



ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ БАНКОВ В СФЕРЕ КРЕДИТОВАНИЯ

Быстрова Валерия Александровна

учащийся

Солод Виктория Алексеевна

учащийся

СИУ РАНХиГС, г. Новосибирск

Цифровая трансформация в стратегиях развития современных кредитных организаций является ключевым аспектом развития, который на протяжении последних лет акцентирует внимание на инновационных подходах. В современной экономической среде, где санкционные меры оказывают значительное воздействие, ключевым элементом для обеспечения долгосрочного благополучия и конкурентной борьбы является адаптация к неуклонным изменениям и активное внедрение новаторских подходов. Хотя это приводит к усилению конкурентной борьбы, есть и позитивный момент: возникает потребность в создании новаторских продуктов и мобильных технологий, что, в свою очередь, подстегивает инновационную активность. Таким образом, Бариленко В.И. отмечает, что «преобразования и новшества становятся не просто желательными, но и необходимыми для поддержания стабильности и способности противостоять вызовам времени»[.]. Инновации в финансовой сфере часто находят свое отражение в прогрессе других отраслей, таких как электроника, информационные технологии и связь. Это прогрессивное движение технологий служит катализатором для трансформации банковской системы, что, в свою очередь, играет ключевую роль в обновлении экономики в целом.

Важнейшую роль в укреплении финансового сектора играет доверие. В этом контексте, регуляторная политика Центрального банка России направлена на искоренение мошенничества среди участников рынка, что подчеркивает его председатель. продукты кредитования заняли третью строчку по популярности в списке банковских продуктов с долей в 9,1%, примерами которых являются предложения от Альфа-Банка по кредитованию клиентов CMS, банкоматное кредитование Промсвязьбанка, а также процессы он-лайн – одобрения ипотечных кредитов.

Кредитные учреждения часто сталкиваются с серьезными угрозами, исходящими изнутри, когда их работники замешаны в недобросовестных действиях. Такие инциденты не только влекут за собой финансовые потери, но и наносят ущерб репутации организации. Две основные формы внутренних нарушений включают в себя:

- во-первых, присвоение финансовых средств через манипуляции с программным обеспечением и осведомленность о внутренних процессах;

- во-вторых, мошенничество с использованием поддельной информации для личной выгоды.

Любая кредитная организация должна стремиться к увеличению доходов от таких продуктов, как кредитование физических и юридических лиц, ведь они представляют собой стабильный источник прибыли на протяжении долгого времени, в отличие от перечисленных продуктов, например, автокредиты не демонстрируют значительного роста или значимой рыночной доли. При анализе жизненного цикла основных финансовых продуктов в рамках матрицы эволюции, становится очевидно, что кредиты для бизнеса и личные кредиты, находящиеся в фазе «Зрелость», имеют все шансы на увеличение своего влияния на рынке и объемов продаж в будущем.

В банковских учреждениях применяют разнообразные механизмы для обеспечения безопасности процедур кредитования, включая распределение ответственностей и уникальные пароли для каждого участника процесса, с обязательным обновлением доступов в соответствии с утвержденными временными рамками. Адаптация комплексных антифродовых систем позволяет осуществлять непрерывное отслеживание всех финансовых операций, обеспечивая тем самым детализированный аудит и эффективный анализ работы кредитной организации. Благодаря строгому управлению информационной безопасностью, преступления подобного рода стали значительно менее частым явлением.

ПАО «Сбербанк» бесспорный лидер в секторе, ключевой финансовый институт в России с самой большой клиентской базой: 107,3 млн активных розничных и 3,1 млн активных корпоративных клиентов по состоянию на июль 2023 г. Доминирующее положение на рынке, разумная политика рисков, а также инновационные подходы с использованием технологии искусственного интеллекта позволяют ПАО «Сбербанк» демонстрировать высокие финансовые результаты при уверенном органическом наращивании капитала. Презентация стратегии развития на 2024–2026 гг. в декабре 2023 г. стала основным событием IV квартала 2023 г. Также вероятен пересмотр дивидендной политики на фоне сильных финансовых результатов за 2023 г. и рекордной прибыли, которые приведут к органическому росту капитала. В рамках текущего прогноза на 2023 г. размер дивидендов составляет 34 руб. на акцию при 50%-ном коэффициенте выплат, что превышает рекордный показатель 2022 г. Потенциально более серьезное ужесточение денежно-кредитной политики может подразумевать риски для дальнейшего выпуска кредитов, а также качества активов. ПАО «Сбербанк» не поменял ожиданий по стоимости риска (100–130 б.п. после 190 б.п. в 2022 г.), а текущее качество активов остается высоким при уровне просрочки в рамках отчета по РСБУ – 2,1%. Обычно самый непредсказуемый показатель – стоимость риска (CoR), что может подразумевать риски для банка



