Сергей АФАНАСЬЕВ

Риск персонала, в частности риск внутреннего мошенничества, является одним из самых значимых видов операционного риска. Проверка персонала на этапе подбора — это первичный фильтр. Второй этап — правильная организация рабочего процесса, чтобы возможности для мошеннических действий и ошибок сотрудников были минимальными. Какие методы позволяют это сделать?

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

Сергей АФАНАСЬЕВ,
КБ «Ренессанс Кредит» (ООО), начальник управления расследования мошенничества

Если посмотреть на показатели просрочки портфелей потребительских кредитов в розничных банках, то можно увидеть, что различные каналы продаж различаются по уровню риска. На рисунке показан уровень просрочки по двум типам банковских отделений:

1) банковский офис (БО): численность персонала от трех сотрудников, есть охрана, кассовый узел и видеонаблюдение;

2) микрофис (МО): один-два сотрудника, без охраны, часто в виде стойки в торговом центре.

Из графиков видно, что уровень 90-дневной просрочки на первом платеже (fpd90) в микрофисах существенно выше, чем в банковских офисах. При этом уровень одобрения в микрофисах ниже, чем в банковских офисах. То есть если выровнять уровень одобрения по этим каналам, то разница в рисках будет еще более значимой. Из графиков также видно, что разница в рисках на каналах БО и МО не зависит ни от суммы кредита, ни от профиля клиента (скоринга). Кроме того, отмеченные закономерности подтверждаются на данных разных банков и не зависят от года выдачи кредитов.

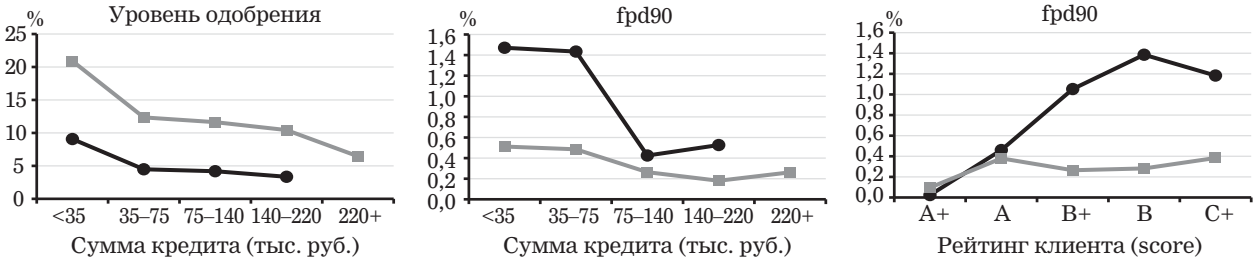
Это значит, что риски в различных типах банковских отделений объясняются не только внешними факторами (плохой клиентский поток, внешнее мошенничество), но и внутренними (ошибки персонала, внутреннее мошенничество).

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

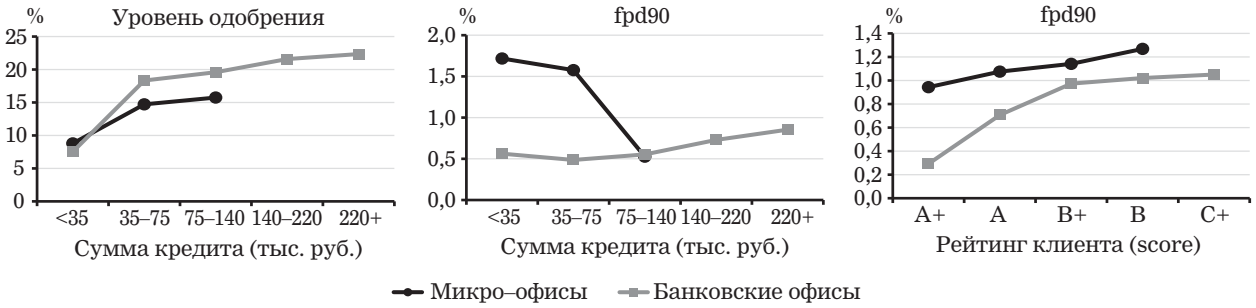
Рисунок

Уровень одобрения и 90-дневная просрочка на первом платеже в зависимости от типа банковского отделения (кредиты наличными)

Банк 1. Портфель кредитов наличными за 2014 г.



