XXXXXXXXXX

Операционный риск включает в себя несколько видов риска, среди которых одним из самых значимых является риск персонала. К риску персонала, в свою очередь, относится внутреннее мошенничество, за выявление и предотвращение которого отвечают аналитики и сотрудники службы безопасности. Но что делать, если источником риска становятся сами проверяющие? На кого в таком случае возложить ответственность и контроль? Как уменьшить этот вид риска?

Роль человеческого фактора при расследовании внутреннего мошенничества

Сергей АФАНАСЬЕВ,
риск-менеджер[1]

Математика ошибок

Одна из возможных схем выявления внутреннего мошенничества в розничном кредитовании представляет собой процесс, состоящий из четырех этапов (рис. 1).

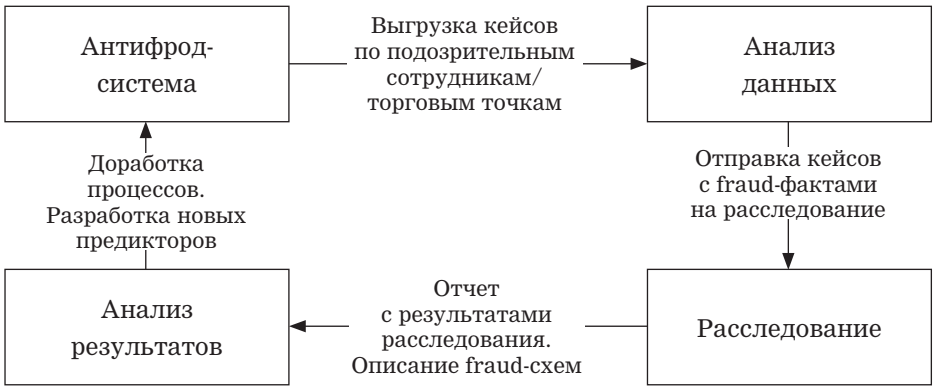
На первом этапе работает антифрод-система, которая в автоматическом режиме выявляет подозрительных сотрудников и партнеров (например, торговые точки в POS-сегменте). Антифрод-система формирует список кейсов, которые направляются на ручной анализ к сотруднику аналитического подразделения. На втором этапе аналитик проверяет кейсы, анализирует выгруженные подозрительные факты, убирает «мусорные» данные и, если необходимо, проводит дополнительные проверки и сбор данных. После проведения анализа сотрудник принимает решение: отправлять данные на расследование сотруднику службы безопасности или нет. На третьем этапе сотрудник службы безопасности проводит расследование, используя различные методы криминалистики: осмотр, изучение документов, получение объяснений от подозреваемых и свидетелей, ревизии, оперативно-разыскные мероприятия и др. Результаты расследования сотрудник безопасности направляет аналитику.

[1] Автор имеет 8-летний руководящий опыт в банках ХКФБ и «ТРАСТ».

Роль человеческого фактора при расследовании внутреннего мошенничества

Рисунок 1

Схема процесса выявления внутреннего мошенничества в банке



На четвертом, завершающем, этапе аналитик обрабатывает результаты расследований: смотрит, какие уязвимости в банковских процессах и программном обеспечении были обнаружены, принимает меры по устранению этих уязвимостей, строит новые алгоритмы и правила по выявлению внутреннего мошенничества, которые потом добавляет в антифрод-систему.

В описанной схеме проверку кейсов осуществляют сразу два подразделения, что, с одной стороны, увеличивает роль человеческого фактора при проверке, а с другой — позволяет соблюдать принцип «четырех глаз». Аналитик или сотрудник службы безопасности, проверяя кейсы, может ошибаться, и не всегда эти ошибки будут зависеть от компетенций проверяющего. Например, если предположить, что сотрудник при проверке кейсов ошибается всего в 1% случаев, то по формуле обратной вероятности можно оценить, с какой вероятностью этот сотрудник ошибется хотя бы один раз при проверке 100 кейсов подряд (месячный норматив для аналитика):

$$p = 1 - (1 - q)^N = 1 - (1 - 0{,}01)^{100} = 1 - 0{,}366 = 0{,}634, \quad (1)$$

где q — вероятность индивидуальной ошибки;

N — количество проверенных подряд кейсов.

Результаты, полученные по формуле (1), показывают, что даже при 1%-ном индивидуальном показателе ошибок вероятность того, что сотрудник ошибется хотя бы один раз при проверке 100 кейсов

XXXXXXXXXX

подряд, составляет 63,4%. В табл. 1 представлены различные значения вероятности ошибок p в зависимости от показателя индивидуальных ошибок q и количества проверенных кейсов N.

