УДК. 338.2, ББК 65.052 © Е.А. Касюк
DOI: 10.24412/2225-8264-2023-1-71-78

Е.А. Касюк

НОВЫЕ ТЕНДЕНЦИИ УПРАВЛЕНИЯ И КОНТРОЛЯ ОПЕРАЦИОННОГО РИСКА В ФИНАНСОВЫХ ИНСТИТУТАХ

В статье рассматривается вопрос о современных тенденциях в управлении и контроле операционного риска в финансовых институтах. Цель статьи – определить основные тенденциях в управлении и контроле операционного риска в финансовых институтах, знание которых даст возможность принимать эффективные управленческие решения по минимизации операционных рисков, в т.ч. за счет неправильного использования ИТ-систем.

Исследование проводится на основе теоретических методах изучения, обобщения и анализа. Основой работы являются фундаментальные труды отечественных и зарубежных авторов по вопросам банковского риск-менеджмента и внутреннего контроля.

В настоящее время финансовые учреждения понимают большое влияние эффективного управления рисками на возможности получения прибыли. Таким образом, управление рисками стало важной частью финансовых инструментов. Согласно последним исследованиям, все еще остаются проблемы, связанные с управлением различными видами рисков. Например, Базельский комитет по банковскому надзору Банка международных расчетов призывает финансовые учреждения уделять более пристальное внимание проблемам управления операционными рисками. Из-за возросшей интенсивности проводимых финансовых операций финансовые учреждения стали очень уязвимы к операционным рискам. Во многих случаях высокий уровень операционных рисков обусловлен сбоями ИТ-систем. Принимая во внимание этот факт, можно согласиться, что сокрытие внутренней информации и злоупотребление ею стали одним из наиболее важных факторов, влияющих на управление операционными рисками в финансовых учреждениях. В настоящее время большая часть мероприятий по управлению рисками, в частности, во всех типах финансовых учреждений, сосредоточена именно на предотвращении внутренних инцидентов и случаев мошенничества и борьбе с ними.

В заключении в статье предложены меры по снижению операционного риска, в том числе направленные на уменьшение возможного мошенничества, например, - расширение возможности управления операционными рисками командами для обеспечения информационной безопасности и содействия полноте информационной безопасности в трех основных аспектах информационной безопасности.

Ключевые слова*:* стабильность, банковская система, операционные риски, управление операционным риском, контроль операционного риска, информационные технологии

Стабильность банковской системы играет важную роль в долгосрочном росте экономики. Ослабление банковской системы любой страны представляет угрозу для финансовой стабильности, как в конкретной стране, так и за рубежом. В современном мире роль банков выходит за рамки денежно-кредитных отношений. Современный банк представляет собой супермаркет финансовых услуг. Невозможно представить себе нормальную, рациональную организацию экономической деятельности без банков. Именно по этой причине перед институтами банковского надзора сейчас стоит задача способствовать укреплению финансового здоровья банковской системы. Именно из-за этого все стороны должны быть заинтересованы в успешном управлении банками сегодня и в способности справляться с будущими вызовами. Ответственность за это, прежде всего, лежит на самих банках, однако также учреждения банковского надзора должны играть важную роль в предоставлении банкам возможности сбалансированного управления и разумной капитализации.

Банковские кризисы, которые произошли как в странах с переходной экономикой, так и в развивающихся странах за последние десять лет, укрепили убежденность в важности стабильной и хорошо регулируемой банковской системы. Поэтому все больше внимания уделяется обеспечению его стабильности и анализу его развития.

Стабильность банковской системы можно определить, как способность ее функционирования в устойчивом равновесии при различных экономических обстоятельствах и обеспечивать гарантии отсутствия необходимости вливаний внешних ресурсов для поддержания деятельности всей банковской системы. Анализ исторических аспектов развития банковских систем показывает, что для того, чтобы достичь данное состояния в количественном и качественном отношении требуются регулирование и управление.

Необходимость укрепления финансовой системы становится проблемой, которая привлекает все большее внимание во всем мире. Относительно недавно Базельский комитет банковского надзора и Международный расчетный банк, а также Международный валютный фонд

искали пути укрепления финансовой стабильности в глобальном масштабе.