Банк 2. Портфель кредитов наличными за 2015 г.



В этой статье будут разобраны методы организации рабочего процесса сотрудников, которые позволяют защитить банк от внутреннего мошенничества, а также снизить уровень ошибок персонала.

1. Ограничение полномочий

Полномочия, предоставленные сотрудникам, могут создавать возможности для мошеннических действий. Соответственно чем большими полномочиями наделяется сотрудник, тем больше возможностей создается для мошенничества. Это значит, что в банке нужно проводить регулярный анализ избыточности полномочий и в случае необходимости ограничивать их для сотрудников. Если ограничение полномочий рассматривать с экономической точки зрения, то можно сформулировать следующее правило: чем ниже у сотрудника зарплата, тем меньше полномочий у него должно быть.

В 2011 г. в финансовой корпорации «Открытие» было выявлено внутреннее мошенничество, не имеющее аналогов на российском финансовом рынке. Трейдеры Урумов, Пинаев и Кондратюк провернули

Сергей АФАНАСЬЕВ

крупную мошенническую сделку с аргентинскими ценными бумагами по цене в четыре раза выше рынка. Чтобы афера прошла успешно, мошенники сначала создали прецедент, профинансировав из своих средств маленькую сделку по завышенным ценам, на которой корпорация «заработала». После этого Урумов, Пинаев и Кондратюк оформили сделку на $213 млн, из которых $150 млн были выведены на подставные счета мошенников. Уникальность ситуации заключалась в том, что ошибку в стоимости бумаг заметили сотрудники мидл-офиса, сообщив об этом руководству. Кроме того, на запрос главы риск-менеджмента «Открытия» предоставить ему реквизиты компаний, участвующих в сделке, мошенники ответили отказом, ссылаясь на то, что клиент крупный и хочет остаться конфиденциальным. Таким образом, Урумов и его сообщники были наделены сверхполномочиями, за счет которых им и удалось успешно провести мошенническую сделку.

Когда в «Открытии» начали разбираться с убытками, мошенничество было раскрыто. Урумов и Кондратюк были арестованы, а Пинаеву удалось скрыться в Израиле. В Британии и Швейцарии на них были заведены уголовные дела. «Открытие» по решению суда заморозило активы мошенников и вернуло часть украденных средств. Комментируя произошедшее, член правления корпорации «Открытие» Алексей Карахан отмечал: «Это история про чудовищное развращение людей: в какой-то момент они просто утратили ощущение, что воруют». На вопрос, что изменилось в компании после аферы, он отвечал так: «У нас поменялось восприятие многих процедур. Теперь понятно, что сомневаться и перепроверять нужно обязательно — в этом нет ничего плохого. И очень важно просто не нарушать те требования, которые есть»[1].

2. Конфликт интересов

Организационный конфликт интересов в банковских процессах подразумевает выполнение одним сотрудником конфликтующих функций. Так, например, функции продаж и риск-менеджмента являются конфликтующими, поскольку основная цель бизнес-подразделения — выполнять план продаж, а основная цель риск-менеджмента — минимизировать риски, что зачастую сопровождается снижением высокорисковых продаж. В результате организационного конфликта интересов могут возникать случаи оппортунистического мошенничества, когда ради выполнения плана сотрудники прибегают к нарушениям инструкций, искажению отчетности и сокрытию

[1] Виноградова Е., Оверченко М., Темерина П. Они утратили ощущение, что воруют // Ведомости, 17.02.2014.

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

информации. При организационном конфликте интересов теряет свою эффективность принцип «четырех глаз» — когда одно подразделение контролирует рабочие процессы другого.

Классическим примером организационного конфликта интересов в кредитовании является совмещение одним сотрудником (или подразделением) функций продаж и андеррайтинга (оценки клиентов). При таком подходе уменьшаются затраты на персонал и на внедрение дополнительных бизнес-процессов, но при этом отсутствует контроль правильности принимаемых решений, поскольку конфликтующие функции выполняет один сотрудник. В результате такого конфликта происходит поляризация сотрудников: одни специалисты лучше продают, но очень плохо проводят андеррайтинг, другие хорошо оценивают клиентов, но плохо продают.

