Банк России

МАТЕРИАЛЫ ЗАСЕДАНИЯ ЭКСПЕРТНОГО СОВЕТА ПО РЕГУЛИРОВАНИЮ, МЕТОДОЛОГИИ ВНУТРЕННЕГО АУДИТА, ВНУТРЕННЕГО КОНТРОЛЯ И УПРАВЛЕНИЯ РИСКАМИ В БАНКЕ РОССИИ И ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ ОТ 18 ДЕКАБРЯ 2024 ГОДА

Москва
2025

СОДЕРЖАНИЕ

Материал подготовлен службой главного аудитора Банка России.

Ответственные за выпуск: Н.А. Станик, М.А. Лауфер

Комментарии, предложения и замечания можно направлять по адресу: expert.board@mail.cbr.ru.

Фото на обложке: Shutterstock/FOTODOM

107016, Москва, ул. Неглинная, 12, к. В

Официальный сайт Банка России: www.cbr.ru

ОБРАЩЕНИЕ К ЧИТАТЕЛЯМ

Уважаемые коллеги!

Представляем материалы заседания Экспертного совета по регулированию методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях, состоявшегося 18 декабря 2024 г. в Москве в очно-дистанционном формате. Мероприятие объединило более 200 экспертов из разных регионов России и стран СНГ, что позволило обменяться ценным опытом и обсудить актуальные вопросы.

В дайджесте освещены направления, важные для развития внутреннего аудита и управления рисками в условиях стремительной цифровизации и усложнения бизнес-процессов.

Среди них:

- *Раскрытие данных внешним пользователям: лучшие практики публикации информации с целью развития культуры этичного обращения с данными.*
- *Оценка цифровой зрелости: модели и методики измерения интеграции цифровых технологий в операционные процессы финансовых организаций.*
- *Обеспечение непрерывности бизнеса: стратегии поддержания стабильности операций в условиях современных вызовов, включая кибератаки и санкции.*
- *Инновационные методы внутреннего аудита: применение Code Mining для анализа исходного кода автоматизированных систем и повышения эффективности аудиторских проверок.*
- *Экосистемность на рынке финансовых услуг: тенденции формирования экосистем и связанные с ними риски, а также предложения по регулированию этого процесса.*
- *Интеграция киберрисков: методы включения киберугроз в общую систему управления рисками для обеспечения устойчивости и безопасности финансовых организаций.*

Надеемся, что данный дайджест будет полезен специалистам в области внутреннего аудита и управления рисками, а также руководителям финансовых организаций, стремящимся повысить эффективность своих процессов и укрепить устойчивость на фоне современных вызовов. Благодарим всех наших экспертов за активное участие и ценный вклад в обсуждение.

В.П. Горегляд
главный аудитор Банка России, председатель Экспертного совета по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях

ВСТУПЛЕНИЕ

Экспертный совет по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях при Банке России на заседании 18 декабря 2024 г. рассмотрел ряд ключевых вопросов, направленных на совершенствование практик внутреннего аудита, включая инновации во внутреннем аудите, управление данными, цифровую трансформацию, обеспечение непрерывности бизнеса и интеграцию киберрисков в систему управления рисками.

Раскрытие данных внешним пользователям

В рамках заседания было проведено исследование существующих российских и международных практик предоставления данных внешним пользователям с целью развития культуры этичного обращения с информацией. Уникальность исследования заключается в обобщении опыта различных организаций с учетом разнообразия их деятельности, применяемых методологий и инструментов, а также национальных особенностей выявления и управления рисками. Это позволило сформулировать рекомендации по прозрачному и ответственному раскрытию информации, что способствует укреплению доверия между организациями и их внешними стейкхолдерами.

Модель оценки цифровой зрелости Банка России

В ходе исследования были рассмотрены практические аспекты проведения внутреннего аудита оценки цифровой зрелости Банка России, представлены результаты апробации методики и обозначена дальнейшая роль внутреннего аудита во взаимодействии с профильными подразделениями для периодической оценки и повышения уровня цифровой зрелости организации. Эти меры направлены на обеспечение эффективной адаптации к быстро меняющимся условиям цифровизации и управлению возникающими рисками.

Обеспечение непрерывности бизнеса в Группе «Московская Биржа»

В ходе заседания были обсуждены ключевые элементы организации процессов обеспечения непрерывности бизнеса, включая системный подход к оценке и регулярный аудит, а также три основных направления оценки: организация процесса, ИТ-архитектура и ИТ-инфраструктура. Обсуждены актуальные вызовы, такие как кибератаки и санкционное давление, подчеркнута необходимость привлечения внешней экспертизы для повышения надежности ИТ-систем и инфраструктуры, а также важность квалификации внутренних аудиторов для эффективного управления непрерывностью бизнеса. Приведены результаты комплексной оценки, проведенной за последние 5 лет, и рекомендации по улучшению процессов. Обсуждается роль внутреннего аудита во взаимодействии с профильными подразделениями для обеспечения эффективного управления непрерывностью бизнеса.

Инновации во внутреннем аудите: Code Mining

Представлен инновационный подход в использовании методов Code Mining в деятельности аудиторов для проверки бизнес-процессов. Code Mining представляет собой анализ исходного кода цифрового бизнес-процесса и может применяться для подтверждения идентифицированных проблем, а также для обнаружения новых инсайтов. Одним из решений при реализации Code Mining может быть использование больших языковых моделей, например GigaChat, которые способны объяснить логику кода, проанализировать его структуру и выявить ошибки. Применение Code Mining открывает аудиторам перспективные возможности для анализа цифрового оригинала бизнес-процесса, установления корневых причин отклонений и повышения скорости и качества аудита.

Построение функции внутреннего аудита в Группе «Аэрофлот»

В ходе заседания было рассмотрено построение эффективной функции внутреннего аудита в Группе «Аэрофлот» в контексте риск-ориентированного планирования и использования карты гарантий. Описана нормативно-правовая основа, регулирующая деятельность внутреннего аудита в России, включая ключевые федеральные законы и методические рекомендации. Анализируются нововведения, касающиеся ежегодного заключения внутреннего аудита для акционеров, а также создание подкомитета по внутреннему аудиту в Росстандарте. Рассматриваются подходы к риск-ориентированному планированию, включая инструменты риск-анализа, карты рисков и поставщиков гарантий. Представлены шаги по оценке и актуализации карты гарантий, что позволяет выявить пробелы и дублирование в обеспечении уверенности. В заключение описываются практические инструменты адаптации работы внутреннего аудита с учетом внешних и внутренних факторов.

Развитие экосистемности на рынке финансовых услуг

Обсуждены актуальные вопросы развития экосистемности на рынке финансовых услуг, включая особенности экосистем и развитие встроенных финансов на платформах экосистем. Под экосистемой понимается партнерство организаций (включая кредитные, страховые и иные финансовые организации), осуществляющих деятельность на основе цифровых платформ, интернет-сервисов, аналитических и информационных систем для реализации продуктов и оказания услуг. В выступлении отражены внутренние и внешние противоречия функционирования экосистем на рынке финансовых услуг, а также макроэкономические и микроэкономические эффекты их развития. Развитие финансовых услуг в экосистемах происходит по принципу встраивания. Встроенные финансовые услуги пока в большей части находятся вне регуляторного поля, что создает дополнительные риски для потребителей. Экосистемность на рынке финансовых услуг, являясь позитивным трендом экономического развития, может генерировать серьезные риски, требующие особого регулирования. Представленные предложения по регулированию экосистем могут стать основой для совершенствования законодательства в данной области.

Модель трех линий защиты[1] и переход к четырем линиям с интеграцией внешних аудиторских функций

Рассмотрено взаимодействие между компонентами четырех линий защиты: взаимодействие между советом директоров и первыми двумя линиями, слаженность их кооперации с внутренним аудитом и динамика долгосрочной прибыли от привлечения внешних акторов. Для этого использовались вариации фундаментальных моделей теории игр, позволяющие анализировать возникающие внутри корпоративной структуры конфликты, подходы к их разрешению и выгоды от синергии – как на примере конкретных бизнес-подразделений, так и на уровне функционирования кредитной организации в рыночной системе.

[1] Модель трех линий защиты является ключевой концепцией управления рисками и внутреннего контроля в организации. Она включает:
- **Первая линия:** операционные подразделения, которые несут ответственность за управление рисками в своей зоне деятельности. Они реализуют основные процессы и контролируют риски на уровне исполнения.
- **Вторая линия:** функции управления рисками и обеспечения соответствия (compliance), которые разрабатывают методологии, политики и процедуры для поддержки первой линии. Эти функции контролируют выполнение стандартов и нормативных требований.
- **Третья линия:** внутренняя аудиторская служба, которая проводит независимые проверки и предоставляет объективные оценки эффективности управления рисками и контроля.

Интеграция киберрисков в систему управления рисками

Особое внимание уделено интеграции киберрисков в систему управления рисками финансовых организаций. В условиях увеличения количества кибератак и их сложности важно эффективно идентифицировать и оценивать киберугрозы, управлять ими. Обсуждены методы и инструменты, позволяющие финансовым организациям минимизировать потенциальные убытки и укрепить информационную безопасность. Подчеркнута необходимость комплексного подхода к управлению киберрисками, включающего их идентификацию, анализ, разработку стратегий управления и постоянный мониторинг эффективности принятых мер. Киберриски необходимо рассматривать в структуре общего ландшафта рисков компании для обеспечения взвешенных решений и прозрачности процесса принятия решений руководством.

Целью представленных материалов является обмен опытом и разработка конкретных рекомендаций по совершенствованию практик внутреннего аудита и управления рисками в условиях цифровизации и современных вызовов.

О.В. ВАГАНОВА
Начальник отдела аудита операций Банка России на финансовых рынках, Департамент внутреннего аудита Банка России

ОБЗОР ОПЫТА ПУБЛИКАЦИИ (РАСКРЫТИЯ) ДАННЫХ ВНЕШНИМ ПОЛЬЗОВАТЕЛЯМ

Аннотация

Проведено исследование существующих российских и международных практик предоставления данных внешним пользователям в целях развития культуры этичного обращения с данными[1]. Уникальность исследования заключается в обобщении международного и российского опыта раскрытия данных внешним пользователям, полученного от различных респондентов, с учетом многообразия направлений их деятельности, широты применяемых методологий и инструментов предоставления данных внешним пользователям, национальных особенностей выявления и управления рисками.
Ключевые слова: раскрытие данных внешним пользователям; оценка риска раскрытия данных; реализация концепции открытости данных; порталы данных.
Коды JEL: L20; M37; F63; G41.

Одной из задач Банка России является создание технологий и сервисов по предоставлению данных внешним пользователям для исследовательских и аналитических целей с учетом совершенствования процессов категоризации данных, методов защиты и снижения рисков раскрытия информации ограниченного доступа.

В целях изучения существующих российских и международных практик предоставления данных внешним пользователям и развития культуры этичного обращения с данными[2] во втором полугодии 2023 г. проведено анкетирование государственных органов исполнительной власти Российской Федерации, финансовых и иных организаций, иностранных регуляторов, а также самостоятельное исследование 31 официального интернет-сайта иностранных регуляторов[3] в двух наиболее востребованных пользователями бизнес-областях – «Платежи и переводы» и «Инвестиционные фонды» с определением единого глоссария понятий и сущностей. В анкетировании приняли

---

1 Культура этичного управления данными – совокупность ценностей, норм, практик и поведения внутри организации, направленных на ответственное и этически обоснованное обращение с данными. Она включает обеспечение прозрачности в сборе, хранении и обработке данных, защиту конфиденциальности информации, получение согласия субъектов данных, ответственность за соблюдение этических стандартов, постоянное обучение и повышение осведомленности сотрудников, а также соблюдение применимых законодательных и нормативных требований. Культура этичного управления данными способствует укреплению доверия между организацией и ее заинтересованными сторонами, минимизации рисков утечки информации и повышению общей репутации компании (примечание Редакционной коллегии).

2 Этичное обращение с данными подразумевает следование моральным принципам, к которым, в частности, относится стремление к достоверности.

3 Великобритания и Северная Ирландия, Германия, Испания, Италия, Мексика, Португалия, Турция, Франция, Чили, Аргентина, Бразилия, Индия, Индонезия, Китай, Саудовская Аравия, Южная Африка, ОАЭ, Армения, Азербайджан, Беларусь, Грузия, Казахстан, Таджикистан, Египет, Бахрейн, Пакистан, Вьетнам, Малайзия, Сингапур, Филиппины, Южная Корея.

участие **10 российских респондентов**: 6 членов Экспертного совета, 3 федеральных органа исполнительной власти (Федеральная служба государственной статистики, Федеральная налоговая служба, Министерство цифрового развития), Счетная палата Российской Федерации. Ответы на анкеты получены от **14 международных регуляторов**[4].

Уникальность исследования заключается в обобщении международного и российского опыта раскрытия данных внешним пользователям, полученного от различных респондентов, с учетом:
- многообразия направлений деятельности (организации, относящиеся к финансово-банковской сфере и прочие организации; государственные структуры);
- широты применяемых методологий и инструментов предоставления данных внешним пользователям;
- национальных особенностей выявления и управления рисками.