Основной мировой тенденцией в развитии банковского надзора является повышение его эффективности. Под повышением эффективности, с точки зрения автора, подразумевается лучшее выполнение его основных задач без пропорционального увеличения ресурсов, выделяемых на эти цели. Эту тенденцию можно охарактеризовать как повышение производительности банковского сектора. Это подтверждается следующими изменениями в системе банковского надзора:

1) совершенствование организационной структуры институтов банковского надзора. Здесь необходимо указать на переход от принципов универсализма и функциональной однородности к принципам функциональной и производственной специализации подструктур, а также развитие подчиненных звеньев в структуре;

2) улучшение взаимодействия между внутренним и внешним банковским аудитом, которое представляет собой важный инструмент в обеспечении стабильности банков;

3) совершенствование инструментов надзора. Основными составляющими этого направления являются:

- совершенствование методики анализа и оценок (использование стресс-тестирования, моделирующего процесс, т.е., оценка стабильности системы при определенных неблагоприятных условиях эксплуатации), а также переход от оценки уровня определенных рисков к комплексной оценке качества управления рисками);

- создание организационных условий, обеспечивающих эффективное принятие оптимальных решений.

- повышение квалификации персонала.

4) Переход от экстенсивной модели надзора к интенсивной. Это выражается в спецификации объекта наблюдения. Модель интенсивного надзора основана на методологиях, направленных на определение областей повышенного риска в деятельности кредитных организаций и концентрация надзорных ресурсов в этих областях.

Этот подход получил название надзора, основанного на оценке рисков.

Нет общего согласия относительно наиболее подходящего определения риска для экономистов, финансовых специалистов, специалистов по теории принятия решений и теоретиков страхования. В результате в разных областях рассматриваются разные типы рисков и, соответственно, разные методы управления рисками. В бизнесе четырьмя основными общими типами риска могут быть признаны: стратегические, рыночные, кредитные и операционные риски. В проведенном исследовании анализируются актуальные вопросы управления операционными рисками, связанные с применением информационных технологий.

Дадим краткий обзор литературы по рассматриваемой проблеме. Современная концепция стратегии была определена в XX веке Дж. Фон Нейманом и О. Моргенштерном. Согласно этим авторам, стратегия - это набор действий фирмы, который определяется конкретной ситуацией. Позже понятие стратегии было уточнено, например, путем определения ее как модели планов, политики, задач, задач и возможностей, предназначенных для достижения ранее определенных целей.

Первая литература, посвященная стабильности системы коммерческих банков и управлению стабильностью, появилась только во второй половине XX века, и ее появление было связано с концом Бреттон-Вудской системы. Экономические исследования второй половины XX века рассматривали проблемы достижения и поддержания стабильного экономического равновесия. Теоретические аспекты стабильности банковской системы были отражены в академических исследованиях G. Schinasi [10], Дж. Синки [5], а также в работе, проделанной Международным Валютным фондом и Европейским центральным банком.

Особенно актуальным является вопрос о том, какие факторы влияют на стабильность банковской системы. Первое эмпирическое исследование, в котором анализировались взаимосвязи между условиями финансового сектора и экономическим ростом, показало, что существует взаимосвязь между экономическим и финансовым развитием [7, 9].

Однако вопрос о причинно-следственной связи между уровнем экономического и финансового развития остается открытым. Бойд и Хонохан, например, рассмотрели влияние инфляции на финансовый рынок и показатели финансового сектора [6, 8].

В соответствии с Базель II «Международная конвергенция измерения капитала и стандартов капитала: новые подходы», который был принят в 2004г. Базельским комитетом по банковскому надзору и содержащим методические рекомендации в области банковского регулирования, выделяются следующие категории топов событий операционного риска, представленные на рисунке 1.