Одна известная на российском рынке микрофинансовая организация построила процесс выдачи кредитов по курьерской схеме. Согласно этой схеме кредитный менеджер выезжал к потенциальному заемщику на дом или на работу, проводил оценку платежеспособности, после чего принимал решение, выдавать кредит или нет. Если решение по заявке было положительным, заемщик подписывал договор и получал деньги. Когда у заемщика наступал платежный период, этот же кредитный менеджер проводил коллекторскую работу: информировал клиента о предстоящих платежах, звонил с напоминаниями в случае просрочки, выезжал к клиенту на дом для взыскания долга. Поскольку в функциях курьерской схемы был очевидный конфликт интересов, такой подход привел организацию к массовым случаям внутреннего мошенничества. Сотрудникам, выполнявшим роли продавца, андеррайтера и коллектора, было сложно выполнять одновременно три плана: продаж, рисков и взыскания. В результате кредитные менеджеры стали «зарабатывать» за счет сокрытия от организации части взысканного с клиента долга. Мошенничество также стало возможным благодаря отсутствию должного уровня контроля, на котором микрофинансовая организация также решила сэкономить. Таким образом, согласно концепции Дональда Кресси[1], у сотрудников появилась мотивация в виде финансового давления (отсутствие премий за выполнение плана), появились возможности в виде отсутствия контроля, а оправдание, стоит полагать, сотрудники придумали себе сами. В результате руководству этой микрофинансовой организации пришлось пересматривать свои

Классическим примером организационного конфликта интересов в кредитовании является совмещение одним сотрудником (или подразделением) функций продаж и андеррайтинга.

[1] Cressey D.R. Other people's money; a study in the social psychology of embezzlement. Glencoe: The Free Press, 1953.

Сергей АФАНАСЬЕВ

процедуры, разделять конфликтующие функции по разным подразделениям и внедрять методы защиты от внутреннего мошенничества. Благодаря своевременному исправлению организационных ошибок эта микрофинансовая организация осталась на плаву и теперь успешно работает на рынке потребительского кредитования.

3. Разделение труда

Адам Смит в своем «Исследовании о природе и причинах богатства народов» писал: «Величайший прогресс в развитии производительной силы труда и значительная доля искусства, умения и сообразительности, с какими он направляется и прилагается, явились, по-видимому, следствием разделения труда».

Разделение труда можно использовать и для снижения рисков внутреннего мошенничества как один из методов ограничения полномочий. При конвейерных бизнес-процессах, к коим относится процесс выдачи кредита, метод разделения труда может быть реализован следующим способом:

— первый сотрудник (кредитный консультант) оформляет заявку на кредит;

— в случае одобрения кредита второй сотрудник (старший менеджер) проверяет данные и ставит свою подпись;

— после этого третий сотрудник (кассир) проверяет наличие подписей и выдает клиенту деньги или кредитную карту.

Принцип разделения труда не всегда требует большого количества сотрудников и может быть реализован в кредитных организациях с небольшим штатом, где часть разделенных функций может выполняться дистанционно.

В примере трейдерского мошенничества в ФК «Открытие» формально использовался метод разделения труда. Однако игнорирование функций проверки компаний и контроля параметров сделки позволило мошенникам провернуть аферу на $150 млн.

История с внутренним мошенничеством в МФО стала возможной по причине того, что сотрудники выполняли сразу несколько функций. И только после того, как функции были разделены по разным подразделениям, МФО смогла снизить критический для своего бизнеса уровень внутреннего мошенничества.

Рассмотренные выше примеры показывают: антифрод-эффект метода разделения труда достигается за счет того, что с одной стороны ограничиваются полномочия сотрудников, с другой — разделяются конфликтующие функции.

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

4. Разграничение доступов к информационным системам

Права доступа к информационным системам банка являются частным случаем полномочий. Избыточность прав доступа повышает риски внутреннего мошенничества, и, следовательно, организация должна контролировать процесс присвоения и выдачи прав сотрудникам.