В ходе исследования всеми респондентами отмечена необходимость публикации внешней информации в целях обеспечения непротиворечивого и полного информирования клиентов / посетителей сайта о продуктах/услугах и деятельности организации. Публикуемые данные не должны вводить клиентов в заблуждение или формировать у них неправильные ожидания о продуктах/услугах.

Консолидируя полученные ответы, можно отметить, что процесс раскрытия информации практически у всех респондентов определен во внутренних документах. Условно его можно разделить на четыре этапа: подготовка; проверка/согласование/акцепт; принятие решения / санкционирование; раскрытие/публикация. Виды подразделений, участвующих в проверке и согласовании информации, и распределение функций между ними зависят от набора (спектра) раскрываемой информации, сферы деятельности организации и ее размеров.

Несмотря на схожесть в оценке чувствительности информации[5] для внешних пользователей, респонденты отметили тот факт, что уровень чувствительности данных к раскрытию часто зависит от конкретных обстоятельств и требует анализа со стороны организации и ее руководства. Отмечены возможности раскрытия конфиденциальной информации при соблюдении условий законодательства. Вопрос чувствительности данных к раскрытию решается также путем раскрытия анонимизированных (обезличенных) и, при необходимости, агрегированных данных.

Респонденты в ходе анкетирования в отношении публикации информации на официальном сайте отметили идентификацию основных рисков:
- риск введения клиентов в заблуждение;
- риск нарушения секретности;
- риск возможной недостаточности/недостоверности данных;
- риски, связанные с работой сайта (нефинансовые риски);
- регуляторный риск;
- правовой риск;
- репутационный риск.

Есть особенности в идентификации основных рисков, связанные с направлениями и целями деятельности организаций. Международные респонденты дополнительно отметили риски:
- некорректного использования данных внешними пользователями;
- неправильной интерпретации данных;
- риски, связанные с работой прикладных систем (целостность, доступность, полнота, секретность).

---

[4] Национальные банки Киргизии, Таджикистана, Беларуси, Казахстана, а также регуляторы Бахрейна, Египта, Пакистана, Вьетнама, ОАЭ, Филиппин, Южной Кореи, Аргентины, Бразилии, Азербайджана.

[5] В ходе анкетирования респондентами выделялись следующие категории данных по уровню чувствительности к раскрытию: информация, чувствительная к санкционным ограничениям; отдельные сведения о финансово-хозяйственной деятельности; информация о членах органов управления и об аффилированных лицах; персональные данные; государственная тайна; коммерческая тайна; банковская тайна; конфиденциальная информация.

Риски митигируются респондентами в соответствии с утвержденными внутренними документами и внешними рекомендациями (COSO ERM[6], ISO 31000[7], ISO/IEC 27001[8]) путем установления требований к составу информации, автоматизации процесса проверки информации, ограничения доступа, выстраивания системы согласования материалов, планируемых к публикации для внешних пользователей. Внутренний контроль выстроен с учетом их организационной структуры, направлений деятельности и достижения ими поставленных целей.

Также хотелось бы отметить достижение федеральных органов исполнительной власти в реализации концепции открытости[9], целью которой является повышение прозрачности и подотчетности государственного управления, расширение возможностей непосредственного участия гражданского общества в процессах разработки и экспертизы решений. В рамках национальной программы «Цифровая экономика Российской Федерации» создана национальная система управления данными как совокупность нормативных правовых, организационных, методологических правил, процедур и информационных систем: Федеральная государственная информационная система «Единая информационная платформа национальной системы управления данным» и иные информационно-технологические элементы; цифровая аналитическая платформа предоставления статистических данных. Счетная палата Российской Федерации запустила специальный проект – портал-агрегатор «Госрасходы» с целью информирования пользователя о направлениях бюджетных средств на национальные проекты. Оценка уровня удовлетворенности пользователей внешними данными проводится федеральными органами исполнительной власти путем опросов референтных групп и общественных советов.

В ходе исследования также отмечено, что сайты международных регуляторов отдельных стран содержат ссылки на единые порталы данных, представляющих собой каталоги информации (в том числе статистические данные), сгруппированной по различным показателям, позволяющим пользователям находить интересующие их наборы данных, понимать их структуру и ограничения, а также получать доступ к интересующим данным. Аналитический инструмент или программное обеспечение дает пользователю возможность программировать доступ к информации через размещенный на портале URL-адрес, по которому расположена интересующая информация.

По итогам анкетирования в целом можно сделать вывод, что процесс раскрытия информации внешним пользователям формализован и организован с учетом их индивидуальных особенностей функционирования и сферы деятельности.

Активному участию гражданского общества в анализе данных и развитии инноваций в финансово-банковском секторе Российской Федерации в дальнейшем будет способствовать:

- развитие онтологического единства данных на основе концептуальной модели данных, содержащей основные понятия (сущности) управления данными;
- совершенствование нормативно-правовой, методологической базы (включая формирование единых требований к управлению данными) и унификации требований к управлению внешними данными;
- дальнейший рост информационно-технологического обеспечения управления данными.

---

[6] Стратегия управление рисками предприятия Комитета спонсорских организаций Комиссии Тредвея (примечание Редакционной коллегии).

[7] Международный стандарт ISO 31000 по управлению рисками (примечание Редакционной коллегии).

[8] Международный стандарт ISO/IEC 27001 по системе управления информационной безопасностью (примечание Редакционной коллегии).

[9] Утверждена распоряжением Правительства Российской Федерации от 30.01.2014 № 93-р в целях реализации Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы.

Список источников

1. DAMA-DMBOK: Свод знаний по управлению данными. М.: Олимп-Бизнес, 2020.
2. Хартия открытых данных «Группы восьми». Июнь 2013. URL: https://www.minfin.gov.ru/.
3. Хафф Д. Как лгать при помощи статистики, 1954. URL: https://www.litres.ru/book/darell-haff/.
4. Официальные сайты организаций:
   - Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России): https://digital.gov.ru;
   - Федеральная налоговая служба (ФНС России): http://nalog.gov.ru;
   - Федеральная служба государственной статистики (Росстат): http://rosstat.gov.ru;
   - Счетная палата Российской Федерации: https://ach.gov.ru.

5. Официальные сайты иностранных регуляторов:

Страна	Наименование регулятора	Адрес сайта
Азербайджан	Central Bank of Azerbaijan	https://www.cbar.az/
	State Committee for Securities	http://www.scs.gov.az/
Аргентина	Central Bank of Argentina (BCRA)	http://bcra.gov.ar/
	Securities and Stock Exchange Commission of Argentina (CNV)	https://www.cnv.gov.ar/
Армения	Central Bank of Armenia	https://www.cba.am/
Бахрейн	Central Bank of Bahrain	https://www.cbb.gov.bh/
Беларусь	Национальный банк Республики Беларусь	https://www.nbrb.by/
	Министерство финансов Республики Беларусь	http://www.minfin.gov.by/
Бразилия	Central Bank of Brazil	https://www.bcb.gov.br/
	Securities and Exchange Commission of Brazil (CVM)	http://www.cvm.gov.br/
Великобритания	Bank of England (BoE)	https://www.bankofengland.co.uk/
	Financial Conduct Authority (FCA)	https://www.fca.org.uk/
Вьетнам	State Bank of Vietnam	https://www.sbv.gov.vn/
	The Ministry of Finance	https://www.mof.gov.vn/
Германия	Deutsche Bundesbank	https://www.bundesbank.de/
	BaFin	https://www.bafin.de/
Грузия	National Bank of Georgia	https://www.nbg.gov.ge/
Египет	Central Bank of Egypt	https://www.cbe.org.eg/
	Financial Regulatory Authority	http://www.fra.gov.eg/
Индия	Reserve Bank	https://m.rbi.org.in/
	Securities and Exchange Board of India (SEBI)	https://www.sebi.gov.in/
Индонезия	Bank Indonesia (BI)	https://www.bi.go.id/
	Otoritas Jasa Keuangan (OJK) – Financial Services Authority	https://www.ojk.go.id/
Испания	Banco de España (BdE)	https://www.bde.es/
	Spanish Market Authority "Comisión Nacional del Mercado de Valores (CNMV)"	http://cnmv.es/

Страна	Наименование регулятора	Адрес сайта
Италия	Banca d'Italia	https://www.bancaditalia.it/
	CONSOB	http://www.consob.it/
Казахстан	National Bank of Kazakhstan	https://nationalbank.kz/
	Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan	https://finreg.kz/
Китай	People's Bank of China	http://www.pbc.gov.cn/
	China Securities Regulatory Commission (CSRC)	http://www.csrc.gov.cn/
Малайзия	Central Bank of Malaysia/ Bank Negara Malaysia	https://www.bnm.gov.my/
	Securities Commission Malaysia (SC)	https://www.sc.com.my/
Мексика	Banco de México	https://www.banxico.org.mx/
	National Banking and Securities Commission (CNBV)	https://www.gob.mx/cnbv
Объединенные Арабские Эмираты	Central Bank Of The UAE	https://www.centralbank.ae/
	Securities and Commodities Authority	https://www.sca.gov.ae/
Пакистан	State Bank of Pakistan	https://www.sbp.org.pk/
	Securities and Exchange Commission of Pakistan (SECP)	https://secp.gov.pk/
Португалия	Banco de Portugal	https://www.bportugal.pt/
	Comissão do Mercado de Valores Mobiliários	https://www.cmvm.pt/en/
Саудовская Аравия	Saudi Central Bank	http://www.sama.gov.sa/
	Capital Market Authority	https://cma.org.sa/
Сингапур	Monetary Authority of Singapore	https://www.mas.gov.sg/
Таджикистан	National bank of Tajikistan	https://nbt.tj/
	Министерство финансов Республики Таджикистан	https://www.minfin.tj/
Турция	Central Bank of the Republic of Turkey	http://www.tcmb.gov.tr
	Banking Regulation and Supervision Agency	https://www.bddk.org.tr/
	Capital Markets Board of Turkey	https://www.cmb.gov.tr/
Филиппины	Bangko Sentral ng Pilipinas (BSP)	https://www.bsp.gov.ph/
Франция	Banque de France	https://www.banque-france.fr/
	Autorité des Marchés Financiers	https://www.amf-france.org/
Чили	Central Bank of Chile	https://www.bcentral.cl/
	Financial Market Commission	https://www.cmfchile.cl/
Южная Корея	BOK (the Bank of Korea)	http://www.bok.or.kr/
	FSC (the Financial Services Committee)	https://fsc.go.kr/
	FSS (the Financial Supervisory Service)	https://english.fss.or.kr/
Южно-Африканская Республика	South African Reserve Bank	https://www.resbank.co.za/
	Financial Sector Conduct Authority (FSCA)	https://www.fsca.co.za/

6. Специальные порталы:
   - портал (открытых) данных Центрального банка Бразилии: https://dadosabertos.bcb.gov.br;
   - портал статистических данных Банка Италии: https://infostat.bancaditalia.it/;
   - сайт системы экономической статистики Банка Южной Кореи: https://ecos.bok.or.kr;
   - портал данных EasyData Государственного банка Пакистана: https://easydata.sbp.org.pk/;
   - статистический портал Банка Португалии: https://bpstat.bportugal.pt/;
   - портал «Электронная система распределения данных» Банка Турции: https://evds2.tcmb.gov.tr/.

7. Нормативные правовые акты:

Федеральные законы:
   - от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями);
   - от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» (с изменениями);
   - от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (с изменениями);
   - от 05.04.2013 № 41-ФЗ «О Счетной палате Российской Федерации» (с изменениями).

Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Постановления Правительства Российской Федерации:
   - от 02.06.2008 № 420 «О Федеральной службе государственной статистики» (с изменениями);
   - от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»;
   - от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;
   - от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» (с изменениями);
   - от 14.05.2021 № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» (с изменениями);
   - от 22.06.2021 № 956 «О государственной информационной системе «Цифровая аналитическая платформа предоставления статистических данных».

Распоряжения Правительства Российской Федерации:
   - от 06.05.2008 № 671-р «Об утверждении Федерального плана статистических работ» (вместе с Федеральным планом статистических работ) (с изменениями);
   - от 10.07.2013 № 1187-р «Об утверждении перечня общедоступной информации о деятельности федеральных государственных органов, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, размещаемой в информационно-телекоммуникационной сети «Интернет» в форме открытых данных»;
   - от 30.01.2014 № 93-р «Об утверждении Концепции открытости федеральных органов исполнительной власти»;
   - от 03.06.2019 № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожной карты») по созданию национальной системы управления данными на 2019–2021 годы».

Иные документы:

- Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных, с дополнениями и изменениями (утверждены протоколом заседания Правительственной комиссии по координации деятельности Открытого правительства от 29.05.2014 № 4).
- График раскрытия приоритетных социально-значимых наборов данных (утвержден протоколом заседания Правительственной комиссии по координации деятельности Открытого правительства от 28.10.2016 № 7).
- Актуализированный план-график создания витрин данных (одобрен президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 06.05.2022 № 16).

