Приложение

к постановлению Правления

Национального банка

Кыргызской Республики

от «\_\_\_\_» \_\_\_\_\_\_\_\_2025 года

№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Изменения

в некоторые нормативные правовые акты

Национального банка Кыргызской Республики

1. Внести в постановление Правления Национального банка Кыргызской Республики «Об утверждении Положения «О минимальных требованиях по управлению операционным риском в коммерческих банках Кыргызской Республики» от 15 декабря 2005 года № 37/5 следующее изменение:

Положение «О минимальных требованиях по управлению операционным риском в коммерческих банках Кыргызской Республики», утвержденном вышеуказанным постановлением, дополнить главой VI следующего содержания:

«VI. Минимальные требования к системе противодействия внутреннему и внешнему мошенничеству (антифрод)

6.1. Банк обязан обеспечить наличие и эффективное функционирование системы противодействия внутреннему и внешнему мошенничеству (антифрод) в соответствии с требованиями настоящей главы.

6.2. Требования настоящей главы применяются в качестве основного механизма противодействия внутреннему и внешнему мошенничеству в банковских информационных системах, в том числе в случае несоответствия имеющихся в банковских информационных системах алгоритмов противодействия внутреннему и внешнему мошенничеству требованиям настоящей главы.

6.3. Банк обязан разработать, утвердить советом директоров и внедрить Политику противодействия мошенничеству в системах удаленного/дистанционного банковского обслуживания (далее – Политика). Политика может быть оформлена в виде отдельного документа или являться составной частью политики управления рисками банка.

Политика как минимум должна содержать:

- стремление руководства, подтверждающее приверженность защите клиентов от внутреннего и внешнего мошенничества в системах удаленного/дистанционного банковского обслуживания;

- принципы раннего выявления, предупреждения и предотвращения мошенничества в системах удаленного/дистанционного банковского обслуживания;

- порядок применения адекватных и своевременных автоматизированных или полуавтоматизированных мер реагирования на выявленные случаи или попытки мошенничества, соразмерных оцененному уровню риска;

- меры ответственностей в соответствии с законодательством Кыргызской Республики, применяемых к сотрудникам банка за бездействие или ненадлежащие действия в сфере противодействия мошенничеству, включая мониторинг угроз, разработку и внедрение мер противодействия, а также реагирование на инциденты.

Политика подлежит пересмотру и актуализации не реже одного раза в год.

Внутренние процедуры и документы банка, регламентирующие противодействие мошенничеству в системах удаленного/дистанционного банковского обслуживания, подлежат пересмотру по мере необходимости, но не реже одного раза в два года, с учетом эффективности применяемых мер, лучшего международного опыта и актуальных угроз.

Банк обязан интегрировать вышеуказанные процедуры и документы в систему управления рисками и обеспечить ознакомление с ними всех необходимых сотрудников банка.

6.4. Банк обязан внедрить системы противодействия мошенничеству в информационных системах удаленного/дистанционного банковского обслуживания для предотвращения как внутреннего, так и внешнего мошенничеств. Эти системы должны осуществлять мониторинг и оценку риска мошенничества для каждой расходной транзакции, проводимой через системы удаленного/дистанционного банковского обслуживания. Реализация данных систем допускается двумя способами:

- в виде отдельного, независимого программного или программно-аппаратного комплекса, взаимодействующего со всеми используемыми банковскими автоматизированными системами удаленного/дистанционного банковского обслуживания.

- путем интеграции специализированного модуля противодействия мошенничеству непосредственно в каждую из используемых банковских автоматизированных систем удаленного/дистанционного банковского обслуживания.

6.5. При использовании программного обеспечения для противодействия внутреннему и внешнему мошенничеству в банковских информационных системах банк должен направить соответствующее уведомление с полным описанием реализованной архитектуры, принципов функционирования, применяемых методов оценки риска согласно требованиям Положения, в адрес Национального банка.

6.6. Система противодействия внутреннему и внешнему мошенничеству в информационных системах удаленного/дистанционного обслуживания должна производить оценку риска мошенничества в отношении каждой совершаемой расходной транзакции на основании правил, поведенческих моделей, шаблонов и результатов анализа. В результате оценки риска мошенничества система должна присваивать как минимум один из трёх признаков:

- низкий риск: транзакция безопасна;

- средний риск: транзакция подозрительна и может быть мошеннической;

- высокий риск: транзакция является мошеннической.

6.7. При присвоении транзакции среднего уровня риска на основании существенного отклонения от стандартного поведения клиента или наличия совокупности факторов банк обязан обеспечить ее обязательную проверку. Проверка может быть выполнена автоматически или вручную уполномоченным сотрудником банка. По результатам проверки банк обязан выполнить одно или несколько из следующих действий:

- переоценить уровень риска и присвоить транзакции новый уровень: низкий или высокий;

- внести необходимые изменения в правила и шаблоны системы противодействия мошенничеству в удаленное/дистанционное банковское обслуживание, дополнив их выявленными признаками мошеннических операций, выявленных при анализе транзакций с высоким уровнем риска.