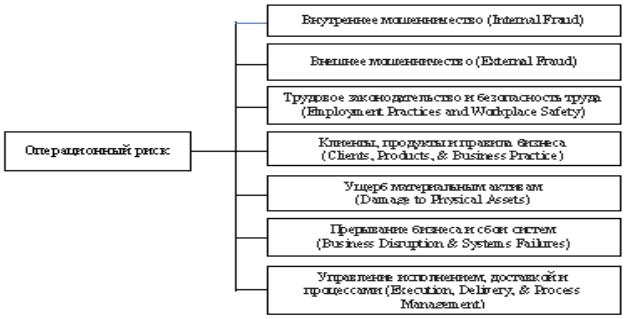

Рис. 1 Категории операционных рисков

В рамках данной статьи рассматриваются следующие документы по управлению операционными рисками: Базель II, Базель III, Закон Сарбейнса-Оксли, Разъяснения Банка России от 25.04.2022 № 716-Р-2021/63 «Рекомендации по осуществлению оценки эффективности системы управления операционным риском.

Международная конвергенция измерения капитала и стандартов капитала («Международная конвергенция измерения капитала и стандартов капитала: новые подходы» Базель II (New Capital Accord Basel II) [3], а также содержащая методические рекомендации в области банковского регулирования третья часть Базельского соглашения были разработаны в ответ на недостатки в финансовом регулировании, выявленные финансовым кризисом конца 2000-х годов. Базель III «Завершение посткризисных реформ» («Basel III: Finalising post-crisis reforms») усиливает требования к капиталу банка и вводит новые нормативные требования по ликвидности [4]. Главной целью соглашения «Базель III» является повышение качества управления рисками в банковском деле, что, в свою очередь, должно укрепить стабильность финансовой системы в целом. Для этого должны быть внедрены современные технологии управления рисками. Новое соглашение о капитале Базель III претендует на кардинальную модернизацию банковских информационных систем. Новые требования Базеля II Соглашения о капитале, которые могут соответствовать операционному управлению ИТ-рисками, могут быть перечислены следующим образом:

- управление ИТ-рисками: совет директоров должен осознавать необходимость системы управления операционными рисками; разрабатывать политику, процессы и процедуры для управления операционным риском; выявлять и оценивать операционный риск; регулярно отслеживать профили операционных рисков и существенную подверженность убыткам; иметь политику, процессы и процедуры для контроля и/или смягчения существенные операционные риски; иметь структуру для выявления, оценки, мониторинга и контроля снижения существенных операционных рисков;

- внутренний ИТ-аудит: система управления операционными рисками подлежит эффективному и всестороннему внутреннему аудиту; проводить регулярные независимые оценки политики банка, процедур и практик, связанных с операционным риском;

- обеспечение непрерывного ИТ-обслуживания: иметь планы на случай непредвиденных обстоятельств и обеспечения непрерывности бизнеса;

ИТ-обеспечение менеджмента компании: обеспечить достаточное публичное раскрытие информации.

Закон о реформе бухгалтерского учета в публичных компаниях и защите инвесторов (Закон Сарбейнса-Оксли) подчеркивает тот факт, что эффективность системы внутреннего контроля напрямую зависит от эффективности системы контроля деятельности в области ИТ [2]. Внешний аудит денежно-кредитных и финансовых учреждений охватывает их финансовые отделы, ИТ-инфраструктуру, внутренние ИТ-процессы. Закон Оксли также определяет некоторые требования к обеспечению управления ИТ, которые должны быть выполнены руководством высшего уровня денежно-кредитных и финансовых учреждений:

- регулярные проверки точности и полноты финансовых отчетов (статья 302);

- регулярные обзоры эффективности системы оценки внутреннего контроля и отчетности, включая внешний аудит (статья 404);

- составление регулярной отчетности о любых существенных фактах и рисках, которые могут повлиять на финансовые показатели (статья 409).

Следует отметить, что статья 404 «Оценка руководством системы внутреннего контроля» («Management assessment of internal controls») оказывает наибольшее влияние на управление ИТ; в этой статье подчеркивается постоянное процедуры совершенствования корпоративной информационной системы, основанные на эффективности системы внутреннего контроля. В соответствии с этой статьей Закона Сарбейнса-Оксли высшее руководство должно:

- указать ответственность руководства за создание и поддержание адекватной системы внутреннего контроля;

- содержать оценку эффективности внутреннего контроля.