Приказы ФНС России:

- от 06.03.2018 № ММВ-7-17/125@ «Об утверждении Регламента подготовки и раскрытия общедоступной информации в формате открытых данных в соответствии с принципами открытости» (с изменениями);
- от 07.08.2019 № СА-7-19/401@ «Об официальном сайте Федеральной налоговой службы»;
- от 25.12.2020 № ЕД-7-20/957@ «Об утверждении Требований к обезличиванию фискальных данных и методов обезличивания фискальных данных»;
- от 01.03.2023 № ЕД-7-17/143@ «О Ведомственном плане ФНС России по реализации Концепции открытости федеральных органов исполнительной власти на 2023 год».

Приказы Росстата:

- от 07.12.2018 № 732 «Об утверждении Методологических положений по организации процессов производства официальной статистической информации»;
- от 18.06.2019 № 342 «Об утверждении Положения об Общественном совете при Федеральной службе государственной статистики» (с изменениями);
- от 27.10.2020 № 653 «Об утверждении Методологических рекомендаций по организации проведения обследования удовлетворенности пользователей официальной статистической информацией, предоставляемой Федеральной службой государственной статистики и ее территориальными органами, и работой Росстата в целом».

Регламент Счетной палаты Российской Федерации (утвержден постановлением Коллегии Счетной палаты Российской Федерации от 26.09.2023 № 12ПК).

Ознакомиться с презентацией

А.А. ПОЛИН
Начальник управления аудита цифрового развития и внутреннего финансового аудита, Департамент внутреннего аудита Банка России

ОБ ИТОГАХ АПРОБАЦИИ МЕТОДИКИ ОЦЕНКИ ЦИФРОВОЙ ЗРЕЛОСТИ БИЗНЕС-ПРОЦЕССОВ БАНКА РОССИИ

Аннотация

Совершенствование технологий, применение новых и развитие действующих цифровых решений оказывают значительное воздействие на экономическую деятельность и организацию бизнес-процессов. Осознание цифровых возможностей и соответствие текущего уровня цифровой зрелости организации запланированной политике цифровой трансформации играет решающую роль в достижении поставленных целей. В статье описана модель оценки цифровой зрелости Банка России, представляющая собой трехуровневую иерархическую структуру, состоящую из направлений цифровой трансформации, критериев и показателей их оценки и включающую пять уровней зрелости. Кроме того, рассмотрены практические аспекты проведения внутреннего аудита оценки цифровой зрелости. Приведены изменения, внесенные в методику оценки цифровой зрелости Банка России и касающиеся модели оценки цифровой зрелости и подходов к проведению анкетирования и методов оценки. Описана дальнейшая роль внутреннего аудита во взаимодействии с профильными подразделениями в проведении периодической оценки цифровой зрелости Банка России.
Ключевые слова: цифровая трансформация, цифровая зрелость, оценка цифровой зрелости, аудит цифровой зрелости.
Коды JEL: O31, O32, O33.

Совершенствование технологий, применение новых и развитие действующих цифровых решений оказывают значительное воздействие на экономическую деятельность и все ее отрасли. Происходит не просто внедрение технологий в уже существующие процессы (цифровизация), но и преобразование и реорганизация этих процессов с учетом новых вызовов, подходов и требований, осуществляются организационные и структурные изменения. Данные изменения представляют собой цифровую трансформацию.

Цифровая трансформация – это не модное течение, тенденция или гонка технологий, это действующий инструмент оптимизации процессов и рационализации ресурсов, а главное – способность быстрой адаптации к текущим изменениям. Цифровая зрелость, в свою очередь, отражает, насколько эффективно организация использует цифровые технологии для оптимизации, автоматизации и повышения гибкости своих процессов, и представляет собой уровень интеграции цифровых технологий и инструментов в операционные процессы компании.

Цифровая зрелость характеризует уровень цифровой трансформации и является одним из критериев для оценки достижения ее целей.

Актуальность данной темы для Банка России, помимо прочего, состоит в определении в качестве одного из показателей достижения национальной цели Российской Федерации по цифровой трансформации государственного и муниципального управления, экономики и социальной сферы *достижение к 2030 году цифровой зрелости государственного и муниципального управления, ключевых отраслей экономики и социальной сферы,* предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта.

Осознание реальных цифровых возможностей организации и соответствие текущего уровня ее цифровой зрелости запланированной политике цифровой трансформации играет решающую роль в достижении поставленных целей, успехе и результативности этой политики в целом, помогает избежать невозможности внедрения каких-либо технологий или излишней потери ресурсов, в том числе финансовых и временных.

Существуют лучшие практики, определяющие основные подходы к оценке цифровой зрелости, ключевые же критерии и области оценки цифровой зрелости должны учитывать и быть ориентированы на особенности и стратегию каждой конкретной организации. Организация, также основываясь на своей стратегии, должна определить оптимальный уровень цифровой зрелости.

Оценка цифровой зрелости представляет собой многоуровневую модель, где каждый уровень соответствует определенной степени интеграции цифровых решений. Формализованная модель цифровой зрелости служит средством получения объективной информации, основанной на критериальной оценке бизнес-процессов.

Модель оценки цифровой зрелости Банка России разработана внутренним аудитом с учетом предложений внешних экспертов и консультаций профильных подразделений. Она основана на базовых принципах модели CMMI[1], а также опубликованных практиках ее применения для отдельных направлений. Модель адаптирована для целей Банка России и в настоящее время представляет собой трехуровневую иерархическую структуру, состоящую из стратегически значимых направлений цифровой трансформации, критериев и показателей их оценки, и включает пять уровней зрелости: начальный, развивающийся, определенный, управляемый, оптимизируемый.

В Банке России определено пять направлений цифровой трансформации: стратегия цифровой трансформации и управление ею; бизнес-процессы; данные и аналитика; кадры и цифровая культура; инфраструктура и инструменты. По результатам оценки каждого из указанных направлений формируется итоговая интегральная оценка цифровой зрелости. В целях формирования комплексного видения внутренним аудитом состояния цифровой трансформации цифровая зрелость оценивается на уровне Банка России.

Существующие методики оценки цифровой зрелости находятся в постоянной динамике и систематически совершенствуются, что не является исключением и для Банка России. Так, методика оценки цифровой зрелости Банка России была скорректирована по итогам апробации в 2024 г. в рамках проведения процедуры внутреннего аудита.

---

[1] Capability Maturity Model Integration – Комплексная модель производительности и зрелости (примечание Редакционной коллегии).

В отношении практики проведения внутреннего аудита по вопросу оценки цифровой зрелости следует отметить, что оптимальными с точки зрения сбора и анализа аудиторских доказательств были приняты такие аудиторские процедуры, как опрос (анкетирование и интервьюирование), расчеты и анализ. Источниками информации, помимо автоматизированных систем и внутренних ресурсов, служили непосредственно анкеты подразделений, ответы подразделений по отдельным тематическим запросам, интервью с экспертами.

По итогам аудита определены зоны роста цифровой зрелости и выстраивания стратегии цифровой трансформации, а также установлена необходимость корректировки методики оценки цифровой зрелости.

В процессе доработки, в том числе в целях сближения применяемых профильными подразделениями подходов к оценке цифровой зрелости, в методику внесены следующие изменения:

- сокращено количество направлений цифровой трансформации с 7 до 5 за счет объединения блоков «Данные» и «Модели» и блоков «Кадры» и «Цифровая культура»;
- добавлены и уточнены отдельные критерии и показатели;
- доработаны названия уровней зрелости и описание их характеристик;
- обновлен подход к проведению анкетирования: осуществление оценки подразделений на уровне бизнес-процессов, а не самих подразделений, в связи с чем разработаны анкета профильных подразделений, включающая общие вопросы нормативного регулирования, и анкета подразделений центрального аппарата для детальной оценки бизнес-процессов;
- уточнены методы обобщения данных анкетирования и оценки степени достижения показателей.

Проведение первичной оценки цифровой зрелости предоставляет исходные данные для последующего стратегического планирования и формирования плана цифровой трансформации организации и является инструментом, позволяющим сделать краткосрочные и среднесрочные цели более четкими, реалистичными и реализуемыми при текущем уровне информационных технологий и развития корпоративной культуры.

С целью обеспечения равномерного развития всех направлений цифровой трансформации после определения текущего состояния цифровой зрелости и областей, требующих приоритетного развития, дальнейшая роль внутреннего аудита будет заключаться в проведении периодического мониторинга и сопоставления текущих и целевых уровней зрелости, отслеживании достижений и определении необходимых корректировок стратегии цифровой трансформации. Такой подход способствует своевременному выявлению перспективных сторон развития, существующих разрывов, недостающих ресурсов или неиспользуемых возможностей.

Разработка профильными подразделениями методики оценки цифровой зрелости по своим направлениям деятельности с конкретизацией критериев и проведение ими регулярной оценки в рамках текущей деятельности впоследствии обеспечат аудит исходными данными, которые могут быть применены при аудите как по вопросам цифровой зрелости, так и по иным направлениям.

Таким образом, аудит цифровой зрелости рассматривает вопросы, выходящие за рамки проверки наличия или применения тех или иных систем и оценки уровня автоматизации бизнес-процессов. Он затрагивает все направления деятельности организации и дает целостный взгляд на цифровую трансформацию, позволяет из ее абстрактного представления сформулировать объективные и измеримые показатели, в первую очередь в соотношении с готовностью бизнес-процессов к изменениям и стратегическими целями организации.

Список литературы

1. Кричевский М.Л., Мартынова Ю.А., Дмитриева С.В. Оценка цифровой зрелости предприятия // Санкт-Петербургский государственный университет аэрокосмического приборостроения. 2022. № 4.
2. Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».

Ознакомиться с презентацией

Е.И. ЖДАНОВ
Руководитель Службы внутреннего аудита
ПАО Московская Биржа

ПОДХОД К ОЦЕНКЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА ДЛЯ ГРУППЫ «МОСКОВСКАЯ БИРЖА»

Аннотация

Обеспечение непрерывности бизнеса (ОНБ) является стратегически важной задачей для Группы «Московская Биржа», направленной на поддержание стабильности операций и соблюдение обязательств перед клиентами и регуляторами. В статье рассматриваются ключевые аспекты и меры, необходимые для эффективного обеспечения ОНБ, включая организацию процессов, ИТ-архитектуру и ИТ-инфраструктуру. Особое внимание уделяется новым вызовам, таким как кибератаки и санкционное давление, а также важности регулярной независимой оценки процессов обеспечения непрерывности. Обсуждается роль внутреннего аудита в этой области, включая периодические проверки и привлечение внешних экспертов для технической оценки. Подчеркивается необходимость комплексного подхода к оценке и актуализации планов противодействия угрозам, что позволяет поддерживать необходимый уровень ОНБ.
Ключевые слова: обеспечение непрерывности бизнеса, внутренний аудит, ИТ-архитектура, кибербезопасность, риск-сценарии, внешняя экспертиза, торгово-клиринговые системы.
Коды JEL: G21, G32, L86.

Обеспечение непрерывности бизнеса представляет собой стратегическую задачу для Группы «Московская Биржа» в связи с необходимостью поддержания выполнения операций на уровне, достаточном для соблюдения как взятых на себя обязательств перед клиентами, так и регуляторных требований, нацеленных на обеспечение устойчивости финансовой системы страны. В связи с этим особую значимость приобретает не только эффективность применения отдельных мер по обеспечению непрерывной работы торгово-клиринговых систем, но системность и комплексность таких мер, их адекватность актуальному ландшафту угроз. Именно для достижения этих целей в Группе осуществляется регулярная независимая оценка процессов обеспечения непрерывности.

Для обеспечения комплексной оценки текущего состояния ОНБ необходимо фокусировать аудиторские процедуры и тесты на всех трех основных аспектах непрерывности:

- общей организации процесса обеспечения непрерывности бизнеса, включая стратегическое целеполагание, полноту планирования и своевременность тестирования аварийного восстановления, обучение и подготовку персонала, обеспечение связности ИТ-процессов с процессами ОНБ;

- ИТ-архитектуре в части ее готовности к поддержанию требуемых уровней отказоустойчивости, доступности, производительности, адаптации к изменениям, масштабируемости, наличии и качестве технической поддержки и документации;
- ИТ-инфраструктуре в части поддержания характеристик ее объектов (таких как срок эксплуатации, мониторинг, наличие запасных частей, актуальность программного обеспечения) на достаточном уровне для достижения целевых параметров доступности и восстановления.

На сегодняшний день перед ОНБ стоят новые вызовы, такие как увеличение количества и интенсивности кибератак, санкционное давление, отключение от системы SWIFT, уход с российского рынка поставщиков ИТ-оборудования и угрозы террористических атак. Важно заблаговременно готовить и постоянно актуализировать планы противодействия, а также прорабатывать и тестировать риск-сценарии, что в результате поддержит необходимый уровень ОНБ.