Так, один из крупнейших розничных банков пострадал от внутреннего мошенничества из-за того, что наделил своих кредитных специалистов избыточными функциями в IT-системах. Сотрудник банка Шарапов и двое его друзей оформляли кредиты на существующих клиентов банка, предварительно меняя в системе банка мобильные телефоны клиентов на свои. В итоге все реквизиты и необходимые пароли по кредитам отправлялись в SMS на личные телефоны Шарапова и его подельников, после чего они снимали наличные в банкоматах. Мошенничество стало возможным благодаря тому, что у Шарапова был доступ к изменению личных данных клиентов (мобильных телефонов). Стоит отметить, что функция изменения клиентских данных была необходима кредитным специалистам для выполнения своих рабочих обязанностей: если клиент банка пришел в офис и захотел поменять свои личные данные, у кредитного специалиста должна была быть возможность сделать это быстро, не задерживая клиента. Однако не было никакой необходимости давать кредитным специалистам неограниченный доступ к таким изменениям. Проблему решили, добавив дополнительную аутентификацию клиента: доступ к изменению личных данных был возможен только при условии ввода номера паспорта клиента, который сотрудник не мог видеть в системе (информация была скрыта), при этом клиент, как правило, всегда берет с собой паспорт при посещении банковского офиса.

5. Автоматизация

Автоматизацию можно считать историческим продолжением процесса разделения труда. Она позволяет не только повысить скорость и эффективность рабочего процесса, но и обезопасить банк от внешних и внутренних угроз. Так, например, автоматический скоринг повышает качество принимаемых решений и страхует от случайных и умышленных ошибок кредитных экспертов. Автоматизированные проверки документов позволяют выявлять и отсекать подделки. Выдача кредита на карту клиента позволяет защитить банк от внутреннего мошенничества, которое практикуется при работе с наличными.

Сергей АФАНАСЬЕВ

Примеры снижения рисков мошенничества через автоматизацию бизнес-процессов можно увидеть и в других сферах бизнеса. Так, многие рестораны пользуются эквайрингом и подключают POS-терминалы для того, чтобы клиенты могли оплатить заказ банковскими картами. Подключение эквайринга можно считать автоматизацией процесса работы с наличными. Для владельцев ресторанов функция оплаты банковскими картами позволяет не только привлечь дополнительных клиентов, но и обезопасить свой бизнес от нечистых на руку сотрудников, которые при оплате наличными могут проводить часть заказов «мимо кассы».

6. Принцип «четырех глаз»

Важным элементом контроля рисковых операций является принцип «четырех глаз», известный также как правило «двух людей». Использование принципа «четырех глаз» снижает не только уровень ошибок, но и риски внутреннего мошенничества, поскольку для совершения противоправных действий требуется сговор всех сотрудников, участвующих в согласовании. Математический эффект этого принципа заключается в следующем: если вероятность совершения мошенничества каждым сотрудником составляет p, то вероятность совершения мошенничества двумя сотрудниками в сговоре составит p^2 (для наглядности считается, что события независимы). То есть если предположить, что $p = 10\%$, то вероятность мошенничества в сговоре составит $p^2 = 1\%$ (т.е. при увеличении уровня бюрократии в два раза вероятность мошенничества снизится в 10 раз).

Несмотря на математически выверенный эффект принципа «четырех глаз», среди сотрудников встречаются настолько смелые и находчивые, что их не останавливает никакая защита «четырех глаз». Одна из таких мошенниц на протяжении 2,5 лет воровала деньги со счетов клиентов банка, в котором она работала кредитным специалистом. Когда служба безопасности банка раскрыла эту мошенническую схему, сотрудница раскаялась, описав все детали схемы в своей объяснительной (инициалы и фамилии изменены):

«Я, Матвеева И.С., работала в банке с 12.2007 по 20.05.2010 в должности кредитного специалиста. Совершила хищения денежных средств с закрытых кредитов, а именно перевела положительные остатки с кредитных счетов клиентов. Выбор клиентских счетов осуществлялся в случайном порядке, а именно когда я работала со счетами клиентов (по заявлениям, жалобам и т.д.). Денежные средства похищались следующим способом: видя положительный