Как и вышеупомянутые документы,

разъяснение Банка России от 25.04.2022 № 716-Р-2021/63 «Рекомендации по осуществлению оценки эффективности системы управления операционным риском» (вместе с «Рекомендациями по осуществлению оценки эффективности системы управления операционным риском в кредитной организации (головной кредитной организации банковской группы)») [1], не определяют определенных требований к ИТ. Тем не менее, эти рекомендации указывают на необходимость системы управления операционными рисками и регулярной оценки операционных рисков, которые могут быть получены с помощью эффективной системы управления ИТ и контроля. Таким образом, требования, которые могут соответствовать операционному управлению ИТ-рисками, следующие:

- осуществление управления такими операционными рисками, которые связаны с несанкционированным внешним доступом к информационным ресурсам и ненадлежащим обращением с конфиденциальной информацией клиентов;

- понимание ответственности высшего руководства финансового учреждения за разработку системы контроля операционных рисков и контроль эффективности методов управления операционными рисками;

- обеспечение регулярного выявления и оценки операционных рисков.

Обобщая вышесказанное, можно предложить две гипотезы в отношении взаимосвязи управления операционными рисками и эффективностью деятельности финансовых институтов:

1) Управление операционными рисками повышает стабильность финансовых институтов.

2) Утечка внутренней информации и злоупотребление ею стали одним из наиболее важных факторов, влияющих на управление операционными рисками и контроль в финансовых учреждениях.

Систематизация источников операционных рисков, которые влияют на информационные и технологические активы, имеет решающее значение, поскольку их внедрение может оказать влияние на конфиденциальность, доступность и целостность этих активов. Все источники рисков можно разделить на четыре основных класса:

1) действия человека,

2) сбои программного и аппаратного обеспечения,

3) слабые стороны внутренних процессов;

4) внешние события.

Каждый класс разделен на подклассы и отдельные элементы (таблица 1).

Таблица 1

Источники операционных рисков

Действия человека	Сбои программного и аппаратного обеспечения	Слабые места во внутренних процессах	Внешние события
Непреднамеренные действия: - ошибка; - невежество; - несоблюдение.	Отказы оборудования: - нехватка мощностей; - недостаточная производительность; - неправильное техническое обслуживание; - устаревание оборудования.	Процесс проектирования и внедрения: - неадекватный процесс; - ненадлежащее документирование процесса; - отсутствие понимания роли и обязанности; - неадекватное уведомление и предостережение; - неверные информационные потоки; - ненадлежащая эскалация проблем; - отсутствие соглашений об уровне обслуживания - проблемы с неэффективной передачей.	Бедствия: - погодные условия - пожар - наводнение - землетрясение - карантин.
Преднамеренные действия: - злоупотребление; - мошенничество; - саботаж; - кража; - вандализм.	Сбои программного обеспечения: - несовместимость неправильное; - управление конфигурацией; - неправильное управление изменениями; - неправильные настройки безопасности;	Управление технологическим процессом: - отсутствие мониторинга; - отсутствие показателей; - отсутствие периодического обзора; - ненадлежащий процесс владения.	Юридические проблемы: - неадекватность изменений в законодательстве; - судебный процесс.

	- небезопасные методы программирования; - неправильное тестирование.		
			Зависимости от служб: - проблемы со снабжением; - зависимость от экстренных служб; - транспортные проблемы.

Внутренние правонарушения остаются одной из наиболее актуальных проблем для риск-менеджеров в бизнес-секторе. Экономические колебания могут привести к большому мошенничеству или неправомерному использованию, и как только сотрудники окажутся под финансовым давлением, они могут столкнуться с искушением украсть информацию или злоупотребить ею для проведения выгодных торговых сделок с этой информацией, обеспечивая, таким образом, хорошую прибыль для себя, с одной стороны, и ставя под угрозу ИТ-безопасность в целом и безопасность бизнес-данных в частности, с другой.

До тех пор, пока национальная экономика остается вялой из-за высокого уровня безработицы, мошенничество с информационной безопасностью будет оставаться серьезной проблемой. Также полезно помнить, что обычно на раскрытие уже проведенного мошенничества уходит 2-3 года, а это значит, что злоупотребления, имевшие место в разгар кризиса 2008-2009 годов, будут выявлены только сейчас.