В области мошенничества выделяются две основные формы:

- работники компании злоупотребляют своим положением, информационными преимуществами и знанием внутренних процессов для присвоения активов или финансовых средств;
- работники компании содействуют в выдаче кредитов лицам, известным как недобросовестные заемщики или мошенники.

Для предотвращения таких инцидентов кредитные учреждения вводят жесткие правила, запрещающие сотрудникам манипулировать личными данными клиентов при оформлении заявлений, принимать копии удостоверяющих личность документов без проверки подлинности, а также подделывать клиентскую информацию, включая недопустимость подписи от имени клиента.

Каждый сотрудник банка несет ответственность за обеспечение прозрачности и честности в процессах работы с клиентскими данными и документацией. Как часть этой обязанности, необходимо осведомлять соответствующий отдел безопасности о любых подозрениях, связанных с внутренними махинациями внутри организации, предоставляя детали инцидента для дальнейшего расследования. В случае обнаружения подделки информации о клиентах, включая данные о работе и контактную информацию, или искажения в заявлениях, такие действия будут квалифицированы как нарушение внутренних правил и могут повлечь за собой определенные последствия. Скрытие причин отклонения запросов или нарушение иных аспектов профессионального кодекса также не допускается.

Изучение случаев нарушений в финансовом секторе позволяет выявить ключевые аспекты, способствующие совершению незаконных операций. Одним из явных стимулов для преступлений является ожидание большей прибыли по сравнению с угрозой последующего наказания. Чтобы противостоять этому, крайне важной мерой является создание и актуализация базы данных о должниках, которая бы была доступна для всех учреждений, предоставляющих займы. Предупреждение финансовых махинаций в бизнес-структурах во многом зависит от осведомленности субъектов о последствиях противоправных поступков и неизбежности воздействия закона в случае их выявления.

Чтобы минимизировать риск неправомерных действий в бизнес-структурах, руководство активно занимается просвещением своих работников и обновлением команды через перестановку персонала. Специалист в области страхования и эксперт по обеспечению безопасности в кредитной отрасли, Джеймс Э. Уитакер, который является главой компании «Whitaker Group, LLC», утверждает, что «предупреждение преступности через образовательные мероприятия и ознакомление сотрудников с последствиями нарушений, регламентированными законодательством, является эффективным методом»[2]. В то же время, защита



конфиденциальной информации клиентов получает особое внимание со стороны американских финансовых учреждений.

В современной цифровой эпохе, когда Интернет стал неотъемлемой частью нашей повседневной жизни, пользователи часто становятся жертвами хитроумных интернет-мошенников. Важно подчеркнуть, что эффективность мер безопасности определяется их способностью предотвращать финансовые преступления до того, как они произойдут. Компании по всему миру прибегают к различным стратегиям защиты, направленным на предотвращение таких инцидентов. Таким образом, ключевыми аспектами защиты являются введение временных ограничений на пребывание в системе, автоматическое отключение при бездействии, защита информации путем её шифрования, а также строгий контроль транзакций через платежные системы на предмет обнаружения подозрительной активности.

Список литературы:

1. Финансовая политика. – Электрон. текстовые дан. – Режим доступа: <http://government.ru/govworks/2/events/>. – Загл. с экрана
2. Денежно-кредитная политика // Центральный банк Российской Федерации. – Электрон. текстовые дан. – Режим доступа: <http://www.cbr.ru/DK>. – Загл. с экрана