остаток на счете клиента, я переводила его на сторонние счета. Перевод осуществлялся следующим образом. Я от имени клиента собственноручно писала заявления на перевод денежных средств, слегка изменяя почерк, и выкладывала их на ресепшн. Сотрудники офиса подписывали их, не зная о том, кто писал данные заявления. Денежные средства переводились на 5 счетов на четверых моих знакомых, а именно: Петренко Т.В., Абрамовой Н.А. (2 счета), Казаковой М.М. и Маркиной О.А. Все вышеперечисленные лица являются моими знакомыми, они снимали перечисленные мною средства и передавали их мне. Откуда им поступали средства, они не знали. Денежные средства похищались мною с 2008 г. по конец 2010 г. Свою вину в хищении денежных средств со счетов клиентов признаю полностью. Обязуюсь вернуть похищенные мною средства в размере 1 563 973,79 руб. в срок до конца декабря 2011 г. Прошу не передавать материалы в органы внутренних дел, так как полностью раскаиваюсь в содеянном и обязуюсь возместить ущерб, причиненный банку».

Чтобы раскрыть это мошенничество, сотрудникам службы безопасности банка пришлось допросить всех сотрудников, работавших в банковском офисе за последние несколько лет. При допросах выяснилось, что Матвеева также использовала свою подругу и коллегу по работе Надежкину, которая неоднократно подписывала поддельные заявления на возврат. Даже когда Матвеева уволилась, она еще несколько раз приходила в офис банка с поддельными заявлениями и просила Надежкину их подписать.

Этот кейс показывает, что принцип «четырех глаз» не защищает банк от внутреннего мошенничества на 100%. Чтобы избежать подобных мошеннических схем, необходимо применять и другие методы, которые будут разобраны далее.

7. Функция «Большого Брата»

Одной из модификаций принципа «четырех глаз» является функция «Большого Брата», согласно которой за действиями каждого сотрудника кто-то наблюдает. Функцию «Большого Брата» может выполнять второй сотрудник, который во время совершения значимых операций находится рядом с исполнителем. Для пресечения фактов внутреннего мошенничества любой сотрудник может доложить своему руководству или в службу безопасности банка о противоправных действиях своего коллеги. Чтобы «информаторы» чувствовали себя защищенными, можно использовать анонимный почтовый ящик, адрес которого размещен на интернет-портале банка. Функцию «Боль-

Сергей АФАНАСЬЕВ

шого Брата» также выполняют технические решения, такие как видеонаблюдение, запись телефонных звонков, логирование операций в информационных системах банка и др. Рассылка информационных материалов и публикации в СМИ о раскрытых случаях внутреннего мошенничества также работают по принципу «Большой Брат следит за тобой».

Эффективность функции «Большого Брата» можно проиллюстрировать примером массового оппортунистического мошенничества, выявленного в крупном розничном банке. Ради выполнения планов продаж сотрудники банковских офисов выдавали кредиты на большую сумму, чем требовалось клиентам. Превышающий остаток сотрудники оформляли как частично досрочное погашение (ЧДП), а клиенту в итоге выдавалась требуемая сумма. Чтобы клиент согласился на такую схему, сотрудники банка не оставляли ему выбора: предоставляли ложную информацию, что банк может выдать только максимально одобренную сумму, которая превышала требуемую. Ситуации доходили до абсурда: когда одному из клиентов потребовалось 60 тыс. руб., ему оформили максимальный лимит на 300 тыс. руб., а 240 тыс. руб. вернули в этот же день как частично досрочное погашение. По существующей на тот момент мотивационной схеме сотрудникам банка в план продаж засчитывалась вся оформленная сумма кредита и не вычитались досрочные погашения. После того как обман был раскрыт и злостные нарушители наказаны, всем сотрудникам банка было разослано письмо с предупреждением, что манипуляции с планами продаж впредь будут выявляться, а нарушители понесут строгие наказания вплоть до увольнения. Эффект этой коммуникации оказался впечатляющим: через месяц после отправки письма доля контрактов с ранними ЧДП снизилась с 4,7 до 1% по денежной сумме, то есть почти в пять раз.