Давайте теперь усложним задачу и попробуем оценить вероятность двойной ошибки. Как и ранее, будем считать, что вероятность индивидуальной ошибки сотрудника при проверке кейса составляет 1%. Как и в предыдущей задаче, сотрудник должен проверить 100 кейсов подряд. Только теперь добавим дополнительное условие: каждый кейс должен быть проверен двумя сотрудниками. Для простоты вычислений будем считать, что проверки независимы, то есть решение первого сотрудника не влияет на решение второго. Теперь нам необходимо будет оценить, с какой вероятностью оба сотрудника одновременно ошибутся в одном и том же кейсе (хотя бы один раз), проверив 100 кейсов подряд.

В принятых выше обозначениях вероятность индивидуальной ошибки каждого сотрудника равна q. Тогда вероятность двойной ошибки при проверке одного кейса будет равна q^2. Соответственно при проверке одного кейса вероятность того, что хотя бы один сотрудник не ошибется, составит $1 - q^2$. Вероятность того, что хотя бы один сотрудник не ошибется при проверке N кейсов подряд, составит $(1 - q^2)^N$. Таким образом, вероятность двойной ошибки в одном кейсе при проверке N кейсов подряд определяется формулой:

Таблица 1

Вероятность совершения хотя бы одной ошибки при проверке пула кейсов

Количество проверенных кейсов (N)	Вероятность ошибки при проверке одного кейса (индивидуальной ошибки) (q), %									
	1	2	3	4	5	10	15	20	25	30
20	18	33	46	56	64	88	96	99	100	100
40	33	55	70	80	87	99	100	100	100	100
60	45	70	84	91	95	100	100	100	100	100
80	55	80	91	96	98	100	100	100	100	100
100	63	87	95	98	99	100	100	100	100	100
120	70	91	97	99	100	100	100	100	100	100
140	76	94	99	100	100	100	100	100	100	100
160	80	96	99	100	100	100	100	100	100	100
180	84	97	100	100	100	100	100	100	100	100
200	87	98	100	100	100	100	100	100	100	100

Роль человеческого фактора при расследовании внутреннего мошенничества

$$p_2 = 1 - (1 - q^2)^N. \quad (2)$$

Подставляя исходные значения в формулу (2), получим, что при $q = 0{,}01$ и $N = 100$ вероятность того, что оба сотрудника хотя бы один раз ошибутся в одном и том же кейсе, составляет всего 0,995%. Напомним, что вероятность хотя бы одной ошибки при проверке 100 кейсов подряд одним сотрудником составляет 63,4%, то есть в 64 раза выше, чем при проверке двумя сотрудниками. Чем ниже квалификация проверяющих, тем меньше эффект от двойной проверки, но даже при значении индивидуальной ошибки 5% итоговые вероятности на «дистанции» 100 кейсов отличаются в несколько раз: 99% для одинарной проверки и 22,1% для двойной. В табл. 2 представлены расчеты вероятности двойной ошибки p_2 для различных значений индивидуальных ошибок q и количества проверенных кейсов N.

Таблица 2

Вероятность совершения двойной ошибки при проверке пула кейсов

Количество проверенных кейсов (N)	Вероятность ошибки при проверке одного кейса (индивидуальной ошибки) (q), %									
	1	2	3	4	5	10	15	20	25	30
20	0,2	0,8	1,8	3,2	4,9	18,2	36,6	55,8	72,5	84,8
40	0,4	1,6	3,5	6,2	9,5	33,1	59,8	80,5	92,4	97,7
60	0,6	2,4	5,3	9,2	13,9	45,3	74,5	91,4	97,9	99,7
80	0,8	3,1	6,9	12,0	18,1	55,2	83,8	96,2	99,4	99,9
100	1,0	3,9	8,6	14,8	22,1	63,4	89,7	98,3	99,8	100,0
120	1,2	4,7	10,2	17,5	25,9	70,1	93,5	99,3	100,0	100,0
140	1,4	5,4	11,8	20,1	29,6	75,5	95,9	99,7	100,0	100,0
160	1,6	6,2	13,4	22,6	33,0	80,0	97,4	99,9	100,0	100,0
180	1,8	6,9	15,0	25,0	36,3	83,6	98,3	99,9	100,0	100,0
200	2,0	7,7	16,5	27,4	39,4	86,6	98,9	100,0	100,0	100,0

Полученные результаты показывают, что на «длинной дистанции» ошибаться могут даже высококлассные профессионалы (вероятность такого события высока). Однако вероятность двойной ошибки для специалистов высокого класса очень мала. И если сразу два сотрудника ошиблись в одном кейсе, на это стоит обратить внимание.