- обеспечить хранение полной информации о проведенной проверке, включая результаты, полученные данные, сведения о сотрудниках, принимавших решения, и предоставленные клиенту уведомления в системе противодействия мошенничеству в дистанционное банковское обслуживание. Указанная информация подлежит хранению не менее 5 лет с момента проведения операции.

6.8. Низкий уровень риска должен присваиваться транзакциям, которые соответствуют типичному поведению пользователя, имеют незначительные отклонения от него либо прошли успешную проверку после первоначального присвоения среднего уровня риска.

6.9. Банк вправе приостановить расходные операции по банковскому счету на срок до 30 дней в следующих случаях:

- при выявлении признаков, соответствующих критериям мошенничества, установленным в пункте 6.12 настоящего Положения;

- при отсутствии от клиента подтверждающей информации, однозначно свидетельствующей о самостоятельном совершении операции;

- по уведомлению клиента о мошеннических действиях по его банковскому счету.

Банк в системах дистанционного банковского обслуживания должен предусмотреть возможность подачи физическими лицами уведомления о мошеннических действиях по его банковскому счету.

Такая возможность должна быть реализована в виде отдельной функции, обеспечивающей:

- круглосуточную доступность без необходимости обращения в отделения банка;

- простую, интуитивно понятную форму подачи уведомления, с возможностью указания ключевых параметров транзакции: дата, сумма, реквизиты получателя, описание обстоятельств и наличие доказательств;

- автоматическую фиксацию факта подачи уведомления в информационных системах банка с отметкой времени и идентификатора клиента;

- инициацию процедуры приостановки и анализа транзакции.

Уведомление, поданное через указанную функцию, подлежит незамедлительному рассмотрению и принятию соответствующих мер, по оценке транзакции, с последующим информированием клиента о принятых мерах, в том числе рекомендации по обращению в правоохранительные органы.

Банк обязан незамедлительно информировать клиента о приостановлении операции с использованием доступных каналов коммуникации (мобильное приложение, телефон, иные).

6.10. Системы противодействия внутреннему и внешнему мошенничествам в информационных системах удаленного/дистанционного банковского обслуживания обязаны формировать и поддерживать реестр запрещенных к обслуживанию идентификаторов и атрибутов, используемых при совершении мошеннических операций, в случае присвоения транзакции высокого уровня риска мошенничества. Данный реестр должен включать как минимум номер телефона, ID QR, сервисное имя (идентификатор) получателя или отправителя платежной/банковской системы, а также иные идентификаторы и атрибуты, связанные с мошеннической деятельностью.

6.11. Оценке риска мошенничества должны подвергаться все транзакции, проводимые через системы дистанционного обслуживания и связанные с:

- выдачей кредитов;

- использованием электронных QR-кодов.

- внутрибанковским и межбанковским переводом средств;

- использованием систем ГРОСС/КЛИРИНГ;

- международными переводами средств (SWIFT и другие международные системы денежных переводов);

- снятием наличных денежных средств;

- приемом платежей через POS-терминалы;

- переводом средств на криптокошельки и счета иностранных криптовалютных бирж;

- погашением задолженности из источников, не характерных для пользователя;

- использованием предоплаченных карт для приобретения товаров и услуг;

- зачислением денежных средств через депозитные устройства (кэш-ин устройства);

- транзакцией с использованием виртуальных карт;

- переводом на счета и платформы онлайн-казино, игровых сервисов и сайтов ставок;

- иными операциями, определенными банком в рамках своей политики по предотвращению мошенничества.

Банк должен определить специализированные подразделения, ответственные за мониторинг транзакций в режиме реального времени, а также регулярно пересматривать перечень операций, подлежащих оценке риска, с учетом новых схем мошенничества и изменений в цифровой безопасности.

6.12. Для целей оценки риска мошенничества при проведении транзакций банк обязан использовать критерии мошенничества, являющиеся основанием для признания транзакции подозрительной или мошеннической.

Критерии мошенничества представляют собой один или совокупность признаков и моделей поведения, свидетельствующих об отклонении от стандартной активности клиента и потенциальной попытке совершения мошеннической транзакции.

Применяемые критерии мошенничества должны включать в том числе, но не ограничиваться следующими признаками:

- аномальная частота транзакций: внезапное увеличение количества транзакций, как инициированных клиентом, так и полученных им;

- групповая аномальная активность: внезапный рост активности группы клиентов, осуществляющих транзакции, подобные по сумме, получателю или типу;

- аномальный размер (сумма) транзакций: транзакции на суммы, не соответствующие типичному поведению клиента, а также совершение платежей в непривычных для клиента категориях товаров/услуг;

- аномальное географическое положение: необычное географическое положение
(IP-адрес), регистрация с нового мобильного устройства, использование VPN или прокси-серверов;

- аномальное время проведения операций: необычное время суток или день недели для совершения транзакций клиентом;

- многократные неудачные попытки входа: повторные неудачные попытки авторизации в системе;

- частая смена контактной информации: частая смена контактных данных, особенно перед крупными транзакциями;

- совпадение с известными схемами мошенничества: соответствие транзакции признакам известных схем мошенничества;