Подразделения внутреннего аудита (ВА) Группы проводят комплексную оценку процесса управления непрерывностью не реже чем раз в 2 года. Кроме того, вопросы непрерывности оцениваются ежегодно при проверках других направлений, например:

- аудиты управления и стратегического планирования ИТ – на предмет учета вопросов непрерывности и надежности при формировании стратегических целей ИТ;
- аудиты ключевых систем – на предмет полноты и корректности применяемых к ним мер обеспечения непрерывности;
- аудиты кибербезопасности – на предмет влияния угроз ИБ на непрерывность деятельности;
- аудиты бизнес-процессов – на предмет качества проведения анализа воздействия на бизнес, своевременности проведения DR-тестирования поддерживающих систем.

Оценка соответствия внешним и внутренним требованиям осуществляется с учетом:

- фактического дизайна процессов и уровня остаточного риска с учетом внедренных контрольных процедур;
- критичности бизнес-процессов и поддерживающих их систем;
- утвержденного Наблюдательным советом Московской Биржи риск-аппетита;
- анализа реализовавшихся за конкретный период угроз и рисковых событий;
- уже существующих планов по развитию направления;
- актуального ландшафта угроз и объективной необходимости в разработке и реализации соответствующих мер противодействия изменившимся угрозам.

За 5 лет направление непрерывности комплексно оценивалось 3 раза. Основной фокус в аудитах делался на организации процесса, его связности и соответствии ожиданиям бизнеса. При этом существуют ограничения в части отсутствия у подразделений ВА практической экспертизы в области эксплуатации специализированного оборудования и технологий, опыта построения архитектуры высоконагруженных систем, а также доступа к базам знаний зарубежных вендоров, что затрудняет самостоятельную оценку фактически применяемых технических решений, направленных на обеспечение отказоустойчивости и доступности систем Группы.

Для повышения уровня гарантий руководителем ВА было принято решение о привлечении внешней экспертизы с целью проведения технической оценки надежности инфраструктуры и ИТ-систем, а также сравнения применяемых в Группе решений с применимыми рыночными практиками.

На основании полученного в рамках проведенной внешней оценки опыта хотелось бы подчеркнуть, что консультационные проекты такого рода отличаются высокой стоимостью привлекаемой экспертизы, а достаточное для формирования выводов и адаптации лучших практик к специфике работы торгово-клиринговых систем погружение в уникальные процессы Группы и поиск релевантных объектов бенчмаркинга крайне затруднены и требуют дополнительных трудозатрат.

Несмотря на отмеченные сложности, по итогам проекта были сформированы комплексные рекомендации по критичным платформам, включающие предложения по изменениям в их инфраструктуре и архитектуре. На текущий момент ответственными подразделениями проводится анализ и планирование необходимых действий по повышению надежности работы инфраструктуры Группы. Практика привлечения внешнего специализированного контрагента для проведения технического аудита ОНБ была признана органами управления результативной.

Внутренние аудиторы должны обладать достаточными знаниями и навыками для покрытия проверками основных видов деятельности компании в целях совершенствования процессов и предоставления объективной и независимой оценки органам управления. При этом важно выделять те области, где требуется привлечение внешних экспертов, и уметь организовывать взаимодействие с ними.

Ознакомиться с презентацией

CODE MINING ВО ВНУТРЕННЕМ АУДИТЕ СБЕРА

О.В. ЧИСТЯКОВ
Старший управляющий директор – директор Управления внутреннего аудита ПАО Сбербанк

А.С. МИЛЛИОНОВ
Начальник отдела Управления внутреннего аудита по Волго-Вятскому банку ПАО Сбербанк

А.В. ЕГОРОВ
Менеджер направления Управления внутреннего аудита по Волго-Вятскому банку ПАО Сбербанк

Аннотация

В данной статье рассматривается использование методов Code Mining в практической деятельности внутреннего аудита, что становится особенно актуальным в условиях стремительной цифровизации и технологических изменений бизнес-процессов.
Code Mining как процесс извлечения полезной информации из исходного кода и его производных (код-артефактов) открывает новые перспективные возможности для повышения качества и эффективности внутреннего аудита.
Ключевые слова: Code Mining, анализ кода, цифровой двойник процесса, аудит.
Коды JEL: M42, C81.

Введение

В настоящее время аудиторские проверки, как правило, основываются не на отдельных выборках, а на 100%-ной популяции данных (подход data-driven). Цифровые следы процессов (скан-образы документов, транзакции, аудио- и видеозаписи и т.д.) позволяют воспроизвести цифровой двойник процесса для оценки его состояния и выявления потенциальных проблемных зон.

В основе любого автоматизированного процесса стоит программный код, реализующий запроектированную логику. Таким образом, анализ исходного кода позволяет выявлять реальные корневые причины отклонений в цифровом оригинале процесса, а также существенно снижает риски, связанные с качеством данных[1].

Code Mining является новой исследовательской дисциплиной, которая находится на стыке современных методов обработки больших данных. Он представляет собой процесс извлечения полезной информации из исходного кода автоматизированных систем. Сам анализ может включать в себя поиск зависимостей между различными частями кода, изучение причин использования определенных функций или переменных, а также оценку соответствия продукта заданным функциональным и бизнес-требованиям.

В рамках аудиторской деятельности применение Code Mining целесообразно для подтверждения ранее идентифицированных проблем в проверяемом процессе, а также для обнаружения новых инсайтов. Результатом являются подтвержденные отклонения в исходном коде, которые могут приводить к негативным бизнес-последствиям: отклонениям в качестве клиентского сервиса, финансовым потерям и реализации других рисков.

[1] Например, в случаях полного или частичного отсутствия репликации данных.

Исследуемые данные представляют собой исходный код либо его артефакты, являющиеся второстепенной метаинформацией, которая возникает в процессе разработки программного обеспечения. К такой информации относятся: документация, комментарии разработчиков, даты создания и завершения задачи, информация об изменении требований к функционалу, исправлении ошибок в коде и прочее.

Особенности применения

Исходный код может выступать в виде разных форматов данных для исследования.

Код как текст. Анализ с использованием алгоритмов и методов обработки текста (например, при помощи NLP[2]), которые позволяют анализировать исходный код на более глубоком уровне, выявляя скрытые зависимости, закономерности. Одним из подходов к анализу кода является генерация комментариев к коду, что позволяет повысить его читаемость. В данном случае перевод кода в текст открывает для аудитора возможности проверять соответствие реализованной логики процесса внутренним нормативным документам.

Код как графы. Подразумевается создание графических представлений кода в виде рисунков и диаграмм вызовов функций, структурных диаграмм (UML[3]) для построения взаимосвязей между разными частями кода и облегчения их последующего анализа. Изучение лога исполнения программы для оценки соответствия бизнес-процессу, выявление сложных зависимостей между элементами кода или между различными частями программы может включать следующие методы:

1) анализ AST-дерева[4] – исследование с помощью абстрактного синтаксического дерева;
2) анализ потока управления – исследование различных путей выполнения программы;
3) анализ потока данных – взаимодействие данных и глобальных свойств программы;
4) анализ лога исполнения программы – исследование цифровых следов работы программы, в том числе с использованием инструментов Process Mining или Graph Mining.

Код как исполняемый объект. Подразумевается динамическое тестирование, то есть запуск выполнения кода с различными наборами данных. В процессе тестирования производится эмуляция отклонений – исполнение программы с использованием некорректных параметров либо реальных параметров, приводящих к возникновению ошибок, влияющих на дальнейшую логику выполнения кода. Кроме того, может оцениваться работоспособность, корректность и полнота существующих покрывающих тестов.

Дополнительно запуск кода может применяться для формирования лога исполнения программы, который, в свою очередь, может выступать как самостоятельный артефакт для анализа.

При выявлении ошибок требуется определить причины их возникновения (ошибка разработчика или владельца процесса), оценить масштаб влияния на бизнес-процесс и оцифровать негативные последствия. Также нужно обращать внимание, что отклонение может оказывать побочное негативное действие на смежные задействованные процессы или системы.

---

[2] Natural Language Processing – обработка естественного языка.

[3] Unified Modeling Language – унифицированный язык моделирования.

[4] Abstract Syntax Tree – абстрактное синтаксическое дерево.

Инструментарий

Функционал инструментов для анализа кода, представленных в открытом доступе, направлен на повышение качества и безопасности разработки программного обеспечения. Но для оценки корректности имплементации бизнес-логики в код программы готовые решения отсутствуют. В зависимости от языка программирования и подходов к исследованию в качестве вспомогательных могут использоваться следующие инструменты:

- **языковые модели (LLM[5])** для перевода кода на естественный язык с целью поиска необходимых участков и конструкций (например, используемых интервалов значений или ключевых переменных/функций);
- **библиотеки для построения графов** зависимостей между модулями, функциями и классами, а также для построения AST-деревьев;
- **интегрированные среды разработки (IDE[6])**, которые позволяют запускать код, производить его отладку, визуализировать зависимости в коде.

В нашей практике наибольшую эффективность показали собственные разработки, которые сочетают в себе комбинацию перечисленных инструментов и позволяют реализовать комплексный подход к анализу.

Выводы и практическое применение

Постоянное совершенствование деятельности внутреннего аудита и поиск новых подходов к анализу данных является ключевым вызовом в современных условиях цифровизации. Применение Code Mining открывает для аудитора перспективные возможности:

- анализировать цифровой оригинал бизнес-процесса и оценивать его фактическое соответствие нормативным документам;
- устанавливать корневые причины отклонений в автоматизированных бизнес-процессах и предлагать владельцам процессов эффективные меры по решению проблем;
- повышать скорость и качество аудита в случаях полного или частичного отсутствия цифровых следов процесса. Code Mining позволяет напрямую анализировать бизнес-логику процесса, запрограммированную в код автоматизированной системы.

Список литературы

1. Фаулер М. ULM. Основы. Краткое руководство по стандартному языку объектного моделирования. Символ-плюс, 2004.
2. Ахо А.В., Лам М.С., Сети Р., Ульман Д.Д. Компиляторы: принципы, технологии и инструментарий. М.: ООО «И.Д. Вильямс», 2018.
3. Куликов С. Тестирование программного обеспечения, базовый курс. URL: https://svyatoslav.biz/software_testing_book.
4. Большакова Е.И., Воронцов К.В., Ефремова Н.Э., Клышинский Э.С., Лукашевич Н.В., Сапин А.С. Автоматическая обработка текстов на естественном языке и анализ данных. М.: ВШЭ, 2017.

Ознакомиться с презентацией

[5] Large Language Model – большая языковая модель.

[6] Integrated Development Environment – единая среда разработки.

ПОСТРОЕНИЕ ЭФФЕКТИВНОЙ ФУНКЦИИ ВНУТРЕННЕГО АУДИТА В ГОСКОМПАНИИ. АКТУАЛЬНЫЕ ВОПРОСЫ РИСК-ОРИЕНТИРОВАННОГО ПЛАНИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ КАРТЫ ГАРАНТИЙ

А.Л. ДУШАТИН
Директор Департамента внутреннего аудита ПАО «Аэрофлот»

Аннотация

В статье рассматривается построение эффективной функции внутреннего аудита в Группе «Аэрофлот» в контексте актуальных вопросов риск-ориентированного планирования и использования карты гарантий. Описывается нормативно-правовая основа, регулирующая деятельность внутреннего аудита в России, включая ключевые федеральные законы и методические рекомендации. Анализируются нововведения, касающиеся ежегодного заключения внутреннего аудита для акционеров, а также создание подкомитета по внутреннему аудиту в Росстандарте. Рассматриваются подходы к риск-ориентированному планированию, включая инструменты риск-анализа, карты рисков и поставщиков гарантий. Представлены шаги по оценке и актуализации карты гарантий, что позволяет выявить пробелы и дублирование в обеспечении уверенности. В заключение описываются практические инструменты адаптации работы внутреннего аудита с учетом внешних и внутренних факторов.
Ключевые слова: внутренний аудит, риск-ориентированное планирование, карта гарантий, нормативно-правовая основа, Группа «Аэрофлот», оценка рисков, обеспечение уверенности.
Коды JEL: M42, G34, K22.

Нормативно-правовая основа построения функции внутреннего аудита

Становление и развитие функции внутреннего аудита в Группе «Аэрофлот» неразрывно связаны с внедрением и трансформацией нормативно-правовых основ регулирования внутреннего аудита в Российской Федерации:

- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;
- Приказ Росимущества от 04.07.2014 № 249 «Об утверждении Методических рекомендаций по организации работы внутреннего аудита в акционерных обществах с участием Российской Федерации»;
- Приказ Росимущества от 03.09.2014 № 330 «Об утверждении Методических рекомендаций по построению функции внутреннего аудита в холдинговых структурах с участием Российской Федерации»;

- Информационное письмо Банка России от 01.10.2020 № ИН-06-28/143 «О рекомендациях по организации управления рисками, внутреннего контроля, внутреннего аудита, работы комитета совета директоров (наблюдательного совета) по аудиту в публичных акционерных обществах»;
- Письмо Банка России от 10.04.2014 № 06-52/2463 «О Кодексе корпоративного управления»;
- Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»;
- Международные стандарты внутреннего аудита и Кодекс этики (IIA).

МСВА в обновленной редакции 2024 г. содержат информацию об особенностях организации и функционирования внутреннего аудита в организациях общественного сектора – подраздел «Применение Международных стандартов внутреннего аудита в общественном секторе» раздела V «Предоставление услуг внутреннего аудита».