За предыдущие пять лет наблюдался быстрый и неуклонный рост случаев подтасовки внутренней информации и ее неправильного использования. В конце 2020 года он вырос на 52%. Также следует отметить, что наблюдается рост действий, совершаемых недобросовестными сотрудниками, направленных на преодоление современных систем защиты от кражи данных, осуществляющие несколько небольших передач данных вместо одной большой, что делает использование упомянутых систем практически бесполезным. Также доступные приложения для кражи данных теперь можно получить через Интернет. Недавно такие приложения стали доступны в виде комплектов, что упрощает их использование даже непрофессионалами. Кроме того, устройства хранения данных, такие как телефоны, флеш-носители, плееры и т.д., в настоящее время используются практически всеми ежедневно, что делает их идеальной средой для новых типов заражений и потери информации.

Типичными атаками с использованием стандартных аппаратных и программных средств являются:

- вредоносный код, такой как вирусы и черви;
- несанкционированный доступ к критически важным для бизнеса данным компании;
- несанкционированное изменение и передача этих данных другим людям.

Можно выделить три уровня сетевой защиты для решения проблемы сетевой безопасности банковских систем:

- уровень физической защиты: на этом уровне контролируется физический доступ к инфраструктуре банковских систем и другое сетевое оборудование;
- внутрифирменный уровень: на этом уровне регулируется доступ персонала к определенной информации;
- внешний уровень: на этом уровне определяются корпоративные информационные ресурсы и технологии, к которым может получить доступ внешний пользователь сети, например, заказчик.

Примеры корпоративного подхода к решению проблем по управлению операционными рисками представлены в таблице 2.

Таблица 2

Корпоративный подход к управлению рисками

Внутренний контроль	Неправильное использование элементов управления	Система и контроль данных
Внутренние политики	Профилактика	Политическая основа
Образование	Обнаружение	Управление уязвимостями и соответствие
Практика найма	Восстановление	Управление доступом
Безопасная аутентификация	Судебная экспертиза	
Модели		

защиты ИТ-системы банка от возможных атак. В дополнение к брандмауэрам системы обнаружения неправомерных действий могут предоставлять дополнительные возможности для систем, борющихся с возможным мошенничеством, расширять возможности системного администратора по обеспечению информационной

безопасности и способствовать обеспечению полноты информационной безопасности в трех основных аспектах информационной безопасности.

Профилирование поведения конечного пользователя является наиболее важным аспектом защиты данных с упором на операционные риски. Кроме того, не менее важным аспектом является программная и сетевая активность, так как этот метод эффективен при обнаружении внешних атак, которые составляют почти две трети безопасности корпоративной системы. В информационных системах на основе операционных систем UNIX или Linux, последовательности команд оболочки представляют собой легко собираемую и анализируемую информацию, тем самым являясь исходным материалом для создания профилей конечных пользователей. С другой стороны, принимая во внимание разницу между поведением end-пользователей, построение профилей их активности является более сложной задачей по сравнению с построением профиля поведения программы. Хакеры могут даже попытаться адаптировать свое поведение, чтобы обмануть системы IDS.

В последние годы большая часть исследовательской деятельности в области выявления злоупотреблений и мошенничества сосредоточена на изучении поведение конечных пользователей и создание их профилей на основе файлов журнала системных вызовов. До сих пор простым и широко используемым методом обнаружения неправильного использования, является мониторинг системных вызовов, инициируемых активными и привилегированными процессами используемой системы.

Профиль нормального поведения конечного пользователя строится путем перечисления всех уникальных системных вызовов, которые наблюдаются в данных журнала и считаются ежедневными нормальными, в свою очередь, ранее неопределенные последовательности считаются ненормальными. Этот подход был расширен различными другими методами. Было предложено использовать подход интеллектуального анализа данных для изучения выборок системных вызовов и построения небольшого набора правил, содержащихся в обычных данных. Во время мониторинга и обнаружения последовательностей, которые нарушают эти правила, необходимо рассматривать как аномалии и неправильное использование.

Обобщим полученные выводы. Как ранее уже отмечалось, количество случаев кражи и неправильного использования внутренней информации выросло более чем на 50%. Очевидно, что, принимая во внимание этот факт, можно согласиться с гипотезой данной статьи, что скрытие внутренней информации и злоупотребление ею стали одним из наиболее важных факторов, влияющих на управление операционными рисками и контроль в финансовых учреждениях. В настоящее время большая часть мероприятий по управлению рисками, в частности, во всех типах финансовых учреждений, сосредоточена именно на предотвращении внутренних инцидентов и случаев мошенничества и борьбе с ними.