Человеческий фактор

Два года назад в одном крупном розничном банке произошел довольно интересный случай внутреннего мошенничества. Группа сотрудни-

XXXXXXXXXX

ков уфимского банковского офиса в составе руководителя группы продаж и трех его подчиненных оформляла мошеннические кредиты по поддельным документам. Мошенническая схема была достаточно распространенной и хорошо известной аналитикам и сотрудникам службы безопасности банка. Уникальность ситуации заключалась в том, что группа оформляла мошеннические кредиты в течение четырех месяцев, а финальные потери оказались самыми большими за всю 10-летнюю историю работы банка на рынке розничного кредитования.

Первые попытки оформления мошеннических кредитов начались в октябре. Через несколько дней антифрод-система выдала первый сигнал. Аналитик обработал кейс и направил его на расследование сотруднику службы безопасности. На мошеннические действия сотрудников банка указывали несколько выявленных фактов:

1) кредиты оформлялись по украденным паспортам (по данным сервиса ФМС);

2) у разных заемщиков совпадали номера страховых свидетельств;

3) у разных заемщиков совпадали номера мобильных телефонов.

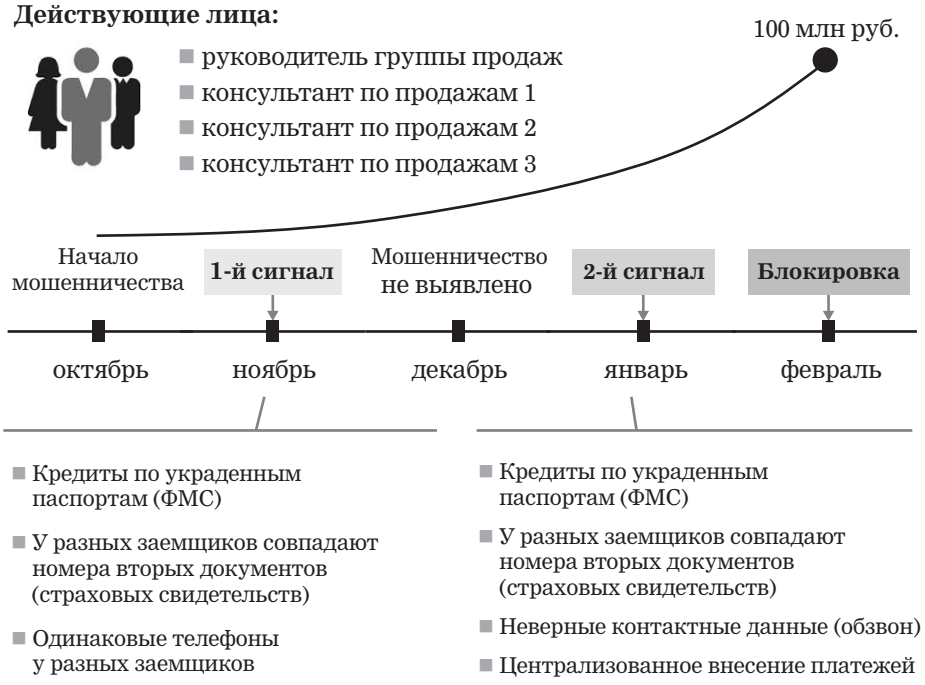
В декабре сотрудник службы безопасности прислал ответ: «Платежи по кредитам вносятся своевременно, просрочки нет. Мошенничество не выявлено». Аналитик не стал вникать в детали расследования и ушел на новогодние каникулы. В январе после праздников антифрод-система повторно выдала сигнал по тем же самым сотрудникам. Факты были аналогичными: кредиты оформлялись по поддельным паспортам, для разных заемщиков указывались одинаковые номера вторых документов и одинаковые номера мобильных телефонов. К выявленным фактам добавились результаты звонков колл-центра, согласно которым большая часть оформленных клиентов были «неконтактными». Аналитик также выявил, что первые три платежа по выданным кредитам вносились в течение одного часа и с одного терминала (поэтому показатели просрочки по сотрудникам были почти нулевые). Материалы были повторно направлены в службу безопасности, которая на этот раз вынесла вердикт: «внутреннее мошенничество». В феврале деятельность мошенников была прекращена. За четыре месяца они успели вывести из банка около 100 млн руб. (рис. 2).