В соответствии с требованиями Федерального закона «Об акционерных обществах» руководитель внутреннего аудита ПАО «Аэрофлот» готовит ежегодное заключение для акционеров компании с оценкой надежности и эффективности системы внутреннего контроля и управления рисками в компании «Аэрофлот» и Группе компаний «Аэрофлот». Такое заключение внутреннего аудита предоставляется акционерам в составе материалов к ГОСА начиная с 2022 года.

В 2024 г. под эгидой Института внутренних аудиторов в Росстандарте создан подкомитет «Внутренний аудит» Технического комитета по стандартизации Росстандарта (ПК 4/ТК 076), в который вошли представители регуляторов и крупнейших российских компаний, в том числе и Аэрофлота, осуществляется разработка национальных стандартов по внутреннему аудиту. Предварительный национальный стандарт в области внутреннего аудита будет содержать информацию о порядке организации функции внутреннего аудита и в компаниях госсектора, а также учитывать отраслевую специфику при определении ключевых целей и задач внутреннего аудита.

Риск-ориентированное планирование

Риск-ориентированное планирование функции внутреннего аудита Группы «Аэрофлот» осуществляется в соответствии с МСВА и учитывает:

- риск-анализ модели аудита;
- карту рисков, декларацию риск-аппетита и сведения о реализовавшихся рисках;
- карту поставщиков гарантий;
- запросы заинтересованных сторон, включая предложения Совета директоров, высшего исполнительного руководства и внешних регуляторов;
- Стратегию развития Группы;
- Стратегию развития ДВА;
- внешние факторы: отраслевые тенденции, передовые практики и тренды рынка;
- компетенции и ресурсы ДВА.

В практической деятельности ДВА ПАО «Аэрофлот» проект риск-ориентированного плана рассматривается Правлением и Комитетом по аудиту Совета директоров, а затем утверждается Советом директоров.

Модель аудита

Для проведения оценки рисков организации руководителю внутреннего аудита следует рассмотреть цели и стратегию на уровне не только организации в целом, но и отдельных подлежащих аудиту единиц.

В практической деятельности ДВА ПАО «Аэрофлот» применяются инструменты по составлению (и последующей актуализации) модели аудита и ее риск-анализа. Предпосылками для актуализации модели аудита являются изменение структуры Группы, изменение организационной структуры компаний Группы, трансформация бизнес-процессов и иные существенные изменения, оказывающие влияние на деятельность Группы.

Риск-анализ модели аудита является одним из инструментов планирования, применением которого ДВА ПАО «Аэрофлот» связано с требованиями стандартов и изменением/переоценкой рисков, в том числе в связи с устранением ранее выявленных недостатков, изменением стратегии развития, изменением внешних условий ведения бизнеса и другими факторами.

Карта гарантий

В соответствии с МСВА 9.5 предусмотрено координирование деятельности внутреннего аудита с другими сторонами, обеспечивающими уверенность, и возможность полагаться на результаты их работы. Инструментом, применяемым ДВА ПАО «Аэрофлот», выступает карта гарантий – карта обеспечения уверенности или матрица рисков организации и внутренних и внешних поставщиков услуг по обеспечению уверенности. Примерами координации деятельности с поставщиками могут быть:

- синхронизация характера, объема и сроков выполнения запланированной работы;
- обеспечение общего понимания способов и методов обеспечения уверенности и используемой терминологии;
- доступ к рабочим программам и отчетам поставщиков, аудитам СМК и другим;
- использование предоставляемой руководством и поставщиками гарантий информации об управлении рисками для проведения совместной оценки рисков.

Шаг 1. Определение поставщиков (пример)

- Внутренние: авиационная безопасность, безопасность полетов, экономическая безопасность, информационная безопасность, охрана труда, экологический менеджмент, управление рисками (СУР), юридическое обеспечение, контроль качества (ИСМ, наземное обслуживание, поставки запчастей и прочие сферы деятельности).
- Внешние: аудиторы БФО (РСБУ, МСФО), аудиторы нефинансовой отчетности (отчет по ДПР, отчет о деятельности в области устойчивого развития, прочие виды ESG-отчетности, отчетность по CO2 и так далее), аудиторы по ISO, внешние отраслевые регуляторы (IATA, SkyTeam).

Шаг 2. Оценка поставщиков (пример)

- Этап 1. Предварительная оценка поставщика: сущность работ, независимость и объективность, категории рисков.
- Этап 2. Углубленная оценка поставщика: компетентность (применимость и достоверность их опыта, квалификации, сертификации), порядок выполнения работ, наличие нормативной документации (методология и должная профессиональная осмотрительность), периодичность выполняемых работ, вид и объем информации, которая может быть предоставлена ДВА (наблюдения и заключения, рабочая документация).
- Результатом выполнения шага 2 будет являться вывод об уровне надежности поставщика.

Шаг 3. Составление и последующая актуализация карты

Карта является практическим инструментом, позволяющим выявить пробелы и дублирование в обеспечении уверенности, что дает руководителю внутреннего аудита возможность оценить достаточность услуг и ресурсов по обеспечению уверенности в каждой области риска.

В докладе представлено подробное описание процесса внедрения и развития функции внутреннего аудита в Группе «Аэрофлот», а также раскрыты практические инструменты по адаптации плана работы внутреннего аудита с учетом влияния внешних и внутренних факторов.

Список литературы

1. Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах».
2. Приказ Росимущества от 04.07.2014 № 249 «Об утверждении Методических рекомендаций по организации работы внутреннего аудита в акционерных обществах с участием Российской Федерации».
3. Приказ Росимущества от 03.09.2014 № 330 «Об утверждении Методических рекомендаций по построению функции внутреннего аудита в холдинговых структурах с участием Российской Федерации».
4. Информационное письмо Банка России от 01.10.2020 № ИН-06-28/143 «О рекомендациях по организации управления рисками, внутреннего контроля, внутреннего аудита, работы комитета совета директоров (наблюдательного совета) по аудиту в публичных акционерных обществах».
5. Письмо Банка России от 10.04.2014 № 06-52/2463 «О Кодексе корпоративного управления».
6. Международные стандарты внутреннего аудита и Кодекс этики (IIA).
7. Новые Международные стандарты внутреннего аудита (МСВА). Вступают в силу с 09.01.2025. URL: МСВА 2024 (дата обращения: 25.12.2024).

Ознакомиться с презентацией

С.В. ЗУБКОВА
Доцент кафедры банковского дела и монетарного регулирования, ведущий научный сотрудник Института финансовых исследований финансового факультета, Финансовый университет при Правительстве Российской Федерации, к.э.н.

ЭКОСИСТЕМНОСТЬ НА РЫНКЕ ФИНАНСОВЫХ УСЛУГ: ПЕРСПЕКТИВЫ РАЗВИТИЯ И РИСКИ

Аннотация

В статье рассматриваются актуальные вопросы развития экосистемности на рынке финансовых услуг, в том числе особенности экосистем на рынке финансовых услуг, развитие встроенных финансов на платформах экосистем. Экосистемность на рынке финансовых услуг, являясь, безусловно, позитивным трендом экономического развития любой страны, может генерировать серьезные риски, которые требуют особого регулирования. Представленные предложения по регулированию экосистем могут стать основой первых шагов по изменению законодательства в данной области.
Ключевые слова: экосистемность, рынок финансовых услуг, стратегический риск, банкоцентричные экосистемы, предпринимательские экосистемы.
Коды JEL: G20, G28, O33, L86, D83.

Изменившаяся среда функционирования институтов финансового рынка стала драйвером выбора новой модели ведения бизнеса – экосистемной.

Предпосылками нового тренда на рынке финансовых услуг стали развитие цифровизации, обострение конкуренции, необходимость повышения доходности бизнеса, появление новых технологических решений.

Клиентоориентированный подход постепенно трансформируется в клиентоцентричный, где главным становятся возрастающие потребности и качество жизни клиента. Расширение присутствия на рынке финансовых услуг технологических и других компаний способствует развитию встроенных финансовых услуг, которые становятся основой экосистемности на финансовом рынке. Цифровая трансформация экономики привела к возрастанию роли экосистем, влиянию их на формирование устойчивости финансовой системы через активное развитие на своих платформах финансовых услуг. Особенностью экосистем является их способность объединять различные сервисы на единой платформе, что не только упрощает взаимодействие с клиентами, но и способствует повышению эффективности деятельности.

Необходимо отметить, что четкое и однозначное понимание экосистемы и экосистемности на рынке финансовых услуг пока не сформировалось. Нет также полноценных исследований о роли и перспективах развития экосистемности на рынке финансовых услуг.

В процессе изучения обширного круга источников сформировано следующее определение экосистемы на рынке финансовых услуг: это партнерство организаций (одна из которых является кредитной/страховой или иной финансовой организацией), которые осуществляют свою деятельность на основе совокупности цифровых платформ, прикладных интернет-сервисов, аналитических и информационных систем, обеспечивая взаимодействие участников с целью реализации продуктов и оказания услуг.

Следует также отличать экосистему, действующую на рынке финансовых услуг, от маркетплейса, который является онлайн-платформой, объединяющей участников рынка финансовых услуг и позволяющей им представлять и продавать разнообразные финансовые услуги.

В свою очередь финансовые услуги – это услуги, оказываемые банковскими, страховыми компаниями, услуги по купле-продаже ценных бумаг, паевых инвестиционных фондов, негосударственных пенсионных фондов, других небанковских финансовых институтов, включая соответствующие транзакции.

Ученые и практики выделяют следующие особенности функционирования экосистем: пространственность и глобальный охват; клиентоцентричность; мультипликация положительных сетевых эффектов; многосторонний характер финансирования участников на основе перекрестного субсидирования; усиление дезинтермедиации – исключение посредников из цепочек создания новой стоимости; обеспечение повышения информационной насыщенности систем и сокращения асимметрии информации; инновационный характер – обеспечение особой среды для ускоренного внедрения инноваций; затратный выход – поскольку экосистемы предоставляют большой набор товаров, услуг, информации, ресурсов, доступ к разнообразным сервисам, платформам, выход из них затруднен для большинства пользователей [1, 2].

Экосистемы можно разделить на банкоцентричные (сформированные на основе банковских групп и партнерские) и предпринимательские, организаторами которых выступают организации различных отраслей экономики, в том числе крупные технологические компании. Для российского рынка основным типом стали банкоцентричные экосистемы, в то время как для зарубежного – предпринимательские экосистемы.

Крупнейшие мировые компании, выбравшие путь развития экосистем, получили серьезные конкурентные преимущества, о чем свидетельствует рост их капитализации за последние 10 лет в 10–15 раз. Среди них – Amazon, Apple, Baidu, Tecent, Alphabet. На первом месте по темпам роста стоимости находятся американские экосистемные компании, на втором – китайские. Согласно прогнозам международной консалтинговой компании McKinsey, доля организаций, базирующихся на экосистемной модели, в мировом ВВП достигнет 30% к 2025 г., обеспечив совокупный доход в размере более 60 трлн долл. США [3].

Капитализация российских компаний, к которым можно отнести в первую очередь ПАО Сбербанк, Банк ВТБ (ПАО), АО «ТБанк», Озон, Яндекс, ПАО «МТС», X5 Group, Вайлдберрис, Мегафон, Авито, по сравнению с зарубежными институтами пока еще в десятки раз ниже.

Рост конкуренции не только между институтами финансового рынка, но и между разными типами экосистем, зачастую отсутствие регулирования экосистемности на рынке финансовых услуг, влияние цифровизации на необходимость защиты персональных данных и соблюдение прав потребителей предопределили необходимость осмысления происходящих процессов, идентификации рисков, выявления противоречий макроэкономического и микроэкономического характера и разработки единой модели регулирования финансовых услуг, оказываемых на цифровых платформах экосистем.

Среди источников рисков новой модели бизнеса можно выделить такие, как использование большого запаса пользовательских данных, цифровая зависимость участников друг от друга, интеграция и взаимосвязанность всех приложений и участников экосистемы, а также внедрение искусственного интеллекта, тесная интеграция с социальными сетями, активно влияющими на поведение потребителей, и другие.

К группе основных рисков, возникающих в экосистемной модели ведения бизнеса, отнесены: стратегические, предопределяющие перспективность бизнеса; риск ответственности организаторов экосистем, в том числе организации систем управления рисками; появление принципиально новой группы рисков, обусловленных цифровизацией (нарушения прав потребителей при использовании цифровых и дистанционных услуг; риски потери операционной и цифровой устойчивости, риски встроенных финансовых услуг), и некоторые другие. Значительный перечень приведенных рисков находится вне регуляторного поля.

Экономико-статистическое моделирование, проведенное коллективом ученых Финансового университета при Правительстве Российской Федерации, показало положительную роль экосистем в экономическом развитии страны.

В то же время развитие сервисов встроенного финансирования в крупных экосистемах может привести к серьезным рискам, таким как риски, связанные с безопасностью данных, репутационные риски, регуляторные риски, риски мошенничества и финансовых преступлений. Возможность встроить финансовые услуги, такие как платежи и кредитование, в нетрадиционные финансовые и нефинансовые платформы, позволяет клиентам получать доступ к финансовым решениям с минимальными трудностями в момент необходимости.

