Взгляд в будущее с умеренным оптимизмом

Уровень экономических преступлений снизился на 20 % в результате реализации мер по борьбе с мошенничеством

48%
респондентов отметили, что их компании столкнулись с экономическими преступлениями за последние два года

30%
респондентов отметили, что их компании пострадали от взяточничества и коррупции. По сравнению с 2014 годом количество таких респондентов уменьшилось

50%
респондентов, компании которых стали жертвами экономических преступлений, подчеркнули, что экономические преступления оказали значительный отрицательный эффект на моральное состояние сотрудников

65%
респондентов опроса отметили, что в их компаниях оценка рисков выполняется не реже одного раза в год, а 83% опрошенных указали наличие в их компаниях официальной программы по соблюдению правил деловой этики и нормативно-правовых требований

95%
респондентов считают, что риск мошенничества наиболее высок на этапе отбора поставщиков при осуществлении закупок товаров и услуг

pwc

www.pwc.ru/ru/forensic-services

Содержание

Предисловие

Джереми Оутен
Партнер
Руководитель практики услуг форензик – независимые финансовые расследования
PwC Russia

Представляем вашему вниманию результаты обзора экономических преступлений в России за 2016 год. Настоящий отчет подготовлен на основе ответов респондентов из России, полученных в рамках проведения восьмого Всемирного обзора экономических преступлений, проводимого PwC.

Во Всемирном обзоре приняли участие более 6 тысяч респондентов из 115 стран, включая представителей 120 российских компаний.

Первый выпуск обзора экономических преступлений увидел свет в 1999 году, и с тех пор задача этого издания состояла в том, чтобы узнать мнение респондентов об экономических преступлениях в целом, о причинах экономических преступлений, о методах выявления и предотвращения экономических преступлений и последствиях экономических преступлений.

В этом году в центре внимания нашего исследования находятся три вопроса: программы по соблюдению правил деловой этики и нормативно-правовых требований; противодействие легализации (отмыванию) доходов, полученных преступным путем; и киберпреступления. Помимо конкретных аспектов экономических преступлений, на которых следует сосредоточить особое внимание, в обзоре подчеркивается важность реализации более комплексных и эффективных мер, которые позволяют минимизировать указанные риски.

Хотя экономические преступления остаются одной из основных проблем для компаний, ведущих деятельность в России, результаты нашего исследования свидетельствуют о снижении экономической преступности в России на 20 %. Мы считаем, что эта положительная тенденция является результатом принятия новых инициатив по противодействию коррупции, усиления роли функции внутреннего аудита и реализации других мер, которые рассматриваются далее в нашем обзоре.

В нашем обзоре представлен широкий спектр российских компаний, в том числе частных компаний (34%), компаний, акции которых обращаются на бирже (59%) и предприятий государственного сектора (3%). Респонденты представляют различные отрасли экономики, в том числе сектор финансовых услуг (23%), промышленное производство (12%), топливно-энергетический сектор (9%), фармацевтическую и медико-биологическую отрасль (9 %), сектор розничной торговли и производства потребительских товаров (7 %), транспорт и логистику (7 %).

Большинство респондентов занимают руководящие позиции, такие как финансовый директор/главный казначей/главный контролер или руководитель бизнес-подразделения/отдела (департамента). Кроме того, 50 % респондентов работают в компаниях, где численность сотрудников превышает 5 тысяч человек.

Мы выражаем большую благодарность всем участникам данного опроса. Мы очень надеемся, что результаты нашего исследования помогут читателям этого обзора в их борьбе с экономическими преступлениями.

С уважением,

Джереми Оутен
Партнер, руководитель практики услуг форензик – независимых финансовых расследований,
PwC Россия

Участники опроса

Респонденты

72%
респондентов занимают руководящие должности и возглавляют финансовую функцию, функцию управления рисками, функцию аудита, функцию соблюдения нормативно-правовых требований.

25%
респондентов работали в компаниях, где численность сотрудников составляет от 1 тысячи до 5 тысяч человек

38%
респондентов работали в компаниях, где численность сотрудников превышает 10 тысяч человек

