V. Gracheva[2], V.A. Vladychenskaya[3], B.S. Galtsev[4]

[1] *Bauman Moscow State Technical University, 105005, 2-ya Baumanskaya Street, 5/1, Moscow, 105005, Russian Federation. E-mail: vev@bmstu.ru*
[2] *Bauman Moscow State Technical University, 105005, 2-ya Baumanskaya Street, 5/1, Moscow, 105005, Russian Federation. E-mail: uvgracheva@bmstu.ru*
[3] *Bauman Moscow State Technical University, 105005, 2-ya Baumanskaya Street, 5/1, Moscow, 105005, Russian Federation. E-mail: varvara_zi@mail.ru*
[4] *Non-state private educational institution of higher education «Moscow Financial and Industrial University "Synergy", Meshchanskaya Street, 9/14, building 1, Moscow, 129090, Russian Federation. E-mail: b.galtsev@gmail.com*

The article analyzes the existing approaches and methods of risk assessment used in monitoring and internal control of business processes. The authors consider various methods of risk assessment and their applicability in the context of monitoring and internal control.
The relevance of the topic is due to the need to develop and implement effective risk assessment methods in an ever-changing business environment. The results of this study can be useful for risk management specialists, internal control and monitoring of business processes.
The article also analyzes the risks associated with the business process of "Opening, maintaining and closing bank accounts for legal entities and individuals". The main types of risks that can arise at each stage of this process, as well as methods of their assessment and management, are considered.

Keywords: core banking system, remote banking services, vulnerability, threat, risk assessment

REFERENCES

1. GOST R 51897–2011. *Menedzhment riska. Terminy i opredeleniya* [State Standard R 51897–2011. Risk management. Terms and definitions].Moscow, Standartinform Publ., 2012.

2. GOST R ISO 31000–2019. *Menedzhment riska. Printsipy i rukovodstvo* [State Standard R ISO 31000-2019. Risk Management. Principles and guidelines]. Moscow, Standartinform Publ., 2019.

* *Received 26 November 2024.*
The work was carried out according to the state assignment of the Ministry of Education and Science of the Russian Federation (topic No. FSFN-2024-0030).

3. GOST R MEK 61160–2006. *Menedzhment riska. Formal'nyi analiz proekta* [State Standard R IEC 61160–2006. Risk management. Formal design review]. Moscow, Standartinform Publ., 2006.

4. Baldin K.V., Perederyaev I.I., Golov R.S. *Upravlenie riskami v predprinimatel'stve* [Risk management in entrepreneurship]. Moscow, Dashkov & Co. Publ., 2017.

5. Vyatkin V.N., Gamza V.A., Maevskii F.V. *Risk-menedzhment* [Risk Management]. Moscow, Yurayt Publ., 2023.

6. Domashchenko D.V., Finogenova Yu.Yu. *Upravlenie riskami v usloviyakh finansovoi nestabil'nosti* [Risk management in conditions of financial instability]. Moscow, Magistr Publ., Infra-M Publ., 2010.

7. Kachalov R.M. *Upravlenie ekonomicheskim riskom: teoreticheskie osnovy i prilozheniya* [Economic risk management: theoretical foundations and applications]. St. Petersburg, Nestor-Istoriya Publ., 2012.

8. Kogdenko V.G. Analiz finansovykh riskov v ramkakh fundamental'nogo analiza kompanii [Analyzing financial risks within fundamental analysis of the company]. *Finansovaya analitika: problemy i resheniya = Financial Analytics: Science and Experience*, 2015, vol. 8, iss. 34, pp. 2–14.

9. Larionova I.V., ed. *Risk-menedzhment v kommercheskom banke* [Risk management in a commercial bank]. Moscow, KnoRus Publ., 2014. 454 p. ISBN 978-5-406-02907-7.

10. Mamaeva L.N. *Upravlenie riskami* [Risk management]. Moscow, Dashkov & Co. Publ., 2013.

11. Ploshkin V.V. *Otsenka i upravlenie riskami na predpriyatiyakh* [Assessment and risk management at enterprises]. Staryi Oskol, TNT Publ., 2014.

12. Rykhtikova N.A. *Analiz i upravlenie riskami organizatsii* [Analysis and risk management of an organization]. Moscow, Forum Publ., 2012.

13. Urodovskikh V.N. *Upravlenie riskami predpriyatiya* [Enterprise risk management]. Moscow, Infra-M Publ., 2011.

14. Shapkin A.S., Shapkin V.A. *Teoriya riska i modelirovanie riskovykh situatsii* xTheory of risk and modeling of risky situations]. Moscow, Dashkov & Co. Publ., 2019.

15. Lobanov A.A., Chugunov A.V., ed. *Entsiklopediya finansovogo risk-menedzhmenta* [Encyclopedia of financial risk management]. Moscow, Alpina Publisher, 2003.

Для цитирования:

Анализ существующих подходов и методик оценки рисков, применяемых при проведении мониторинга и внутреннего контроля бизнес-процессов / Е.В. Вайц, Ю.В. Грачёва, В.А. Владыченская, Б.С. Гальцев // Безопасность цифровых технологий. – 2024. – № 4 (115). – С. 66–83. – DOI: 10.17212/2782-2230-2024-4-66-83.

For citation:

Vaitc E.V., Gracheva Y.V., Vladychenskaya V.A., Galtsev B.S. Analiz sushchestvuyushchikh podkhodov i metodik otsenki riskov, primenyaemykh pri provedenii monitoringa i vnutrennego kontrolya biznes-protsessov [Analysis of existing approaches and methods for risk assessment used in monitoring and internal control of business processes]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 4 (115), pp. 66–83. DOI: 10.17212/2782-2230-2024-4-66-83.