Также следует отметить, что успешное управление рисками (все виды рисков должны приниматься во внимание: как ИТ-риски, так и различные операционные риски) резко оптимизирует текущие расходы учреждений, тем самым увеличивая общую финансовую эффективность, а также стабильность финансовых институтов. Вышеизложенное приводит к выводу, что можно принять и первую гипотезу статьи.

Результаты анализа систем обнаружения неправильного использования ИТ-системы банка показали, что доступные в настоящее время системы могут помочь использовать так называемый метод профилирования поведения конечного пользователя, особенно в информационных системах, основанных на UNIX и Linux, где последовательности команд оболочки являются легко собираемой и анализируемой информацией, являясь при этом исходным материалом для создания профилей конечных пользователей. Таким образом, в качестве дополнения к брандмауэрам системы обнаружения неправомерных действий можно предоставить дополнительные возможности для систем, борющихся с возможным мошенничеством, расширить возможности управления операционными рисками командами для обеспечения информационной безопасности и содействия полноте информационной безопасности в трех основных аспектах информационной безопасности.

Библиографический список

1. Российская Федерация. Банк России. Рекомендации по осуществлению оценки эффективности системы управления операционным риском» (вместе с «Рекомендациями по осуществлению оценки эффективности системы управления операционным риском в кредитной организации (головной кредитной организации банковской группы)»): Разъяснение Банка России «Рекомендации по осуществлению оценки эффективности системы управления операционным риском» (вместе с «Рекомендациями по осуществлению оценки эффективности системы управления операционным риском в кредитной организации (головной кредитной организации банковской группы)») от 25.04.2022 № 716-Р-2021/63. - URL: https://www.consultant.ru/document/cons_doc_LAW_415759/

2. Закон Сарбейнза — Оксли Закон о реформе бухгалтерского учета публичных компаний и защите инвесторов. - URL: http://www.sarbanes-oxley-101.com/

3. Базельский комитет по банковскому надзору: Базель II Международная конвергенция измерения капитала и стандартов капитала: новые подходы. - URL: https://www.bis.org/publ/bcbsca.htm

4. Базельский комитет по банковскому надзору: Базель III Завершение посткризисных реформ. - URL: // https://www.bis.org/bcbs/publ/d424.htm

5. Синки, Дж. Финансовый менеджмент в коммерческом банке и в индустрии финансовых услуг / Д. Синки — «Альпина Диджитал», 2002 – 112с.

6. Boyd, H., Smith, D. The Impact of Inflation on Financial Market Performance. // Journal of Monetary Economics. 2000. N 2. pp. 221-248.

7. Goldsmith, R.M. Financial Structure and Development/ R.M. Goldsmith. - Yale University Press, 1969. – 561p.

8. Honohan, P. ― The Accidental Tax: Inflation and the Financial Sector.‖ In Taxation of Financial Intermediation, Theory and Practice for Emerging Economies, edited by P. Honohan . Washington DC: World Bank Publications and Oxford University Press, 2003. pp. 381–420

9. McKinnon, R. Money and Capital in Economic Development/ R. McKinnon. – Brooking, 1973. – 184p.

10. Schinasi, G. Defining Financial Stability 2004. - URL: // https://www.imf.org/external/pubs/ft/wp/2004/wp04187.pdf

References

1. Rossijskaya Federaciya. Bank Rossii. *Rekomendacii po osushchestvleniyu ocenki effektivnosti sistemy upravleniya operacionnym riskom» (vmeste s «Rekomendaciyami po osushchestvleniyu ocenki effektivnosti sistemy upravleniya operacionnym riskom v kreditnoj organizacii (golovnoj kreditnoj organizacii bankovskoj gruppy)»): Raz"yasnenie Banka Rossii «Rekomendacii po osushchestvleniyu ocenki effektivnosti sistemy upravleniya operacionnym riskom» (vmeste s «Rekomendaciyami po osushchestvleniyu ocenki effektivnosti sistemy upravleniya operacionnym riskom v kreditnoj organizacii (golovnoj kreditnoj organizacii bankovskoj gruppy)»)* ot 25.04.2022 N 716-P-2021/63 - - URL: https://www.consultant.ru/document/cons_doc_LAW_415759/