8. Текущий и последующий контроль

Другой модификацией принципа «четырех глаз» является текущий и последующий контроль. Контроль в текущем режиме может осуществляться по выборочным операциям. Так, например, случайную выборку кредитных заявок можно отправлять на верификацию и андеррайтинг. Последующий контроль осуществляется по уже подтвержденным операциям. Например, сотрудники бэк-офиса могут проверять комплекты документов по выданным кредитам на ошибки и признаки совершения мошеннических действий.

В качестве последующего контроля также используют процедуру Welcome Calls — звонок клиенту через некоторое время после оформ-

ления договора. Процедура Welcome Calls позволяет выявлять и предотвращать внутреннее мошенничество, а также снижать уровень ошибок сотрудников, работающих с клиентами. Звонки осуществляются выборочным клиентам в зависимости от уровня риска канала продаж. При внедрении выборочного контроля необходимо руководствоваться правилом «критической массы», то есть отправлять на проверку такое количество операций, которое было бы ощутимо и заметно для сотрудников.

С помощью процедуры Welcome Calls можно не только дисциплинировать сотрудников, но и выявлять случаи партнерского мошенничества. Один из таких случаев произошел в розничном банке, занимающемся POS-кредитованием. Заемщики, оформившие POS-кредит в одной из торговых точек, попадали «на прозвон» к сотрудникам колл-центра банка. По результатам звонков четверо из пяти клиентов оказались неконтактными. Информация была передана аналитикам, которые провели расследование и выявили, что личные данные по неконтактным клиентам пересекаются: в кредитных заявках были указаны одинаковые адреса, совпадающие мобильные и рабочие телефоны. Среди неконтактных клиентов также встречались заемщики, проживающие в удаленных от торговой организации регионах, что нетипично для поведения обычного клиента. При проведении расследования удалось найти контакты и дозвониться до пострадавших людей, на документы которых были оформлены кредиты. Они и сообщили, что не оформляли кредиты в этой торговой организации, но при этом посещали данную торговую точку, чтобы купить SIM-карту или сделать ксерокопии документов. По результатам расследования был разоблачен руководитель группы продаж торговой организации, который оформлял мошеннические кредиты по ксерокопиям чужих документов.

Стоит отметить, что мошенничество было выявлено через две недели после оформления мошенником первого кредита. И если бы в банке не была запущена процедура Welcome Calls, первые просрочки, возможно, были бы заметны через полтора-два месяца после начала мошенничества.

9. Метод «тайный покупатель»

Еще одной модификацией принципа «четырех глаз» является метод «тайный покупатель» (Mystery Shopper). В целях снижения рисков внутреннего мошенничества такие проверки проводят сотрудники безопасности. Проверки методом «тайный покупатель» трудоза-

Сергей АФАНАСЬЕВ

тратны, поэтому проводятся по выборочному количеству сотрудников. Для снижения уровня мошенничества необходимо, чтобы количество проверок достигало «критической массы», тогда сотрудники будут понимать, что любой пришедший клиент может оказаться сотрудником безопасности в лице «тайного покупателя». Иногда для проекта «тайный покупатель» привлекают стороннюю организацию, а результаты направляются на обработку аналитикам или сотрудникам безопасности.

Результаты проверок «тайных покупателей» можно также использовать для аудита бизнес-процессов в офисах продаж. Так, в одном POS-банке, входящем в группу торговой сети сотовой связи, с помощью процедуры Mystery Shopper было выявлено, что 40% сотрудников продаж допускали грубые нарушения при оформлении кредитов, в том числе и нарушения нормативов Банка России. По результатам проверок руководство банка приняло решение усилить контроль за работой сотрудников и ужесточить политику наказаний за допущенные нарушения.

В другом розничном банке по результатам проверок Mystery Shopper было выявлено, что уровень нарушений в банковских офисах в два раза ниже, чем в микроофисах (офисах с одним сотрудником). Это исследование показало эффективность принципа «четырех глаз» и позволило скорректировать продуктовые политики и требования к клиентам в зависимости от канала продаж.

