УДК 336.71

ДИАГНОСТИКА БАНКОВСКИХ РИСКОВ В ОБЕСПЕЧЕНИИ И ПОДДЕРЖКЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЭКОСИСТЕМЫ БАНКА

Пригодич Ирина Александровна, к.э.н., доцент
Полесский государственный университет
Pryhodzich Iryna, PhD, Polessky State University, prigodich.i@polessu.by

Аннотация. Статья описывает алгоритм, который помогает банкам управлять своими рисками и обеспечивать финансовую безопасность своей экосистемы. Он основан на интегрированной системе диагностики рисков, которая позволяет выявлять, оценивать и контролировать все угрозы.

Ключевые слова: безопасность, экосистема, банк, диагностика, риск, угроза, анализ, устойчивость.

Финансовая безопасность экосистемы банка – это комплексное состояние, характеризующееся ее устойчивостью к внутренним и внешним угрозам, способностью минимизировать потенциальные убытки, выполнять обязательства перед всеми участниками и сохранять доверие. В этой динамичной среде, интегрированная система диагностики банковских рисков играет критически важную роль, выступая краеугольным камнем в обеспечении и поддержке финансовой безопасности. Она представляет собой фундаментальный механизм, обеспечивающий своевременную идентификацию и оперативную реакцию банка на риски [1]. Ее роль в обеспечении финансовой безопасности экосистемы многогранна и сводится к следующим аспектам:

– объединение данных из различных источников – от внутренних банковских операций до внешних макроэкономических факторов и данных о партнерах по экосистеме, что позволяет увидеть риски не в изоляции, а в их взаимосвязи;

– анализ корреляции и паттернов, в ходе которого можно обнаружить риски, которые не видны при локальном анализе (например, риск контрагента, который может повлиять на кредитный риск банка);

– диагностика всех ключевых видов рисков: кредитный, рыночный, операционный, риск ликвидности, мошенничества, комплаенс, киберриски, репутационные риски, а также специфических рисков, связанных с функционированием экосистемы (например, риски, связанные с утечкой данных через партнеров);

– использование количественных методов (статистический анализ, стресс-тестирование, VaR) и качественные оценки для определения уровня риска, его вероятности и потенциального ущерба;

– ранжирование рисков по степени их критичности, позволяя банку сосредоточить ресурсы на наиболее значимых угрозах;

– визуализация рисков в виде матрицы «вероятность – воздействие» дает наглядное представление о профиле риска банка и его экосистемы»;

– составление объективной и актуальной информации для принятия стратегических и операционных решений;

– формирование политики, процедуры и конкретных мер по их снижению (хеджирование, диверсификация, внедрение новых систем контроля, обучение персонала);

– направление инвестиций и усилий на те области, где риски наиболее высоки;

– оценка рисков, связанных с ключевыми партнерами банка (например, их финансовой устойчивости, уровня кибербезопасности, комплаенс-практик);

– управление рисками взаимозависимости, в ходе которого определяется как проблемы одного участника экосистемы могут повлиять на банк и других партнеров, позволяя выстраивать более устойчивые связи;

– демонстрация наличия надежной системы управления рисками, что повышает доверие со стороны клиентов, регуляторов и инвесторов;

– выявление зарождающихся рисков до того, как они превратятся в серьезные проблемы;

– обеспечение постоянного мониторинга ситуации для оперативной корректировки стратегии и мер безопасности в ответ на меняющиеся условия.

В условиях растущей сложности финансовых операций, цифровизации и взаимосвязанности, интегрированная система диагностики банковских рисков является не просто вспомогательным инструментом, а ключевым элементом обеспечения и поддержки финансовой безопасности экосистемы банка. Она трансформирует управление рисками из реактивного процесса в проактивную, системную деятельность, позволяя банку не только выживать в условиях угроз, но и уверенно развиваться, сохраняя доверие и устойчивость в долгосрочной перспективе. Без мощной и интегрированной системы диагностики рисков, эффективное управление финансовой безопасностью современной банковской экосистемы становится практически невозможным. Алгоритм обеспечения безопасности экосистемы банка представим в виде таблицы.

Таблица – Алгоритм обеспечения и поддержки финансовой безопасности экосистемы банка с учетом интегрированной системы диагностики банковских рисков

Этап / Фаза	Основные задачи	Действия / Инструменты	Ответственные	Результат / Продукт
1. Диагностика и оценка рисков	Сбор и анализ данных	- сбор внутренних данных; - сбор внешних данных; - анализ данных с использованием Big Data, AI / ML.	ИТ-отдел, риск-менеджмент, комплаенс, бизнес-подразделения, центр анализа данных.	Единая база данных, предобработанные данные.
	Идентификация и классификация рисков	- определение всех возможных рисков; - создание реестра рисков.	Риск-менеджмент, комплаенс.	Реестр идентифицированных рисков.
	Количественная и качественная оценка рисков	- использование статистических моделей; - сценарный анализ, стресс-тестирование; - экспертные оценки; - оценка рисков партнеров по экосистеме.	Риск-менеджмент, финансовый департамент, комплаенс.	Оцененные уровни рисков (вероятность, потенциальный ущерб), веса рисков.
	Построение карты рисков	- Визуализация рисков по матрице «вероятность vs. ущерб»; - определение критических зон.	Риск-менеджмент, руководство банка.	Визуальная карта рисков, приоритизированный список угроз.