Как упоминалось выше, в банке работала полноценная антифрод-система, которая позволяла выявлять внутреннее мошенничество на ранних этапах. По хронологии видно, что первый сигнал сработал в ноябре, то есть в течение месяца после начала деятельности мошенников эту деятельность могли прекратить, но не прекратили. Почему?

Роль человеческого фактора при расследовании внутреннего мошенничества

Рисунок 2

Пример внутреннего мошенничества в розничном банке



В этой истории можно увидеть несколько проблем, которые привели к таким последствиям и которые обычно относят к категории «человеческий фактор».

Первое, что бросается в глаза, — это проблема в коммуникации между аналитиками и сотрудниками службы безопасности. Аналитик отправил кейс, содержащий, казалось бы, очевидные факты мошенничества: кредитные специалисты оформили большое количество кредитов по украденным паспортам, в заявках совершенно разных заемщиков часто совпадали номера вторых документов и мобильных телефонов. Однако сотрудник безопасности счел эти факты незначимыми, прислал ответ, что никакого внутреннего мошенничества не обнаружено, и, что самое интересное, аналитик этот ответ принял.

Вторая проблема, которая не так очевидна, но также повлияла на исход дела, — это мотивация сотрудников, не зависящая от размера потерь. Убытки по обычным кейсам, которые попадают в поле зрения аналитиков, исчисляются несколькими сотнями тысяч рублей. Внутреннее мошенничество с убытком 3–5 млн руб. считается круп-

XXXXXXXXXX

ным и случается нечасто. В рассмотренном кейсе после первого сигнала убытки приблизились к отметке 20 млн руб. Элементарная математика подсказывает, что расследование по этому кейсу должно было проводиться в 10 раз тщательнее, чем по обычному. Но и аналитики, и сотрудники службы безопасности проверяли этот кейс в обычном режиме, не придавая значения масштабу потерь. Почему?

Дистанцированность от власти

Шестого августа 1997 г. на острове Гуам произошла одна из самых тяжелых катастроф в современной авиации. Авиалайнер «Боинг-747-3B5» авиакомпании Korean Air, совершая посадку, врезался в холм в местности Нимиц-Хилл и полностью разрушился. Погибли 228 человек из 254 находившихся на борту. Расследование, проводимое Национальным комитетом по вопросам транспортной безопасности (NTSB), показало, что самолет находился в отличном состоянии, а экипаж был осведомлен обо всех факторах, осложнявших посадку в тот день:

— плохие погодные условия и низкая видимость;

— неработающая курсо-глиссадная (радарная) система посадки;

— нестандартно расположенные маяки VOR, которые находились в 4 км от посадочной полосы и выводили на Нимиц-Хилл.

Американская национальная ассоциация безопасности полетов распространила заявление, в котором обвинила экипаж в ошибочных действиях. Более того, внешний аудит Korean Air показал, что в период с 1988 по 1998 гг. аварийность у корейского авиаперевозчика составляла 4,79 на миллион взлетов. Это в 17 раз выше показателей аварийности в таких компаниях, как американская United Airlines, где за тот же период данный показатель составлял 0,27 на миллион взлетов. Корейские самолеты падали так часто, что NTSB был вынужден включить в свой отчет о катастрофе на Гуаме перечень крушений, которые произошли с корейскими самолетами с начала расследования. Через год после трагедии на Гуаме, заходя на посадку в сеульском аэропорту Кимпо, разбился «Боинг-747», принадлежащий Korean Air. Через два месяца в корейском аэропорту Ульсан реактивный самолет не успел взлететь и сошел с взлетно-посадочной полосы. В аэропорту Поханга самолет «McDonnel-Douglas-83» врезался в заграждение. Затем через месяц пассажирский самолет упал на жилой район Шанхая. К этому списку можно добавить аварию грузового самолета, который спустя месяц после окончания расследования катастрофы на Гуаме рухнул при взлете в лондонском аэропорту Станстед.

Роль человеческого фактора при расследовании внутреннего мошенничества

Катастрофа в Шанхае переполнила чашу терпения общественности, и президент Южной Кореи Ким Дэ Чжун заявил, что проблемы в Korean Air — это проблемы всей страны, ставящие под угрозу ее репутацию.