59%
представляли компании, акции которых обращались на бирже

Отрасли экономики

23%
сектор финансовых услуг

12%
промышленное производство

9%
топливно-энергетический сектор

9%
фармацевтическая и медико-биологическая отрасль

7%
транспорт и логистика

7%
сектор розничной торговли и производства потребительских товаров

Основные выводы

- За последние два года 48% компаний и организаций в России столкнулись с экономическими преступлениями. Это значительно ниже результата за 2014 год (60 %), но тем не менее выше общемирового показателя (36%).
- Снижение уровня экономических преступлений может быть вызвано следующими рыночными тенденциями: усилением роли внутреннего аудита в организациях и усовершенствованием систем, предназначенных для выявления противоправных действий.
- 65% процентов респондентов в России отметили, что в их компаниях оценка рисков мошенничества выполняется не реже одного раза в год. Общемировой показатель значительно ниже: только 51% респондентов ответили, что в их компаниях оценка рисков выполняется как минимум один раз в год. В то же время, 83% респондентов в России ответили, что в их организациях есть официальная программа по соблюдению правил деловой этики и нормативно-правовых требований (это значение соответствует общемировому среднему показателю).
- Участники нашего опроса отметили, что большинство экономических преступлений в России выявляются функцией внутреннего аудита и службой корпоративной безопасности (20% и 15% соответственно). По сравнению с 2014 годом ситуация изменилась: тогда большинство случаев выявлялось службой корпоративной безопасности (19%), и лишь 10% опрошенных указали процедуры внутреннего аудита. Это означает, что внутренний аудит является наиболее действенной мерой для выявления мошенничества в России. По сравнению с 2014 годом в России значительно возросло значение информирования о подозрительных операциях как механизма выявления экономических преступлений (11% в 2016 году по сравнению с 3% в 2014 году). На глобальном уровне информирование о подозрительных операциях является одним из основных механизмов выявления экономических преступлений. По всей видимости, российские компании приступили к реализации мер реагирования на риски, выявленные в ходе проведения их оценки.
- Однако мошенничество по-прежнему считается значительной потенциальной угрозой. Как минимум 41% респондентов считают, что их компании, вероятно, столкнутся с экономическими преступлениями в ближайшие два года.
- Состав экономических преступлений в России остается традиционным. Самыми распространенными видами мошенничества являются незаконное присвоение активов, мошенничество в сфере закупок товаров и услуг, взяточничество и коррупция. Если на глобальном уровне киберпреступления переместились на второе место, в России этот вид противоправных действий остается на четвертом месте.
- Незаконное присвоение активов остается основным видом мошенничества: его отметили около 72% респондентов в России, компании которых пострадали от экономических преступлений за последние два года, и 64% респондентов во всем мире. По сравнению с 2014 годом ситуация изменилась незначительно. Незаконное присвоение активов традиционно относится к видам противоправных действий, которые легче всего обнаружить, поэтому вполне ожидаемо, что оно из года в год преобладает в нашем исследовании.
- В России второе место после незаконного присвоения активов занимает мошенничество в сфере закупок товаров и услуг. Количество респондентов в России, отметивших мошенничество при осуществлении закупочной деятельности, больше, чем на глобальном уровне (33% и 23% соответственно). При этом самым уязвимым этапом в процессе закупок является выбор поставщика. Например, 95% респондентов считают, что именно на этом этапе закупок происходят мошеннические действия. Также следует отметить, что по ожиданиям респондентов в России в ближайшие два года их компании будут чаще сталкиваться с мошенничеством в сфере закупок, чем с незаконным присвоением активов.
- Существует множество мотивов совершения экономических преступлений. Результаты нашего исследования показывают, что такой фактор, как возможность или способность совершить экономическое преступление, вырос в России на 8% по сравнению с 2014 годом и остается наиболее весомым (84%). Вслед за ним по значимости идут давление внешних обстоятельств (8%) и возможность обосновать противоправное действие/ «самооправдание» (8%). В целом это соответствует глобальным тенденциям: на глобальном уровне возможность или способность совершить мошенничество также является самым весомым фактором (69%).
- В России 44% респондентов отметили, что за последние два года потери их компаний от экономических преступлений составили менее 100 тысяч долларов США, 25% респондентов сообщили о потерях в размере

от 100 тысяч до 1 миллиона долларов США, и 23% респондентов указали убытки в размере более 1 миллиона долларов США. При этом помимо финансовых потерь каждый случай экономического преступления наносит косвенный ущерб.