10. Ротация персонала

Ротация персонала как метод снижения рисков мошенничества была заимствована банками из игорного бизнеса, где в казино этот метод применяется при организации работы крупье (чиперов, дилеров и инспекторов). Про сотрудников казино ходит много интересных историй и легенд. Одна из таких историй произошла в голландском казино Holland Casino, где несколько лет работал титулованный дилер китайского происхождения Хон-Кии Мэн. Мастерство Мэна было настолько отточенным, что официальная комиссия Нидерландов три года подряд присваивала Мэну звание лучшего крупье года по блэкджеку. За его виртуозными действиями приходило наблюдать много профессиональных игроков и обычных людей. Но однажды один из учеников Мэна, наблюдая и осваивая все тонкости дилерского искусства, заметил, что его заслуженный учитель часто переплачивает игрокам, которые имеют выигрышную руку. О своем наблюдении зоркий ученик доложил руководству, которое начало расследование в отношении Мэна. В итоге руководству Holland

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

Casino удалось уличить Мэна в мошенничестве, после чего он был арестован и выведен из зала казино в наручниках. По результатам расследования выяснилось, что Мэн вступал в сговор с третьими лицами и на протяжении трех лет обманывал казино на крупные суммы. Ущерб, нанесенный казино, составил порядка 1 млн евро.

Чтобы минимизировать риски мошеннических сговоров с сотрудниками казино, дилеров меняют между столами, как правило, каждые 20 минут. Более того, ротация осуществляется не только между столами, но и по типам игр, когда один дилер может сначала обслуживать стол с блэкджеком, потом с рулеткой, потом с покером и т.д. Также иногда проводится ротация по ролям, когда сотрудник сначала выполняет роль дилера, потом инспектора или чипера и т.д. Такая ротация позволяет минимизировать время контакта дилера с одним игроком, а значит, и риски мошеннических сговоров.

Метод ротации персонала применяется и в банковской сфере, когда один кредитный специалист работает несколько дней в одном офисе, потом его переводят в другой офис и т.д.

Отсутствие ротации может стать причиной внутреннего мошенничества со стороны сотрудников, которые долго работают в банке и хорошо знают все слабые места в бизнес-процессах. Мошеннические схемы сотрудников-старожилов, как правило, очень продуманы и долгосрочны, вследствие чего банк может понести большие потери.

11. Ограничение доступа в нерабочее время

Используя принципы «четырех глаз» и «Большого Брата», организация может существенно снизить риски мошенничества. Открытые рабочие залы (openspace), заполненные сотрудниками, хорошо подходят для реализации указанных принципов. С другой стороны, личные кабинеты с глухими стенами могут стать той самой возможностью, необходимой сотруднику для совершения мошеннических действий. Об этом знали и наши классики: все свои самые страшные преступные замыслы Раскольников обдумывал в маленькой закрытой комнатушке. В розничном кредитовании регулярно выявляются мошеннические случаи, когда сотрудник оформляет мошеннические заявки по вечерам после окончания рабочего дня или ночью из дома, если есть доступ к банковской системе через веб-браузер. Число таких случаев можно снизить, если ограничить доступ к банковским системам и офисам в нерабочее время. Если сотрудник желает поработать сверхурочно, необходимо, чтобы непосредственный руководитель согласовал эту возможность со службой безопасности банка. Ограничивая доступ сотрудников к системам

Сергей АФАНАСЬЕВ

в нерабочее время, банк, с одной стороны, уменьшает возможности для совершения мошеннических действий, с другой — увеличивает риски мошенника «быть пойманным».

В рассмотренном в п. 4 примере внутреннего мошенничества сотрудник банка Шарапов и его сообщники оформляли мошеннические кредиты на существующих клиентов банка. Чтобы оставаться «незамеченными», они использовали логин и пароль своей коллеги, которые успешно переписали из ее корпоративной почты (среди сотрудников практиковалась передача доступа к своей корпоративной почте). Подозрение в первую очередь пало на сотрудницу, с логина которой оформлялись кредитные заявки. Однако во время оформления кредитов сотрудница находилась в отпуске, а история, сохраненная в лог-файлах, показала, что некоторые заявки оформлялись ночью с домашних компьютеров. По IP-адресам и удалось выйти на настоящих исполнителей. Чтобы распутать это дело, антифрод-аналитикам пришлось несколько дней запрашивать и анализировать различную информацию по мошенническим кредитам. А сотрудники службы безопасности несколько дней допрашивали сотрудников, входящих в окружение Шарапова. Блокировка доступа в нерабочее время позволила бы создать дополнительный барьер для мошенников, и, возможно, мошенничество было бы выявлено быстрее.