В Korean Air начались серьезные преобразования. Привлеченные в компанию внешние специалисты проводили оздоровление Korean Air, руководствуясь культурологическими особенностями взаимоотношений между членами экипажа. Преобразования, проводимые экспертами, были основаны на работах голландского социолога Герта Хофстеде[1].

В 1960–1970-х годах Герт Хофстеде выполнял исследование для европейского офиса IBM. Он ездил по разным странам и проводил собеседования с сотрудниками компании, на которых расспрашивал их о том, как они разрешают те или иные конфликты, как относятся к вышестоящему руководству и т.д. Результатом исследования стала совокупность показателей, определяющих культурные характеристики различных народов. Оценка производилась по пяти параметрам:

1) дистанцированность от власти (восприятие власти) — показывает, насколько та или иная культура ценит и уважает иерархию, испытывают ли члены общества уважение к пожилым людям, пользуются ли власть имущие особыми привилегиями;

2) обособленность (индивидуализм) — измеряет степень тяготения к личностным целям, является противоположностью сплоченности (коллективизму);

3) напористость — нацеленность на достижение результата любой ценой;

4) избегание неопределенности — степень восприятия и реагирования на незнакомые ситуации;

5) стратегическое мышление — ориентированность на решение стратегических, долгосрочных целей, желание заглядывать в будущее.

Для специалистов, осуществлявших изменения в Korean Air, наибольший интерес представлял такой показатель, как индекс дистанцированности от власти. Измерения этого показателя среди пилотов разных стран показывали, что самый высокий индекс в Бразилии, Южной Корее, Марокко, Мексике и на Филиппинах, самый низкий — в США, Ирландии, Южной Африке, Австралии и Новой Зеландии. Но как это было связано с высоким уровнем авиакатастроф в Korean Air? Оказывается, самым прямым образом. Дело в том, что экипажи

Высокий (согласно шкале Герта Хофстеде) индекс дистанцированности от власти мешает построению эффективной коммуникации между аналитиками и сотрудниками службы безопасности, что, в свою очередь, повышает риск внутреннего мошенничества.

[1] http://geert-hofstede.com/.

XXXXXXXXXX

пассажирских лайнеров обычно состоят из трех человек: командира воздушного судна, второго пилота и бортинженера. В сложных ситуациях во время полета и второй пилот, и бортинженер должны сообщать командиру о его ошибках. Если командир не отреагировал, не понял или не принял во внимание полученную информацию, второй пилот имеет право взять управление самолетом на себя. Таким образом, во время полетов снижается количество ошибок экипажа, вероятность которых, как мы уже выяснили ранее, при проверке каждого принятого решения двумя пилотами в десятки раз ниже, чем когда решения принимает только один пилот. В компании Korean Air всем заправляла группа пожилых бывших офицеров военно-воздушных сил. Командиры экипажей также были выходцами из военно-воздушных сил, где большинство из них управляли военными реактивными истребителями, то есть управление было единоличным. А теперь представьте: как бы отреагировал такой командир на замечания младшего по званию второго пилота или бортинженера? К сожалению, замечания об ошибках командира в корейских экипажах делались крайне редко: и второй пилот, и бортинженер вели себя покорно, не смея перечить начальству.

Выяснив все эти нюансы, специально нанятые эксперты в первую очередь стали исправлять ситуацию с дистанцированностью от власти среди членов экипажа. Заставив весь летный состав компании перейти на англоязычное общение, они тем самым убрали иерархические барьеры, которые характерны для людей азиатской культуры. После проделанной работы компания настолько преобразилась, что с 1999 г. в ее отчетах по безопасности не было ни единого «темного пятнышка»[1].

Коммуникация

Рассмотренные проблемы в корейской авиации очень напоминают проблемы, с которыми столкнулся банк, потеряв на одном эпизоде внутреннего мошенничества 100 млн руб. Россия входит в список стран с самым высоким индексом дистанцированности от власти (93 балла из 100 возможных).

Эффективная коммуникация между аналитиками и сотрудниками службы безопасности должна выстраиваться на основе равенства и уважения к личности. Но когда культурные традиции страны требуют не перечить старшим и исполнять любые поручения руководства, выстраивание такой коммуникации становится архислож-

[1] Гладуэлл М. Гении и аутсайдеры. Почему одним все, а другим ничего? М.: Альпина Бизнес Букс, 2013.