- В России каждый второй респондент указал, что самым значительным последствием экономического преступления за последние два года было его негативное влияние на моральный климат среди сотрудников, тогда как на глобальном уровне лишь 44% респондентов отметили это. Кроме того, в России несколько меньше, чем в мире вызывает беспокойство возможное негативное влияние экономических преступлений на отношения с партнерами по бизнесу и репутацию/имидж.
- Как в России, так и во всем мире собственные сотрудники продолжают преобладать среди злоумышленников. Однако количество респондентов, отметивших, что мошеннические действия совершили внешние лица, уменьшилось на 12%. В России и во всем мире основная доля правонарушителей из числа сотрудников компании приходится на менеджеров среднего звена (42% и 35% соответственно). Сотрудники младшего руководящего звена также составляют большую долю среди внутренних правонарушителей (31% и 32% соответственно). Большинство мошенников среди сотрудников компании составляют мужчины (77%) в возрасте от 31 года до 40 лет (62%), имеющие высшее образование (72%). За последние два года в России доля мошенников среди руководителей высшего звена уменьшилась с 36% до 15%.
- Увеличилось количество респондентов, обратившихся в правоохранительные органы в связи с экономическими преступлениями, в которых участвовали третьи стороны (67% в 2016 году и 60% в 2014 году). Такое действие в отношении внешних правонарушителей остается самым распространенным и во всем мире. Примечательно, что прекращение деловых отношений стало менее популярной мерой в России (56% в 2016 году и 70% в 2014 году), но все равно этот показатель значительно выше по сравнению с общемировым показателем (25%).
- В то время как на глобальном уровне незаконное присвоение активов, взяточничество и коррупция, мошенничество в сфере закупок и манипулирование данными бухгалтерского учета несколько снизилось по сравнению с показателями за 2014 год, киберпреступления вышли на второе место (32%). Однако в России лишь 23% респондентов отметили, что их компании пострадали от киберпреступлений за последние два года – это на 2% меньше по сравнению с 2014 годом. Изменилось и восприятие угрозы, которую представляют собой киберпреступления. Например, 53% наших респондентов во всем мире считают, что этот риск вырос за последние два года, тогда как в России лишь 32% респондентов ощущают его рост. Согласно результатам проведенного нами опроса руководителей крупнейших компаний, киберпреступления и неэффективная защита данных входят в число основных бизнес-рисков для руководителей компаний, ведущих деятельность в России (43%).
- Взяточничество и коррупция остаются серьезной проблемой в России. Например, 30% респондентов в России отметили, что взяточничество и коррупция оказали воздействие на деятельность их компаний, тогда как соответствующий общемировой показатель находится на уровне 24%. Результаты за 2016 год оказались ниже показателей в 2014 году, когда 58% респондентов отметили, что их компании пострадали от этого вида экономических преступлений. Помимо этого, 21% участников нашего опроса заявили, что их просили заплатить – это меньше по сравнению с 2014 годом (41%). Более того, 17% респондентов отметили, что их компании упустили возможность, которой воспользовались конкуренты, которые, как они считают, заплатили взятку. В 2014 году таких респондентов было 42%. Положительное изменение можно объяснить двумя факторами. Во-первых, в течение последних 4 лет в России был принят целый ряд законов и нормативных актов по борьбе с коррупцией. Вполне возможно, что сейчас мы видим результаты принятых мер. Во-вторых, доля публичных компаний, которые участвовали в опросе, увеличилась с 40% в 2014 году до 59% в 2016 году. Наш опыт показывает, что публичные компании, как правило, имеют более проработанные и эффективные программы по соблюдению правил деловой этики и нормативно-правовых требований.
- Тем не менее взяточничество и коррупция остаются одним из основных рисков для бизнеса. Например, 70% руководителей высшего звена, принявших участие в нашем последнем опросе руководителей крупнейших компаний, ведущих деятельность в России, считают взяточничество и коррупцию одной из важнейших проблем.
- В России 87% респондентов отметили, что их компании разработали всесторонний кодекс поведения. Однако только 68% из этих респондентов указали, что в их компаниях регулярно проводится обучение по вопросам, связанным с кодексом поведения.
- Результаты нашего исследования показывают, что даже финансовые организации, имеющие комплексные и тщательно проработанные программы по соблюдению требований в области противодействия легализации (отмыванию) доходов, полученных преступным путем (ПОД), сталкиваются с определенными трудностями при их реализации. Респонденты в России отметили, что самой большой проблемой для них в рамках эффективного соблюдения требований законодательства по ПОД является скорость изменения нормативно-правовой базы (58%), что намного превышает общемировой показатель (19%). Нормативно-правовая база в области ПОД подверглась значительным изменениям в последнее время. Дефицит квалифицированных сотрудников – еще одна проблема, с которой сталкиваются компании при реализации программ по соблюдению требований законодательства по ПОД. Ее отметили 19% респондентов во всем мире, тогда как в России лишь 4% участников опроса считают дефицит квалифицированных специалистов важной проблемой.