Встроенные финансы уже назвали трендом 2023 г., а рынок встроенного финансирования (EF) к 2026 г. превысит 7 трлн долл. США от общего объема финансовых транзакций в США (увеличившись с 2,6 трлн долл. США в 2021 г.). Как пишет Саймон Тейлор (в своем информационном бюллетене от 4 июня 2023 г. Fintech Brain Food – The Future of Embedded Finance), «все финансы становятся встроенными». EF полностью интегрирован с потребительскими тенденциями и клиентскими предпочтениями. Скоро вопрос будет уже не в том, какое финансирование встроено, а в том, какое нет [4].

Неконтролируемое развитие встроенного финансирования не только приводит к повышению рисков для участников и организаторов экосистем, но может привести и к реализации рисков для кредиторов и вкладчиков, финансовой стабильности в целом.

Развитие экосистемности на рынке финансовых услуг может сгенерировать неопознанные риски кросс-секторального характера, которые могут оказаться экзистенциальными как для рынка в целом, так и для его отдельных участников, что требует выработки соответствующих корректирующих мер и разработки норм регулирования.

Регулирование финансовых услуг, оказываемых в экосистемах, должно включать такие блоки, как:

- Регулирование рисков, сопутствующих функционированию экосистем в рамках антимонопольного законодательства.
- Регулирование рисков организаторов/управляющих экосистем, занимающих существенную долю на рынке финансовых услуг.
- Регулирование операционной и цифровой устойчивости всех участников финансового рынка, что потребует введения цифровых лицензий.
- Регулирование цифровых и дистанционных финансовых услуг, независимо от места их оказания, то есть непосредственно в экосистеме или нет.

Риски, возникающие в работе цифровых платформ и сервисов экосистем, учитывая их критический характер, требуют принятия самостоятельного закона «О цифровой оперативной устойчивости участников финансового рынка, в том числе связанных компаний». Данный закон должен стать обязательным для всех участников финансового рынка, в том числе экосистем на рынке финансовых услуг, а также для банков, платежных агентов, инвестиционных компаний, страховых компаний, поставщиков информационно-коммуникационных технологий (ИКТ), относимых к критической инфраструктуре. В законе необходимо закрепить требования к системе управления рисками в сфере ИКТ, формирование соответствующей системы управления, составление и представление регулятору соответствующей отчетности; проведение регулярного тестирования устойчивости финансовых операций, правила обмена информацией, а также создание надежной системы контроля практики управления рисками в сфере ИКТ.

В целях защиты прав потребителей дополнительно к существующим нормам Федерального закона «О защите прав потребителей» необходимо обязать организатора экосистемы обеспечить выполнение полного перечня условий, позволяющих защитить потребителей от возможных нарушений всех партнеров экосистемы.

Поправки необходимо внести в федеральное законодательство, регулирующее защиту персональных данных и информации.

В рамках регулирования финансовой устойчивости на рынке финансовых услуг целесообразно определить ответственность Банка России за регистрацию и контроль экосистем, действующих на рынке финансовых услуг, выявление организаторов/управляющих экосистем как объектов регулирования, соблюдение принципов функционирования экосистем, требований транспарентности, формирование отчетности, методическое сопровождение, организацию оценки удовлетворенности пользователей.

Список литературы

1. Клейнер Г.Б. Развитие экосистем в финансовом секторе России / Г.Б. Клейнер, М.А. Рыбачук, В.А. Карпинская // Управленец. 2020. № 4. Том 11. С. 2–15.
2. Раменская Л.А. К вопросу об определении границы экосистемы / Л.А. Раменская // Менеджмент и предпринимательство в парадигме устойчивого развития: Материалы IV Международной научно-практической конференции. Екатеринбург: Уральский государственный экономический университет, 2021. С. 170–173.
3. Investing.com. 2023. URL: (дата обращения: 20.09.2024).
4. Embedded Finance: risks, opportunities, and regulatory pathways – The Paypers. URL: https://thepaypers.com/expert-opinion/embedded-finance-risks-opportunities-and-regulatory-pathways--1263194 (дата обращения: 15.09.2024).
5. Competing with Banking Ecosystems // Accenture Consulting. URL: https://www.accenture.com/_acnmedia/pdf-102/accenture-banking-ecosystem. pdf (дата обращения: 20.09.2024).
6. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_216 363/?ysclid=m1dg6ehh3w901072382 (дата обращения: 24.08.2024).
7. Экосистемы: подходы к регулированию. Доклад для общественных консультаций. Апрель 2021 года // Банк России. М., 2021. URL: https://cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021. pdf (дата обращения: 15.09.2024).

8. Абрамова М.А. Турбулентность угроз финансовой стабильности в новых реалиях развития денежной и платежной систем / М.А. Абрамова, С.Е. Дубова // Банковские услуги. 2022. № 7. С. 9–18.
9. Авис О.У. Проблемы развития рынка BNPL и целесообразности его регулирования // Финансовые рынки и банки. 2024. № 6. С. 236–244.
10. Акименко С.В. Финансовый маркетплейс или экосистема: какой формат посредничества на рынке финансовых услуг выбрать провайдеру // Финансовые рынки и банки. 2024. № 8. С. 78–85.
11. Дубова С.Е. Тренды индустрии финансовых услуг и их влияние на развитие экосистем // Известия СПбГЭУ. 2024. № 3. С. 39–45.
12. Ларионова И.В. Мешкова Е.И. Экосистемная модель бизнеса: устойчивый или нисходящий тренд развития // Банковские услуги. 2024. № 3. С. 2–8.
13. Литвин В.В. Феномен экосистемности на рынке финансовых услуг: сущность, предпосылки формирования, перспективы развития // Финансовые рынки и банки. 2024. № 5. С. 229–240.
14. Платформенная экономика в России: потенциал развития: Аналитический доклад / Г.И. Абдрахманова, Л.М. Гохберг, А.В. Демьянова [и др.]; под редакцией Л.М. Гохберга, Б.М. Глазкова, П.Б. Рудника, Г.И. Абдрахмановой. М.: ИСИЭЗ ВШЭ, 2023.
15. Главные тренды финтех-индустрии на 2024 год // Коммерсантъ. URL: https://www.devere-group.com/6-predictions-for-fintech-in-2024/ (дата обращения: 04.09.2024).
16. Шесть прогнозов для финтеха в 2024 году. URL: https://www.devere-group.com/6-predictions-for-fintech-in-2024/ (дата обращения: 04.09.2024).

Ознакомиться с презентацией

КОНФЛИКТЫ И КООПЕРАЦИЯ ТРЕХ ЛИНИЙ ЗАЩИТЫ ПРИ РАЗРЕШЕНИИ СИТУАЦИЙ ПРИ ПОДДЕРЖКЕ И ОСУЩЕСТВЛЕНИИ ВЗАИМОДЕЙСТВИЯ ПО ОГРАНИЧЕНИЮ ВЛИЯНИЯ РИСКОВ В КОМПАНИЯХ

А.М. КОЗЛОВ
Старший менеджер Департамента управленческого консультирования АО «ДРТ», к.ф.-м.н., МГУ

А.А. КУДРЯШЕВА
Консультант Департамента управленческого консультирования АО «ДРТ», бакалавр по специализации «Экономика и финансы» МИЭФ и LSE

Аннотация

После мирового финансового кризиса 2007–2009 годов разработка и внедрение систем внутреннего контроля привлекли серьезное внимание участников финансовой системы. Модель трех линий защиты традиционно используется для представления взаимодействия между элементами системы корпоративного управления. Однако, согласно рекомендациям Базельского комитета по банковскому надзору, не менее важно привлечение внешних аудиторов-консультантов и регуляторов в структуру защиты для уменьшения асимметрии информации между вовлеченными сторонами и обеспечения дополнительных выгод для организаций. Основой их успешной работы является регулярная и эффективная координация, сотрудничество и коммуникация.
В статье последовательно рассматриваются интеракции между компонентами четырех линий защиты: взаимодействия между советом директоров и первыми двумя линиями, слаженность их кооперации с внутренним аудитом и динамика долгосрочной прибыли от привлечения внешних акторов. Для этой цели были использованы вариации фундаментальных моделей теории игр, позволяющие рассмотреть возникающие внутри корпоративной структуры конфликты, подходы к их разрешению и выгоды от синергии не только на примере конкретных бизнес-подразделений, но и на уровне функционирования кредитной организации в рыночной системе.
Ключевые слова: теория игр, корпоративная структура, корпоративное управление, конфликты, кооперация, риски, аудит, поведенческая экономика, банки, линии защиты.
JEL коды: C11, C68, C71, C73, C78, D23, D81, D82, D83, D84, D86, G21, G32, G34.

Модель трех линий защиты возлагает обязанности по регулированию и управлению рисками на владельцев процессов операционного управления. Средства контроля на этом этапе детализированы и основаны на отдельных транзакциях. Вторая линия обязана быть автономной от первостепенной, осуществлять мониторинг на постоянной или периодической основе и зиждиться на четких критериях оценки рисков. Для того чтобы третья линия – функция внутреннего аудита – была действенной, она должна основываться на независимости и объективности. Аудиторская служба проводит оценку рисков не реже раза в год – таким образом, реализуется лишь периодическая оценка рисков, а не детальный и постоянный

мониторинг, типичный для первой линии. Между службой внутреннего аудита и руководством должно осуществляться регулярное взаимодействие, чтобы обеспечивать актуализацию работы и ее соответствие стратегическим потребностям организации.

Три линии защиты необходимы для более эффективного управления конкретными рисками, которые банки представляют для экономики в целом, сочетая микро- и макропруденциальный подход к надзору. Несмотря на теоретическую слаженность и органичность взаимодействия элементов структуры, предполагаемых моделью, де-факто подобный идеал едва ли достижим. Корпоративное управление предполагает сложное взаимодействие заинтересованных сторон – акционеров, руководителей, сотрудников, клиентов, вендоров и внешних игроков.

Каждая группа неотъемлемо обладает своими интересами, столкновение которых приводит к конфликтам. Ключевые проявления подобных разногласий можно представить в следующих категориях:

- **Организационные структуры и разделение полномочий:** когда комитет по аудиту компании состоит из директоров, тесно связанных с руководством, независимость может быть поставлена под угрозу. Некоторые организационные структуры могут способствовать наблюдению за усилиями руководства. Таким образом, в организациях с несколькими подразделениями проще оценить эффективность работы менеджеров, чем в унитарных предприятиях.
- **Самостоятельные сделки:** руководители, участвующие в сделках с компанией, которую они возглавляют (например, продажа активов на выгодных условиях), создают конфликты. Эти действия могут принести пользу отдельному лицу, но при этом навредить акционерам и испортить репутацию.
- **Инсайдерская торговля:** использование закрытой информации в личных целях является классическим конфликтом. Инсайдерская торговля подрывает целостность рынка и доверие инвесторов.
- **Дублирование ролей:** когда директор одновременно входит в советы директоров конкурирующих компаний, возникают конфликты. Их лояльность может разделиться, что повлияет на принятие решений.
- **Структура вознаграждения:** в отсутствие продуманного дизайна системы вознаграждения сотрудников велик риск недобросовестного поведения работников и, как следствие, ухудшения финансовых показателей компании. Вознаграждение руководителей, привязанное к опционам на акции, может стимулировать получение краткосрочной прибыли в ущерб долгосрочной стабильности.

За последние десятилетия в международном финансовом секторе наблюдался поток скандалов, связанных с непрозрачной активностью. Они сыграли существенную роль в изменении условий ведения бизнеса во всем мире, возникновении значительных материальных потерь в частном секторе, распределении массированной государственной помощи финансовым учреждениям и формировании продолжающихся регуляторных реакций. Так, в 2007 г. Goldman Sachs, JP Morgan Chase и Bank of America признали неоднократные неисполнения своих обязанностей по раскрытию информации инвесторам о низком качестве базисных для ценных бумаг, обеспеченных ипотекой, кредитов. Примерами недостаточных функций второй линии защиты послужили новости о мошеннической торговле в Société Generale в 2008 г. и, годом ранее, финансовые потери UBS, которые возникли в результате ипотечного кризиса в США и едва не привели к краху последнего банка. Европейская комиссия акцентирует внимание на изъянах в управлении рисками, часто встречающихся на уровне совета директоров, включая поверхностное понимание природы и характера рисков, недостаток полномочий для сдерживания действий сотрудников подразделений, принимающих риски, ограниченный опыт в управлении рисками и отсутствие достаточной информации о них в режиме реального времени.