Роль человеческого фактора при расследовании внутреннего мошенничества

ной задачей. Каждый, кто хоть раз общался с представителями банковской службы безопасности, не понаслышке знает, какие ощущения испытывает собеседник во время разговора с сотрудником службы безопасности: дискомфорт, трепет, возможно, даже страх. И это происходит не только потому, что сотрудники службы безопасности, как правило, старше своих собеседников, но и потому, что большинство из них — бывшие офицеры КГБ/ФСБ и МВД, то есть люди, когда-то наделенные достаточно большой властью. А теперь представьте, что испытывает аналитик, которому приходится общаться со службой безопасности банка каждый день. Возникает вопрос: как же тогда, учитывая все сложности, выстроить эффективную коммуникацию между аналитиками и сотрудниками службы безопасности?

На практике при выявлении внутреннего мошенничества наиболее часто используют две схемы коммуникации (рис. 3):

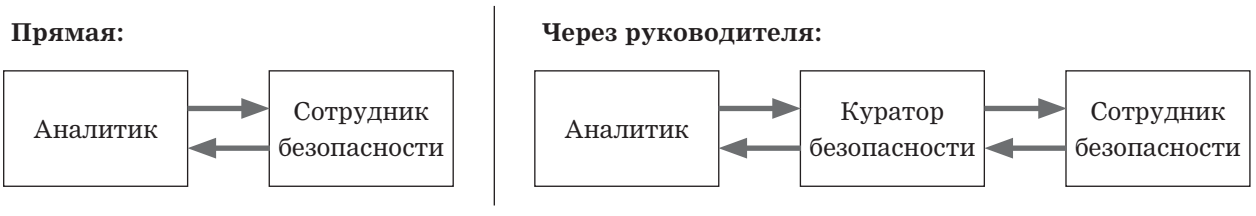
1) прямая — коммуникация между аналитиком и сотрудником службы безопасности, который проводит расследование;

2) через руководителя — коммуникация через куратора службы безопасности, который получает кейсы от аналитика и распределяет их по своим сотрудникам в филиалах. Заключения с результатами расследований также проходят через куратора.

Прямая коммуникация имеет ряд недостатков, среди которых наиболее значимый — это проблема «отцов и детей», о которой мы упомянули ранее. Молодые аналитики не могут договориться со своими старшими коллегами из службы безопасности. В результате либо аналитик становится покорным «вторым пилотом», либо между участниками процесса начинается противостояние, которое со временем перерастает в корпоративную войну. Такая участь постигла банк, кейс по которому был разобран выше: возникавшие на протя-

Рисунок 3

Схемы коммуникации между аналитиками и сотрудниками службы безопасности



XXXXXXXXXX

жении нескольких лет разногласия между аналитиками и сотрудниками службы безопасности привели к многомиллионным потерям всего лишь от одного случая внутреннего мошенничества.

Вторая схема коммуникации (через куратора службы безопасности) не решает всех культурологических проблем, но позволяет повысить качество работы за счет следующих факторов:

1) отношения: аналитик постоянно общается и договаривается только с одним куратором (снижается индикатор дистанцированности от власти);

2) оперативность: куратор контролирует сроки проведения расследования;

3) ответственность: сотрудники службы безопасности отвечают за качество проделанной работы перед своим руководителем (куратором).

Иногда, если возникают сложности с коммуникацией между аналитиками и сотрудниками службы безопасности, поднимается резонный вопрос: почему бы не отдать весь функционал по противодействию мошенничеству либо в подразделение рисков, либо в подразделение безопасности?

Во-первых, при таком подходе, скорее всего, каждое расследование будет проводиться одним сотрудником. А как мы выяснили ранее, вероятность ошибок при одинарной проверке в десятки раз выше вероятности ошибки при двойной проверке. Во-вторых, для проведения расследований необходимо владеть техниками криминалистики, в чем лучшими специалистами, безусловно, являются сотрудники безопасности. С другой стороны, чтобы разрабатывать и поддерживать автоматизированные системы по выявлению мошенничества, необходимо владеть инструментами анализа данных, в чем более сильными специалистами считаются аналитики.

Возвращаясь к схемам коммуникации, необходимо отметить, что схема коммуникации через куратора хорошо работает при сравнительно невысоких объемах ежедневно обрабатываемых кейсов (когда куратор способен контролировать процесс каждого расследования). При больших объемах расследований банки вынуждены применять схему прямой коммуникации. В таких случаях для повышения качества работы сотрудников могут быть использованы мотивационные инструменты, которые мы рассмотрим далее.