Этап / Фаза	Основные задачи	Действия / Инструменты	Ответственные	Результат / Продукт
	Мониторинг и актуализация	- настройка системы оповещений о значительных изменениях; - регулярный пересмотр рисков.	Риск-менеджмент, ИТ-отдел.	Актуализированная карта рисков, дашборды мониторинга.
2. Формирование стратегии финансовой безопасности	Определение целевых показателей финансовой безопасности	- установление лимитов и пороговых значений для ключевых рисков; - определение целевых показателей устойчивости.	Руководство банка, финансовый департамент, риск-менеджмент.	Целевые показатели, нормативы.
	Разработка политик и процедур	- разработка / актуализация Политики управления рисками; - разработка / актуализация правил внутреннего контроля, AML/CFT, кибербезопасности; - разработка Политики управления контрагентами; - разработка Политики управления инцидентами.	Комплаенс, риск-менеджмент, юридический отдел, ИТ-отдел, отдел кадровой работы.	Комплект документов: Политики, процедуры, инструкции.
	Определение зон ответственности	- назначение ответственных за управление каждым типом риска; - формирование риск-ориентированной организационной структуры.	Руководство банка, отдел кадровой работы.	Четкое распределение ролей и ответственности.
3. Реализация механизмов финансовой безопасности	Управление рисками	- кредитный риск: скоринг, диверсификация, залоги; - рыночный риск: хеджирование, диверсификация портфелей; - операционный риск: автоматизация, резервирование, обучение; - риск ликвидности: ALM, буферы ликвидности; - риск мошенничества: AI-мониторинг, MFA, KYC / AML; - киберриск: многоуровневая защита, аудит; - риск-комплаенс: обучение, мониторинг; - экосистемные риски: due diligence партнеров, SLA, аудит партнеров.	Бизнес-подразделения, риск-менеджмент, ИТ-отдел, операционный департамент, комплаенс.	Снижение уровней рисков, соблюдение лимитов.
	Инвестиции в технологии безопасности	- внедрение AI / ML для аналитики; - использование блокчейн; - автоматизация процессов; - системы киберзащиты.	ИТ-отдел, руководство банка.	Современная и надежная IT-инфраструктура, инструменты безопасности.
	Обучение и повышение квалификации персонала	- тренинги по рискам, комплаенсу, кибербезопасности; - формирование культуры безопасности.	Отдел кадровой работы, риск-менеджмент, комплаенс.	Повышение осведомленности и компетенций сотрудников.

Этап / Фаза	Основные задачи	Действия / Инструменты	Ответственные	Результат / Продукт
	Управление финансовой устойчивостью экосистемы	- анализ взаимосвязей рисков внутри экосистемы. - установление требований к партнерам. - мониторинг финансового состояния партнеров.	Риск-менеджмент, финансовый департамент, отдел по работе с партнерами.	Устойчивая финансовая экосистема, минимизация каскадных рисков.
4. Мониторинг, контроль и Корректировка	Непрерывный мониторинг	- отслеживание KPI, метрик безопасности; - анализ отклонений от норм; - мониторинг соблюдения политик.	Риск-менеджмент, ИТ-отдел, комплаенс, внутренний аудит.	Отчеты о мониторинге, дашборды.
	Оперативное реагирование на инциденты	- активация планов реагирования; - расследование инцидентов; - ликвидация последствий; - разработка мер по предотвращению повторений.	Отдел по управлению инцидентами, ИТ-отдел, комплаенс, риск-менеджмент, руководство банка.	Минимизация ущерба от инцидентов, уроки для улучшения системы.
	Внутренний и внешний аудит	- плановые и внеплановые проверки; - оценка эффективности системы управления рисками; - аудит соответствия требованиям регуляторов.	Внутренний аудит, внешние аудиторы, регуляторы.	Аудиторские заключения, рекомендации по улучшению.
	Корректировка стратегии и алгоритма	- анализ отчетов мониторинга, аудитов, инцидентов; - внесение изменений в политики, процедуры, IT-системы; - актуализация интегрированной системы диагностики банковских рисков; - пересмотр карты рисков.	Руководство банка, риск-менеджмент, комплаенс, ИТ-отдел.	Актуализированная стратегия, улучшенный алгоритм, повышенная финансовая безопасность.

Представленный алгоритм является комплексным и многоуровневым, направленным на проактивное управление финансовой безопасностью экосистемы банка. Он предполагает постоянное взаимодействие и обратную связь между всеми элементами. Этот алгоритм является рамочным и должен быть детализирован с учетом специфики конкретного банка, его бизнес-модели, масштаба деятельности и используемых технологий.

Список использованных источников

1. Пригодич, И.А. Диагностика банковских рисков в Республике Беларусь : монография / И.А. Пригодич. – Пинск: ПолесГУ, 2019. – с. 186.

2. Шевченко, Д.А. Теоретические аспекты формирования и развития банковских экосистем / Д.А. Шевченко, Е.В. Маркова // Финансы и кредит. – 2021. – Т. 27. № 1. – С. 2-19.