Одним из способов формализации обширного пула коллизий не только в рамках корпоративной структуры отдельного предприятия, но и за ее пределами является так называемая агентская теория (agency theory), имплементацию которой можно разделить на несколько этапов:

1. **Идентификация акторов:** определение участников в каждом рассматриваемом бизнес-взаимоотношении в иерархии.
2. **Определение потенциальных конфликтов:** предвосхищение, анализ причин и следствий возможных конфликтов интересов.
3. **Разработка актуальной системы вознаграждений:** разработка системы материальных и нематериальных стимулов, соответствующей интересам работников организации и акционеров.
4. **Создание мониторинговых механизмов:** проведение регулярного аудита и ревизионного контроля с целью идентификации и разрешения конфликтов.
5. **Поощрение участия в жизни организации:** соотнесение интересов руководителей и сотрудников посредством совместной формы собственности и иных разумных механизмов.

Типологизация разногласий компонентов корпоративной структуры в рамках агентской теории может быть рассмотрена на примере различных подмножеств взаимоотношений (к примеру, между акционерами и менеджерами или руководителями подразделений, мажоритарными и миноритарными акционерами, советом директоров и генеральным директором). Для обеспечения слаженность всех компонентов необходимо убедиться в поведенческой согласованности на уровне каждой из трех рассматриваемых линий защиты поочередно. Одним из способов обеспечения синтеза является разработка и реализация целесообразной схемы материальных вознаграждений для целей укрощения и предотвращения девиаций.

Ключевой целью данной статьи является последовательное рассмотрение и объединение на основании ключевых механизмов воздействия всех необходимых элементов, обеспечивающих эффективность функционирования предприятия: на основании агентской теории и теории контрактов представляются интеракции между советом директоров и первыми двумя линиями защиты. Затем полученные результаты работ этих компонентов рассматриваются через парадигму их способности к успешной кооперации с внутренним аудитом. В результате удается получить модель трех линий защиты на уровне корпоративного управления. Для транзиции к новому витку жизнедеятельности организации ожидаемые финансовые результаты от ранее рассмотренных этапов переводятся из замкнутой и зависимой от внутренних противоречий системы в доступную и открытую к внешним вызовам динамичную структуру.

С учетом предписаний Инструкции Банка России от 17.06.2014 № 154-И и выделения двух групп работников: сотрудников, несущих риски, и сотрудников, принимающих риски, – создается возможность перенести привычные ранговые связи в расчетную количественную плоскость. Агентская теория возникает из-за несоответствия действий агентов (agents) интересам принципала (principal), что подчеркивает важность договорных отношений и необходимость дизайна системы стимулирования работников в зависимости от уровня рисков и их вклада в деятельность компании для целей согласованности и кооперации. Рассмотрим данную концепцию на примере:

1) главы совета директоров (principal) и работников подразделения розничного бизнеса (первая линия защиты; agents). Целью бизнес-подразделения является увеличение доходности портфеля с заданным уровнем резервирования с учетом стратегии продвижения банка, утверждаемой советом директоров;
2) главы совета директоров (principal) и работников подразделений, отвечающих за контроль уровня ликвидности и резервов (вторая линия защиты; agents). Целью бизнес-подразделения является обеспечение надлежащего уровня достаточности капитала в соответствии с нормативами Банка России.

В рамках модели предполагается два уровня осведомленности руководителя об уровне усилий работников: в организации присутствует абсолютный мониторинг, при котором глава совета директоров наблюдает за процессом исполнения целей бизнес-подразделения, и ситуация, при которой комитетом аудита при совете директоров в организации не реализуются достаточные меры для проведения регулярного контроля. В связи с этим руководитель основывается на своих личных ожиданиях о вероятности исполнения функций. Таким образом, с учетом рассмотрения двух категорий работников и соответствующих им уровней усилий, прикладываемых для исполнения бизнес-целей, формируются следующие обстоятельства для задач максимизации:

Наблюдаемые усилия

Глава совета директоров максимизирует прибыль в ситуации, когда наблюдается достижение целей, и осуществляет сравнение материальных выгод со случаем их неисполнения. В данном положении работникам будет выгодно проявлять усилия в связи с более высоким уровнем заработной платы, что тем самым позволит увеличить прибыль организации. Руководитель, предвосхищая положительные результаты работы, готов к достойному вознаграждению труда. Ожидаемый доход компании при выполнении целей эквивалентен или превышает предполагаемую прибыль в обратном случае.

Ненаблюдаемые усилия

1. Глава совета директоров максимизирует свою прибыль в ситуации, когда он ожидает выполнения целей, но не может быть уверен в добросовестности труда работников. При таких условиях прибыль при осязаемых усилиях превышает прибыль при ненаблюдаемых. Руководитель не может быть уверен в том, что большие вознаграждения побудят работников бизнес-подразделений к эффективной деятельности.
2. Глава совета директоров максимизирует свою прибыль в ситуации, когда он ожидает неисполнения плана. В этом положении ожидаемый доход при наблюдаемых низких усилиях идентичен прибыли при ожидаемом неисполнении цели.

Таким образом, при отсутствии мониторинга совету директоров будет невыгодно выбирать компенсационную схему, соответствующую высокому уровню усилий, – он будет мириться с бездействием работников, что приведет к большим рискам неисполнения целей работниками бизнес-подразделений и снижению продуктивности. Предполагается, что руководитель не намерен брать на себя риски (то есть питать надежды на иллюзорную вероятность исполнения целей) на данном этапе. При наблюдаемых усилиях более вероятно, что совет директоров предпочтет высокий уровень усилий, чем в случае ненаблюдаемых, – реализуется система честного вознаграждения за достойный труд.

Для большей реалистичности концептуального представления резонно представить агрегированную ожидаемую прибыль организации с учетом вклада двух подразделений в случаях с наблюдаемыми и ненаблюдаемыми усилиями. Исходя из этого, складывается правдоподобная картина корпоративной структуры с несовершенным мониторингом.

Для полноценного перехода к модели трех линий защиты и непосредственному рассмотрению кооперации между всеми ее элементами можно воспользоваться вариацией модели Гроссмана – Харта. Рассмотрим ожидаемую прибыль организации, найденную ранее, в зависимости от способности к открытому взаимодействию с внутренним аудитом. Для этого введем коэффициент кооперации, значение которого будет равняться или превосходить единицу в случае успешного синтеза всех акторов и уменьшать ожидаемую прибыль в обратном случае.

Кооперация является прибыльной для бизнес-подразделений, если материальная выгода организации от синергии превосходит премии работникам, которым удается привнести вклад

за счет добросовестного сотрудничества (в данной ситуации растет ценность компании и потенциально улучшаются условия труда), и возможные убытки в случае неэффективной работы или обнаружения девиаций от корпоративного курса. Предположим, что издержки для сотрудников, не исполняющих цели (то есть сотрудников с низким уровнем усилий, работающих на стартовых и средних позициях), превосходят штрафные санкции работников на высших должностях (то есть работников с высоким уровнем усилий). В таком случае работники с низким уровнем усилий, ввиду высокой «стоимости» девиаций, скорее всего, предпочтут кооперацию, что позволит организовать массовый трудоспособный пласт. Однако часть сотрудников на высших должностях могут воспользоваться (free-ride) реализуемой другими выгодой, так как большинство работников предпочтут кооперацию. Данная ситуация является распространенной в случаях некорректной оценки способностей и игнорирования идеалистически сильных и идейных руководителей. Подобная несостоятельность чревата для организаций и, в свою очередь, может привести к усугублению асимметрии информации, поскольку такие субъекты не несут всех издержек. При таком дисбалансе сил внутреннего единения может оказаться недостаточно.

До текущего момента рассматривалась замкнутая модель трех линий защиты, не предполагающая взаимодействия с внешними надзорными органами или внешними аудиторами. Стремление части работников к отклонению, несмотря на наличие санкций, в таком положении является неизбежным. Девиаций можно избежать, если издержки, которые возникают при обнаружении сторонними консультантами факта недобросовестного взаимодействия со стороны сотрудников, превышают ожидаемые убытки в случае отсутствия кооперации. Это подчеркивает важность внешнего надзорного органа и вероятность потенциального ущерба на уровне как компании, так и отдельных участников процесса при отсутствии развитой системы корпоративного управления. Именно поэтому Базельским комитетом по банковскому надзору в корпоративный периметр включаются внешние независимые стороны.

Для достоверности рассматриваемых взаимосвязей можно воспользоваться моделью динамической кооперации. Это позволит визуализировать долгосрочные условия и последствия взаимодействия элементов, а также рассмотреть организацию как единицу общей системы. Под кооперацией в данном случае понимается слаженная работа всех четырех линий защиты, включая привлекаемых сторонних агентов. Для реализации динамического моделирования необходимо явно обозначить список стратегий (grim-trigger strategies) и соответствующих им «выплат» (в нашем случае – ожидаемых уровней прибыли). Если отклонение не может быть идентифицировано игроками, стимулы к кооперации отсутствуют. В случае отклонения от общей стратегии организация понесет ущерб, несмотря на краткосрочную выгоду. Количество рассматриваемых периодов кооперации может варьироваться в зависимости от предпосылок. В случае если во всех предшествующих периодах присутствовала кооперация, организация получает высокий уровень прибыли и дополнительную выгоду от взаимодействия с внешними аудиторами. Однако отклонение от совместных действий, хотя и несет в себе достаточный уровень риска, является резонным для работников и может позволить им получить преимущества на индивидуальном уровне. Подобную динамическую «игру» можно рассмотреть в двух вариациях:

1. В течение первоначального периода четыре линии осуществляют взаимовыгодные интеракции, однако в последующий происходит отклонение одного из элементов трех линий защиты, что позволяет этой структурной единице получить дополнительную прибыль. Однако вскоре наступает бессрочная фаза «наказания», в течение которой организация вынуждена получать лишь незначительную прибыль.
2. Линии «сотрудничают» до тех пор, пока никто не откажется от этого действия. В противном случае (если отклонение произошло) организация будет получать низкую прибыль в течение

конечного количества периодов – например, до момента полноценной реализации структурных преобразований, побуждающих к улучшению общего климата. После этого кооперация возобновляется до тех пор, пока не произойдет следующее отклонение.

Первый случай можно представить как неспособность организации к достаточному внутреннему контролю: несостоятельные функции мониторинга, отсутствие достойных материальных стимулов, недостаточное признание роли отдельных элементов и скромные конкурентные позиции. В таком виде фаза «регенерации» или восстановления может потребовать чрезмерных временных затрат. Следующая ситуация предполагает, несмотря на существующие недостатки, готовность и открытость к улучшению условий, стремление к согласованности с национальными и международными стандартами и укреплению собственных позиций. Надзорные органы и внешние консультанты могут не только акцентировать внимание на зачастую скрытых аспектах, но и в случае готовности руководства стать источником инновационного подхода и альтернативного взгляда на стратегию управления.

Моделирование данных сценариев подтверждает, что высокая прибыль от отклонения по сравнению с прибылью от сотрудничества увеличивает стимулы к девиации. Чем ниже прибыль на этапе «наказания» (то есть чем строже санкции, исходящие как изнутри, так и со стороны внешних регулирующих органов), тем более устойчивой является кооперация. Таким образом, на начальных этапах формирования модели взаимодействие отдельных линий защиты и руководства дает четкое представление о необходимости корректного дизайна системы вознаграждений. Она является связующим звеном, влияющим на поведение агентов и обеспечивающим как внутреннюю согласованность компонентов, так и их открытость к внешним вызовам.

При включении большего круга лиц в иерархические отношения возникает общая агентская теория (common agency problem). Интерпретируя ее в рамках заданных концепций, можно прийти к выводу, что в отсутствие непредвиденных внешних обстоятельств и при наличии слаженной системы внутреннего контроля и мониторинга коллективное решение агентов будет оптимальным не только для всех причастных лиц, но и для организации в целом. В результате становится возможным преодолеть изолированность привычной модели трех линий защиты, с неизбежно присущей ей сингулярностью и эскалацией внутренних конфликтов, посредством независимого союза со сторонними наблюдателями, что, в свою очередь, порождает альтернативные точки роста и развития организации.

Список литературы

1. Измалков С.Б., Сонин К.И. Основы теории контрактов // Вопросы экономики. 2017. № 1. С. 5–21.
2. Black D. On the Rationale of Group Decision-making // Journal of Political Economy. 1948. Vol. 56. Pp. 22–34.
3. Grossman S.J., Hart O.D. An Analysis of the Principal-Agent Problem // Econometrica. 1983. Vol. 51. No. 1. Pp. 7–45.
4. Jensen M.C., Meckling W.H. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure // Journal of Financial Economics. 1976. Vol. 3. No. 4. Pp. 305–360.
5. Basel Committee on Banking Supervision: Revisions to the principles for the sound management of operational risk // Consultative Document, 2020.
6. Basel Committee on Banking Supervision: The "four lines of defence model" for financial institutions // Occasional Paper. 2015. No. 11.

Ознакомиться с презентацией

С.В. ДЕМИДОВ
Заместитель Председателя Правления по информационной безопасности,
Группа «Московская Биржа»

ИНТЕГРАЦИЯ КИБЕРРИСКОВ В СИСТЕМУ УПРАВЛЕНИЯ РИСКАМИ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Аннотация

Статья посвящена вопросу интеграции киберрисков в систему управления рисками финансовых организаций. В статье приводятся основные факторы, подчеркивающие значимость киберрисков в структуре рисков финансовой организации. Выделяются ключевые аспекты, в рамках которых реализуется интеграция киберрисков в систему управления рисками. Также в статье рассматривается процесс идентификации и оценки киберрисков. Дается краткое представление об основных преимуществах и недостатках современных инструментов и методов оценки киберрисков. Приведены основные аспекты унификации процесса оценки киберрисков для финансовой организации. Рассмотрены основные подходы управления киберрисками.
Список ключевых слов: кибериски, управление рисками, финансовые организации, оценка рисков, цифровая безопасность.
JEL коды: G20, D81, G32.