2. *Zakon Sarbejnza — Oksli Zakon o reforme buhgalterskogo ucheta publichnyh kompanij i zashchite investorov*. - URL: http://www.sarbanes-oxley-101.com/

3. *Bazel'skij komitet po bankovskomu nadzoru: Bazel' II Mezhdunarodnaya konvergenciya izmereniya kapitala i standartov kapitala: novye podhody*. - URL: https://www.bis.org/publ/bcbsca.htm

4. *Bazel'skij komitet po bankovskomu nadzoru: Bazel' III Zavershenie postkrizisnyh reform*. - URL: // https://www.bis.org/bcbs/publ/d424.htm

5. Sinki, Dzh. *Finansovyj menedzhment v kommercheskom banke i v industrii finansovyh uslug*. / Dzh. Sinki — *Al'pina Didzhital*, 2002. 112p. – Text : unmediated

6. Boyd, H., Smith, D. *The Impact of Inflation on Financial Market Performance*. // *Journal of Monetary Economics*. 2000. N 2. pp. 221-248. – Text : unmediated

7. Goldsmith, R.M. *Financial Structure and Development.*/ R.M. Goldsmith - Yale University Press, 1969. 561p. - – Text : unmediated

8. Honohan, P. *The Accidental Tax: Inflation and the Financial Sector.‖ In Taxation of Financial Intermediation, Theory and Practice for Emerging Economies*, edited by P. Honohan . Washington DC: World Bank Publications and Oxford University Press, 2003. pp. 381–420. – Text : unmediated

9. McKinnon, R. *Money and Capital in Economic Development.*/ R. McKinnon. – *Brooking*, 1973. – 184p.

10. Schinasi, G. *Defining Financial Stability* 2004. - URL: // https://www.imf.org/external/pubs/ft/wp/2004/wp04187.pdf

NEW TRENDS IN OPERATIONAL RISK MANAGEMENT AND CONTROL IN FINANCIAL INSTITUTIONS

Elena A. Kasyuk

candidate of economic Sciences, associate Professor of full-time studies at the Siberian Institute of business and information technology

Abstract: The article discusses the issue of current trends in the management and control of operational risk in financial institutions. The purpose of the article is to identify the main trends in the management and control of operational risk in financial institutions, the knowledge of which will make it possible to make effective management decisions to minimize operational risks, including through the misuse of IT systems.

The research is carried out on the basis of theoretical methods of study, generalization and analysis. The basis of the work is the fundamental works of domestic and foreign authors on banking risk management and internal control.

Currently, financial institutions understand the great impact of effective risk management on profit opportunities. Thus, risk management has become an important part of financial instruments. According to recent studies, there are still problems associated with managing various types of risks. For example, the Basel Committee on Banking Supervision of the Bank for International Settlements calls on financial institutions to pay closer attention to operational risk management issues. Due to the increased intensity of financial transactions, financial institutions have become very

vulnerable to operational risks. In many cases, a high level of operational risks is caused by failures of IT systems. Taking into account this fact, we can agree that the concealment of internal information and its abuse have become one of the most important factors affecting the management of operational risks in financial institutions. Currently, most of the risk management activities, in particular, in all types of financial institutions, are focused specifically on preventing and combating internal incidents and fraud.

In conclusion, the article proposes measures to reduce operational risk, including those aimed at reducing possible fraud, for example, expanding the ability of operational risk management teams to ensure information security and promote the completeness of information security in three main aspects of information security.

Key words: stability, banking system, operational risks, operational risk management, operational risk control, information technology

Сведения об авторе:

Касюк Елена Анатольевна - кандидат экономических наук, доцент факультета очного обучения АНОО ВО «Сибирский институт бизнеса и информационных технологий» (СИБИТ) (644016, Российская Федерация, г. Омск, ул. 1-я Автомобильная, д.5, кв.28, e-mail: kasyuk_ok@bk.ru).

Статья поступила в редакцию 24.02.2023