Пренебрежение масштабом

В 1993 г. экономисты провели исследование, в котором трем группам испытуемых задавали вопрос: «Сколько дополнительных налогов

Роль человеческого фактора при расследовании внутреннего мошенничества

вы готовы были бы ежегодно платить, чтобы спасти птиц, погибающих в открытых нефтехранилищах?»[1]. Формулировка вопроса для каждой группы отличалась количеством ежегодно погибающих птиц: для первой группы в вопросе фигурировало 2000 птиц, для второй — 20 000 птиц, для третьей — 200 000 птиц. Результаты опроса показали, что первая группа готова была заплатить дополнительные налоги в размере 80$ за 2000 птиц, вторая — 78$ за 20 000 птиц, а третья — 88$ за 200 000 птиц. Этот феномен получил название нечувствительности к масштабу или пренебрежения масштабом. Профессор Даниэль Канеман объясняет принцип действия этого феномена следующим образом:

«Вопрос, задаваемый Десвуджем и его коллегами, вероятно, вызывает у большинства испытуемых ментальное представление о некоем событии, возможно — образ истощенной птицы с намоченными нефтью крыльями, не способной спастись. Гипотеза об оценке по первоначальному образу утверждает, что эмоциональное влияние этого образа будет доминировать над рациональным отношением к проблеме, включая готовность платить за решение. То есть оценка по первоначальному образу автоматически означает пренебрежение к остальным деталям ситуации».

Пренебрежение масштабом было продемонстрировано и по отношению к человеческим жизням. Экономисты Ричард Карсон и Роберт Митчелл[2] исследовали, как на людей влияет информация об увеличении риска, связанного с питьем хлорированной воды. Они сообщали испытуемым, что при употреблении хлорированной воды риск смерти увеличивается с 0,004 до 2,43 на 1000 человек в год, то есть в 600 раз. Оказалось, что люди были готовы увеличить плату за очистку воды в среднем с $3,78 до $15,23, то есть всего в 4 раза.

Другая группа экономистов[3], исследуя проблему психофизической нечувствительности, нашла доказательства того, что наше восприятие ценности человеческой жизни подчиняется закону Вебера–Фехнера, то есть оценка значимости жизни осуществляется по логарифмической шкале[4].

[1] Desvousges W.H. et al. Measuring natural resource damages with contingent valuation: tests of validity and reliability. In: Contingent valuation: a critical assessment / J.A. Hausman (ed.). Amsterdam: North Holland, 1993. P. 91-159.

[2] Carson R.T., Mitchell R.C. Sequencing and Nesting in Contingent Valuation Surveys // Journal of Environmental Economics and Management. 1995. Vol. 28. No. 2. P. 155-173.

[3] Fetherstonhaugh D. et al. Insensitivity to the value of human life: A study of psychophysical numbing // Journal of Risk and Uncertainty. 1997. Vol. 14. No. 3. P. 283-300.

[4] См. также: Yudkowsky E. Cognitive biases potentially affecting judgment of global risks. Forthcoming in Global Catastrophic Risks / N. Bostrom, M. Cirkovic (eds.). August 31, 2006.

XXXXXXXXXX

Возвращаясь к примеру с внутренним мошенничеством в банке, мы видим, что эффект пренебрежения масштабом проявился и в этом случае: аналитики и сотрудники службы безопасности не придавали никакого значения размеру понесенных банком убытков, которые уже после первого сигнала исчислялись десятками миллионов рублей. Проводя расследование, сотрудники отнеслись к этому случаю как к одному из нескольких тысяч стандартных кейсов, проверенных ранее за несколько лет работы в банковском антифроде. Привычка сотрудников в совокупности с эффектом пренебрежения масштабом привела к небрежности и халатности, которые мы называем человеческим фактором. К сожалению, человеческий фактор способен перечеркнуть все достоинства современных технологий. И никакие продвинутые автоматизированные системы не смогут заставить сотрудников добросовестно выполнять свою работу. Но как же тогда улучшить качество работы сотрудников?

Мотивация

Когда ресурсы на материальную мотивацию (зарплаты и премии) ограничены, работодатель прибегает к использованию нематериальной мотивации. Психологи считают, что материальная мотивация действует недолго в отличие от нематериальной, которая способна побуждать сотрудников к действию на длительном промежутке времени. Поэтому для сотрудника, который долго работает в компании, нематериальные стимулы могут оказаться сильнее материальных.