Рассмотренные методы организации рабочего процесса (таблица) снижают риски не только внутреннего, но и внешнего мошенниче-

Таблица

Антифрод-мероприятия при организации рабочего процесса сотрудников

Название	Описание
1. Ограничение полномочий	Сотрудник наделяется только теми полномочиями, которые необходимы для выполнения его рабочих обязанностей (подписание чеков, выдача кредитов, оформление документов, подписание приказов и т.д.). Избыточные полномочия не предоставляются
2. Конфликт интересов	Организационный конфликт интересов подразумевает выполнение одним сотрудником конфликтующих рабочих обязанностей. Например, функции продаж и риск-менеджмента являются конфликтующими. Для минимизации рисков внутреннего мошенничества организационная структура в банке должна быть выстроена таким образом, чтобы количество конфликтующих рабочих функций внутри каждого подразделения было минимальным
3. Разделение труда	Разделение труда позволяет ограничить полномочия сотрудников и доступ к IT-системам банка. Разделение труда хорошо подходит для конвейерных бизнес-процессов, например для процесса выдачи кредитов
4. Разграничение доступов к информационным системам	Сотруднику предоставляются только те доступы в IT-системы банка, которые необходимы для выполнения его рабочих обязанностей. Избыточные права доступа не предоставляются

Как снизить риски внутреннего мошенничества через организацию рабочего процесса сотрудников?

Окончание таблицы

Название	Описание
5. Автоматизация	Автоматизация снижает влияние человеческого фактора на банковские процессы, ограничивает полномочия и доступы для сотрудников, то есть позволяет обезопасить банк от внешних и внутренних угроз
6. Принцип «четырех глаз»	Согласно принципу «четырех глаз» для подтверждения каждой значимой операции требуется согласование минимум двух сотрудников. Использование принципа «четырех глаз» снижает риски мошенничества, поскольку для совершения противоправных действий требуется сговор всех сотрудников, участвующих в согласовании
7. Функция «Большого Брата»	Согласно принципу «Большого Брата» за действиями каждого сотрудника должен кто-то наблюдать. Функцию «Большого Брата» могут выполнять второй сотрудник, а также технические решения, такие как видеонаблюдение, запись телефонных звонков, логирование операций в информационных системах и др. Рассылка информационных материалов и публикации в СМИ о раскрытых фактах мошенничества также выполняют функцию «Большого Брата»
8. Текущий и последующий контроль	Текущий и последующий контроль являются модификациями принципов «четырех глаз» и «Большого Брата». Такой контроль может осуществляться по выборочным операциям. Например, случайную выборку кредитных заявок можно отправлять на дополнительные проверки андеррайтинга (текущий контроль) или сотрудники бэк-офиса могут проверять комплекты документов на признаки совершения мошеннических действий (последующий контроль)
9. Метод «тайный покупатель»	Согласно методу «тайный покупатель» специально подготовленные люди осуществляют проверки под видом потенциальных/реальных клиентов. В целях снижения рисков мошенничества проверки проводят сотрудники безопасности банка, которые фиксируют нарушения и мошеннические действия со стороны сотрудников
10. Ротация персонала	Ротация персонала между офисами банка позволяет снизить число мошеннических сговоров как между сотрудниками банка, так и между сотрудниками банка и внешними преступными группировками
11. Ограничение доступа в нерабочее время	Ограничив доступ сотрудников к рабочему месту и IT-системам банка в нерабочее время, можно снизить уровень внутреннего мошенничества, так как уменьшаются возможности для совершения противоправных действий в условиях отсутствия в офисе посторонних наблюдателей. Для сверхурочной работы необходимо получить согласование от руководителя и сотрудников службы безопасности банка

ства, поскольку с правильно работающими процедурами и сотрудниками мошеннику сложно реализовать свой план. Однако использование всех рассмотренных методов не всегда экономически целесообразно, поэтому банку необходимо найти свой баланс между уровнем безопасности и затратами на антифрод-мероприятия.