- частые возвраты или отмены транзакций: необычно большое количество возвратов или отмененных транзакций;

- использование подозрительных получателей: переводы средств на счета получателей, идентифицированных как подозрительные;

- распределение средств на множество получателей: дробление транзакций и распределение средств на большое количество получателей;

- аномальные источники пополнения средств: пополнение счета из источников, не характерных для данного клиента;

- частое привязывание и отвязывание платежных инструментов: частая смена привязанных платежных карт или учетных записей;

- аномальные изменения в режиме доступа: изменения в режиме доступа, включение новых способов авторизации или изменение способа входа, несвойственные для данного клиента;

- несоответствие анкетных данных (домохозяйка, безработный и т.д.) частоте и сумме транзакциям;

- участие счета клиента в дроблении или укрупнении денежных средств и с быстрым переводом на другие счета клиента в другой банк;

- пополнение карты разными лицами с помощью разных инструментов с дальнейшим выводом с карты;

- иные критерии, определенными банком в рамках своей политики по предотвращению мошенничества.

6.13. Все транзакции в отношении запрещённых к обслуживанию идентификаторов должны отклоняться с соответствующим уведомлением клиента.

Банк должен разрабатывать внутренние процедуры и документы, регламентирующие порядок внесения идентификаторов в реестр запрещенных к обслуживанию, а также порядок исключения записей из него в случае обнаружения ошибок или подтверждения самостоятельного проведения операции клиентом.

В случае выявления фактов осуществления транзакции в отношении идентификаторов, обслуживание которых запрещено, а также в случае выявления фактов нарушения установленных требований в соответствии с нормативными правовыми актами Национального банка при предоставлении кредитов банк обязан возместить клиенту причиненный ущерб в результате такой транзакции.

6.14. Реестр запрещённых к обслуживанию идентификаторов может дополняться вручную сотрудниками банка на основании достоверной информации о мошеннической природе того или иного клиентского идентификатора, полученной по линии государственных органов и Национального банка, в результате публикаций в СМИ, в том числе в сети Интернет, или множественных обращений клиентов.

6.15. Реестр запрещённых к обслуживанию идентификаторов должен вестись защищённо, не допуская несанкционированного вмешательства сотрудников банка и третьих лиц, обеспечивая целостность записей.

Доступ к реестру разрешается только уполномоченным сотрудникам банка с использованием многофакторной аутентификации. Любые изменения в системе должны фиксироваться в журнале регистрации событий с указанием ответственного лица, времени внесения изменений и оснований для корректировки. Сведения из журнала регистрации событий должны храниться не менее 5 лет.

6.16. Банк должен разрабатывать и внедрять системы мониторинга эффективности мер противодействия мошенничеству, включая следующие метрики:

- доля заблокированных подозрительных операций, которые впоследствии были подтверждены как мошеннические со стороны правоохранительных и судебных органов;

- доля ложноположительных срабатываний (ошибочно заблокированных транзакций);

- среднее время реагирования на инцидент;

- количество выявленных и задокументированных способов мошенничества;

- показатель клиентского опыта и точности работы системы, включая скорость обратной связи и процент разрешения конфликтных ситуаций в пользу клиента при ошибочной блокировке;

- показатель качества ведения реестра запрещенных идентификаторов.

Результаты оценки эффективности подлежат документированию и предоставлению в Национальный банк не реже 1 (одного) раза в квартал.

6.17. Банк должен регулярно проводить тестирование систем противодействия внутреннему и внешнему мошенничеству для оценки эффективности, точности и устойчивость к новым угрозам.

Тестирование проводится не реже одного раза в год, а также при внесении значительных изменений в систему.

Обязательными являются следующие виды тестирования:

- стресс-тестирование, заключающееся в моделировании массовых мошеннических атак для проверки устойчивости системы;

- тестирование безопасности на проникновение;

- тестирование новых алгоритмов на основе актуальных способов мошенничества.

По результатам тестирования банк должен в течение 30 рабочих дней разработать и внедрить соответствующие корректирующие меры для устранения выявленных уязвимостей.

Банк должен документировать результаты тестирования и ежегодно предоставлять их результаты в Национальный банк по результатам тестирования.

Документация по тестированию подлежит хранению не менее 5 лет.».

2. Внести в постановление Правления Национального банка Кыргызской Республики «Об утверждении Инструкции по работе с банковскими счетами, счетами по банковским вкладам (депозитам)» от 31 октября 2012 года №41/12 следующее изменение:

Инструкцию по работе с банковскими счетами, счетами по банковским вкладам (депозитам), утвержденную вышеуказанным постановлением дополнить пунктом 22-5 следующего содержания:

«22-5. В случае выявления признаков, указывающих на возможный мошеннический характер расходной операции, банк вправе приостановить проведение такой операции на срок до 30 (тридцати) дней.

Порядок выявления указанных признаков, алгоритм приостановки и возобновления операций устанавливаются нормативными правовыми документами Национального банка, устанавливающих минимальные требования к функционированию систем противодействия внутреннему и внешнему мошенничеству (антифрод).».