Один из методов нематериальной мотивации, который используют работодатели в наши дни, применялся во время Корейской войны в лагерях для американских военнопленных. На этой войне многие американские солдаты оказались в лагерях, созданных китайскими союзниками Северной Кореи. Для того чтобы побудить пленных к добровольному сотрудничеству, китайцы использовали психологические методы воздействия без применения насилия, которое любили практиковать их союзники в северокорейских лагерях. Пленных часто просили делать антиамериканские и прокоммунистические заявления в столь мягкой форме, что они казались для пленных незначимыми: «Соединенные Штаты несовершенны», «В социалистических странах нет безработицы» и т.д. Однако, подчиняясь этим малым требованиям, пленные американские солдаты подталкивали самих себя к выполнению более существенных требований. Человека, который только что согласился с тем, что Соединенные Штаты несовершенны, можно спросить, почему, по его мнению, это так.

Роль человеческого фактора при расследовании внутреннего мошенничества

После этого можно попросить составить список «проблем американского общества» и подписаться под ним. Затем можно попросить, чтобы этот человек ознакомил других пленных со списком. Позднее этому человеку можно предложить написать очерк на данную тему: подобные очерки китайцы использовали в антиамериканских радиопрограммах с трансляцией на несколько лагерей. Таким образом, ни в чем не повинный солдат начинал добровольно и осознанно сотрудничать с врагом.

Данная методика, известная как «нога в дверях», была изучена социальными психологами Джонатаном Фридманом и Скоттом Фрезером. В 1966 г. они опубликовали данные экспериментов: эти данные потрясали воображение и доказывали высокую эффективность методики, которую активно применяли китайцы во время Корейской войны[1].

Для создания нематериальных мотивов у аналитиков и сотрудников службы безопасности есть несколько инструментов, работающих по принципу «нога в дверях». Эти инструменты формируют у сотрудников установки обязательности и последовательности, что позволяет снизить влияние человеческого фактора при расследовании внутреннего мошенничества.

Один из таких инструментов — корпоративная газета Fraud News, материалы для которой готовят аналитики и сотрудники службы безопасности. Газету необходимо выпускать регулярно (один раз в месяц), публикуя в ней информацию о ключевых событиях борьбы с внутренним мошенничеством:

1) статистику по мошенничеству и нарушениям со списком лучших и худших филиалов;

2) сведения о новинках, внедряемых в антифрод-процессы банка;

3) кейсы, связанные с раскрытым мошенничеством.

Такая газета способна мотивировать авторов (аналитиков и сотрудников службы безопасности), которые начинают относиться к работе с бóльшей ответственностью и энтузиазмом. Кроме того, рассылка Fraud News кредитным консультантам работает по принципу «Большой Брат следит за тобой»: кредитные специалисты понимают, что банк активно борется с внутренним мошенничеством, ловит внутренних мошенников и возбуждает против таких сотрудников уголовные дела.

Другой инструмент, способный мотивировать аналитиков и сотрудников службы безопасности, — регулярный отчет о выявленных

Рассылка корпоративной газеты Fraud News кредитным консультантам работает по принципу «Большой Брат следит за тобой»: кредитные специалисты понимают, что банк активно борется с внутренним мошенничеством.

[1] См.: Чалдини Р. Психология влияния. Убеждай, воздействуй, защищайся. СПб.: Питер, 2012.

XXXXXXXXXX

случаях мошенничества. Такой отчет представляет собой реестр всех выявленных случаев мошенничества (кейсов). Для каждого кейса приводятся описание мошеннической схемы, даты начала и выявления мошенничества, сумма ущерба и принятые меры (как в части уголовных дел, так и в части доработки процессов). Отчет регулярно отправляется высшему руководству банка; таким образом, принцип «Большой Брат следит за тобой» работает уже для аналитиков и сотрудников службы безопасности. Содержащиеся в отчете данные о размере убытков позволяют снизить эффект пренебрежения масштабом у аналитиков и сотрудников службы безопасности: теперь каждый сотрудник знает, что ему, возможно, придется ответить на вопросы руководства, почему банк понес декларируемые потери.

Резюмируя сказанное, можно заключить, что если правильно организовать рабочий процесс выявления внутреннего мошенничества (через двойную проверку подозрительных фактов), выстроить эффективную коммуникацию между аналитиками и сотрудниками службы безопасности, использовать стимулирующие инструменты в виде регулярных корпоративных газет и отчетов, можно значительно снизить уровень ошибок при расследованиях внутреннего мошенничества и повысить ответственность сотрудников.