В современном мире кибератаки становятся все более частыми и разрушительными для бизнеса. Киберинциденты могут привести к утечке конфиденциальной информации, финансовым потерям, нарушению работы систем и даже к потере репутации компании. Поэтому кибериски сегодня являются неотъемлемой частью общего ландшафта рисков любой организации. Игнорирование этих угроз может привести к серьезным последствиям, поэтому важно интегрировать управление киберрисками в общую систему управления предприятием.

Кибериски становятся все более значимыми для организаций любого размера и сферы деятельности. Это связано с тем, что современные компании активно используют цифровые технологии, интернет-ресурсы и облачные сервисы, а также хранят большие объемы данных о клиентах, сотрудниках и партнерах. Основные факторы, благодаря которым киберриск занимает важное место среди других видов риска:

1. Регуляторика

Банк России, ФСТЭК, ФСБ, Роскомнадзор, Минцифры устанавливают определенные стандарты и нормы, которым должны соответствовать организации для обеспечения безопасности своих информационных систем. Несоблюдение этих стандартов может привести к утрате лицензий, разрешений или аккредитаций, что негативно скажется на финансовой организации. Кроме того, нарушение регуляторных требований в области информационной безопасности может повлечь

за собой серьезные штрафы и санкции. В России в ближайшее время ожидается внесение поправок в КоАП, в рамках которых нарушение законодательства в области обработки персональных данных (Федеральный закон № 152-ФЗ «О персональных данных») будет нести за собой значительные штрафы.

2. Уязвимости

Уязвимости создают точки входа для злоумышленников, которые могут использовать эти слабые места для осуществления атак. Уязвимости могут присутствовать в самых разных компонентах информационных систем – начиная от программного обеспечения и заканчивая аппаратным обеспечением. Это создает множество возможностей для злоумышленников найти и эксплуатировать слабые места. Особую опасность представляют уязвимости нулевого дня, поскольку они еще неизвестны производителям программного обеспечения или оборудования, и, соответственно, отсутствуют официальные патчи или исправления для их устранения.

3. Увеличение числа кибератак

С каждым годом количество и сложность киберпреступлений растут. Кибермошенники разрабатывают новые методы атак, такие как фишинг при помощи нейросетей (Deepfake), атаки на модели машинного обучения, программы-вымогатели (ransomware), атаки через уязвимости программного обеспечения и так далее. Атаки могут привести к утечке конфиденциальной информации, финансовым потерям и нарушению работы бизнеса.

4. Импортозамещение

Отечественные или замещающие иностранные аналоги продукты могут быть менее зрелыми и проверенными временем, чем их зарубежные конкуренты. Это означает, что они могут содержать больше багов и уязвимостей, которые еще не были выявлены и исправлены. При переходе на отечественные или альтернативные зарубежным решениям продукты и технологии компании могут сталкиваться с новыми и незнакомыми системами, которые требуют времени на освоение и интеграцию. Это может увеличить вероятность ошибок в настройке и эксплуатации, что создает дополнительные уязвимости.

5. Зависимость от технологий

Современные бизнес-процессы сильно зависят от цифровых систем и сетей. Даже кратковременный сбой в работе IT-инфраструктуры может парализовать работу компании и привести к значительным убыткам. Например, DDoS-атаки могут сделать недоступными веб-сайты и онлайн-сервисы, что особенно критично для финансовых компаний.

6. Внутренние угрозы

Помимо внешних угроз, существуют внутренние, связанные с действиями сотрудников. Недобросовестные сотрудники могут умышленно или случайно нанести ущерб компании путем передачи конфиденциальных данных третьим лицам. Также большую угрозу составляют атаки на цепочки поставок, когда из-за проникновения в инфраструктуру подрядчика возможно последующее проникновение в инфраструктуру финансовой компании.

7. Репутационные потери

Утечка данных или успешная кибератака могут нанести серьезный ущерб репутации компании. Клиенты теряют доверие к организациям, которые не смогли защитить их данные, что приводит к оттоку клиентов и снижению доходов.

Правильная интеграция киберрисков в общий процесс управления рисками дает возможность руководству компании и наблюдательному совету получить полное представление обо всех аспектах рисков, связанных с деятельностью финансовой организации. Это помогает принимать взвешенные решения и эффективно реагировать на возникающие киберугрозы.

Вот несколько ключевых аспектов интеграции киберрисков в цикл управления рисками финансовой организации:

- **Идентификация рисков**

На этом этапе выявляются все возможные источники киберугроз, включая внешние (например, хакеры, вирусы) и внутренние (ошибки сотрудников, устаревшие системы) факторы. Важно учитывать специфику отрасли и особенности деятельности финансовой компании.

- **Анализ и оценка рисков**

После идентификации проводится детальный анализ каждого риска. Оцениваются вероятность возникновения инцидента и возможный ущерб. Это позволяет определить приоритетность действий по управлению киберрисками.

- **Разработка стратегий управления рисками**

Руководство определяет, какие меры следует принять для снижения вероятности и уменьшения последствий киберрисков. Возможны различные подходы: избегание риска (например, отказ от использования определенных технологий), снижение риска (внедрение защитных механизмов) или передача риска (страхование).

- **Реализация мер по митигации и контроль снижения рисков**

Разработанные стратегии реализуются на практике. Это включает внедрение технических решений, обучение персонала, проведение регулярных проверок и тестов. Важным элементом является постоянный мониторинг эффективности принятых мер.

- **Обратная связь и корректировка**

По мере изменения внешней среды и внутренних условий компании система управления рисками должна адаптироваться. Регулярные отчеты и обратная связь позволяют своевременно вносить необходимые коррективы в стратегии и планы.

Преимущества правильной интеграции киберрисков

Комплексный подход. Учет киберрисков, наряду с другими видами рисков (финансовыми, операционными, юридическими), обеспечивает целостное понимание всей картины угроз.

Повышение устойчивости. Компания становится менее уязвимой перед внешними и внутренними угрозами благодаря внедрению эффективных мер защиты.

Оптимизация ресурсов. Интеграция киберрисков позволяет рациональнее распределять ресурсы между различными направлениями управления рисками исходя из реальной оценки угроз.

Соответствие требованиям регуляторов. Соблюдение нормативных актов и стандартов в области информационной безопасности снижает вероятность штрафов и санкций со стороны контролирующих органов.

Улучшение репутации. Надежная система управления рисками повышает доверие клиентов и партнеров, что положительно сказывается на имидже компании.

Руководители компании и члены наблюдательного совета играют ключевую роль в процессе управления киберрисками. Они должны:

- обладать достаточными знаниями в области кибербезопасности для принятия обоснованных решений;
- участвовать в разработке и утверждении стратегий по управлению киберрисками;
- контролировать выполнение планов и отслеживать результаты;
- поддерживать культуру информационной безопасности внутри компании.

Таким образом, интеграция киберрисков в общую систему управления рисками помогает обеспечить устойчивость и безопасность финансовой компании, минимизировать убытки и поддержать конкурентоспособность на рынке.

Оценка киберрисков – важный процесс, который помогает организациям определить уровень потенциального ущерба от различных типов атак и инцидентов, связанных с информационными технологиями.

В основе оценки лежат факторы и угрозы.

Киберугроза представляет собой конкретное событие или условие, которое может нанести вред информационной системе или данным организации. Она представляет собой источник опасности, который может стать причиной киберриска. Такими источниками могут быть уязвимости в программном обеспечении, вредоносное ПО, нарушения при разработке и эксплуатации систем, сбои и отказы и так далее. В рамках процесса управления киберриском важно определить источники угроз, набор характерных факторов и уязвимостей, способных повлиять на инфраструктуру компании, понять, как эти угрозы могут реализоваться. На основе собранной информации следующим шагом будет проведение оценки киберрисков.

Если киберугроза – это событие или условие, то киберриск – это потенциальная возможность того, что определенная угроза приведет к негативным последствиям для организации. Он определяется сочетанием двух факторов: вероятности наступления события и потерь, которые возникнут в результате этого события. Эти факторы лежат в основе оценки киберрисков. Сама по себе оценка киберрисков – это сложный процесс, так как большой объем киберугроз не всегда говорит о наличии высоких рисков для финансовой компании, так как для нейтрализации угроз реализуются различные компенсирующие меры.

Оценив киберриски, можно понять их высокую значимость для финансовой организации. Последствия от реализации киберугроз могут превышать риск-аппетит организации, так как киберриск может спровоцировать реализацию других видов риска: правового, регуляторного, репутационного, финансового и других. На сегодняшний день известно о случаях, когда компании становились банкротами после реализации киберрисков. И чем больше компания, тем сложнее ее инфраструктура, тем выше вероятность и серьезнее последствия реализации киберугроз. Для финансовых компаний эта взаимосвязь особенно сильна.

Контроль и управление киберриском должны осуществляться на операционном, тактическом и стратегическом уровне. Операционный уровень показывает защищенность компании в момент времени. Для контроля риска разрабатываются ключевые индикаторы. Тактический уровень показывает уровень рисков в целом по группе, целевое соотношение риска и доходности группы. На этом уровне мониторинг киберриска осуществляется посредством установленного риск-аппетита. Стратегический уровень – это уровень общих стратегических целей, зоны фокуса. В его рамках осуществляется мониторинг стратегических метрик.

Киберриск необходимо рассматривать в структуре ландшафта всех рисков компании. Для этого есть две основные причины:

- фокусировка на общем ландшафте будет способствовать принятию взвешенных решений, руководствуясь сравнением фактических значений, фокусировка будет на общей картине, а не на частных данных;
- процесс принятия решений руководством будет более прозрачным.

Проводится оценка рисков, вызванных угрозами, и достаточности мер, которые противостоят этим угрозам и на основании которых осуществляется оценка остаточного уровня риска.

Приведение оценок киберрисков к общему знаменателю играет важную роль в том, чтобы руководство могло правильно интерпретировать и понимать угрозы, возникающие в сфере кибербезопасности. Это позволяет стандартизировать процесс анализа и оценки рисков, обеспечивая единый язык общения между специалистами по информационной безопасности и высшим руководством.

Можно выделить несколько аспектов унификации процесса оценки киберрисков для финансовой организации:

- прозрачность и понятность:
- приведение оценок к единому формату делает их более доступными для понимания людьми без глубоких знаний в области ИТ и кибербезопасности. Руководству проще воспринимать и сравнивать разные виды рисков, когда они выражены в одних и тех же терминах.

Объективность и сопоставимость

Использование единого подхода к оценке рисков позволяет объективно оценивать их значимость относительно друг друга. Это помогает расставить приоритеты и сосредоточиться на наиболее критичных угрозах.

Эффективное распределение ресурсов

Когда риски представлены в унифицированном виде, легче определить, куда именно нужно направить усилия и инвестиции для минимизации потенциальных убытков. Это способствует более рациональному использованию бюджета на кибербезопасность.

Согласованность действий

Единообразие в оценке рисков способствует согласованности действий различных подразделений компании. Все участники процесса понимают, какие угрозы требуют первоочередного внимания, и работают над их устранением совместно.

Кибериски становятся все более значимым компонентом общего ландшафта рисков для финансовых организаций, что обусловлено ростом числа кибератак, ужесточением регуляторных требований и зависимостью бизнеса от цифровых технологий. Интеграция киберрисков в систему управления рисками позволяет компаниям получать комплексное представление обо всех аспектах угроз, связанных с их деятельностью, и принимать взвешенные решения для минимизации потенциальных убытков. Эффективное управление киберрисками требует регулярного мониторинга, внедрения технических и организационных мер защиты, а также постоянной адаптации к изменяющимся условиям внешней среды.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями). URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.
2. Федеральный закон от 02.07.2013 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.kremlin.ru/acts/bank/36875.
3. Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
4. Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».
5. Указание Банка России от 16.11.2017 № 4791-У «О внесении изменений в Положение Банка России «О требованиях к обеспечению информационной безопасности некредитными финансовыми организациями».
6. Национальный стандарт Российской Федерации. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Введ. 01.06.2018. М.: Стандартинформ, 2017.
7. Национальный стандарт Российской Федерации. ГОСТ Р 57580.2-2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. Введ. 01.03.2019. М.: Стандартинформ, 2018.
8. Межгосударственный стандарт. ГОСТ 57580.3-2022. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Основные термины и определения. Введ. 01.08.2022. Минск: Евразийский совет по стандартизации, метрологии и сертификации, 2022.
9. National Institute of Standards and Technology. Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg, MD: NIST, 2012.
10. International Organization for Standardization. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. Geneva, Switzerland: ISO, 2018. DOI: 10.3403/30271099.

Ознакомиться с презентацией