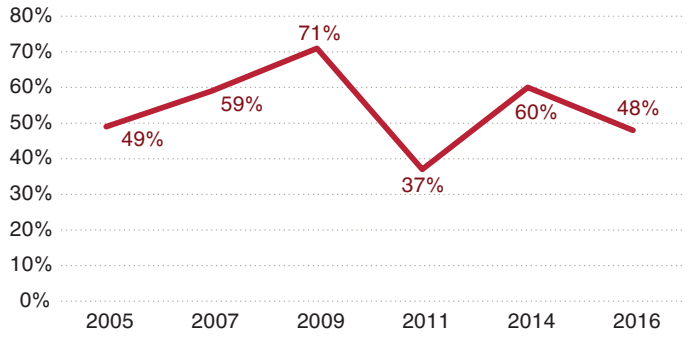
Тенденции в области экономических преступлений

Факты совершения экономических преступлений

Обзор

В России почти половина всех компаний и организаций (48%) столкнулись с экономическими преступлениями за последние два года. Однако это значительно ниже результата в 2014 году, когда соответствующий показатель составил 60%. Тем не менее уровень экономической преступности в России остается выше, чем общемировой средний показатель (36%), а также выше результатов по «большой семерке развивающихся стран» (29%)[1] и странам Восточной Европы (33%).

Рис. 1: Уровень экономической преступности согласно данным обзоров



Стоит отметить, что из числа тех, кто столкнулся с экономическими преступлениями за последние два года, 33% зафиксировали более 10 случаев мошенничества.

Снижение уровня экономической преступности в России можно объяснить несколькими причинами.

Во-первых, результаты нашего опроса свидетельствуют об усилении роли функции внутреннего аудита, а также о совершенствовании других механизмов выявления мошеннических действий. Наш опыт показывает, что компании, которые разработали механизмы выявления противоправных действий и реализовали программы управления рисками мошенничества, лучше подготовлены к выявлению и предотвращению мошенничества.

Во-вторых, в последнее время в России произошли большие изменения в области противодействия коррупции, включая законодательные инициативы, направленные на применение передовой международной практики.

Более детально эти причины будут рассмотрены ниже.

[1] «Большая семерка» развивающихся стран включает Бразилию, Россию, Индию, Китай, Индонезию, Мексику и Турцию.

Изменение видов экономических преступлений

Ниже рассматриваются наиболее распространенные виды экономических преступлений, которые указали респонденты в своих ответах в 2016 году.

Рис. 2: Основные виды экономических преступлений в России по сравнению с мировыми тенденциями

Как в России, так и во всем мире самым распространенным видом экономического преступления считается незаконное присвоение активов. Например, 72% респондентов в России и 64% респондентов в мире, компании которых столкнулись с экономическими преступлениями, стали жертвами незаконного присвоения активов. Неудивительно, что незаконное присвоение активов преобладает над другими видами экономических преступлений. Как правило, его легче выявить, поскольку этот вид мошенничества не такой сложный, как например взяточничество и коррупция или киберпреступления.

Мошенничество в сфере закупок товаров и услуг отметили 33% респондентов, что ставит его на второе место среди экономических преступлений, с которыми чаще всего сталкиваются компании в России. Стоит отметить, что количество респондентов в России, указавших этот вид

Три вида наиболее распространенных экономических преступлений в 2016 г. согласно данным опроса

экономического преступления среди самых распространенных, на 10% больше среднего значения по всему миру. По нашему мнению, этот вид мошенничества представляет собой двойную угрозу, поскольку он оказывает негативное воздействие как на коммерческий, так и на государственный сектор.

В России количество респондентов, отметивших взяточничество и коррупцию, больше, чем в среднем по всему миру (30% и 24% соответственно). Однако по сравнению с двумя годами ранее количество ответов, в которых были указаны взяточничество и коррупция, значительно уменьшилось – с 58% в 2014 году до 30% в 2016 году.

На глобальном уровне киберпреступления были указаны в 32% ответов. В результате они заняли второе место среди видов мошенничества, с которыми чаще всего сталкиваются компании. В то же время количество респондентов в России, указавших в своих ответах киберпреступления, оказалось меньше (23%), причем по сравнению с 2014 годом ситуация изменилась незначительно – два года назад таких респондентов было 25%. Означает ли это, что российский бизнес менее подвержен риску киберпреступлений? Необходимо помнить, что значительный процент тех, кто не указал в своих ответах киберпреступления, возможно, пострадали от этого вида мошенничества даже не зная об этом.

Отрицательные последствия экономических преступлений

В России 44 % респондентов, компании которых столкнулись с экономическими преступлениями за последние два года, указали, что понесенный убыток от них составил менее 100 тысяч долларов США, 25 % респондентов ответили, что убыток от экономических преступлений составил от 100 тысяч до 1 миллиона долларов США. 23% респондентов отметили, что убыток превысил 1 миллион долларов США, тогда как по всему миру лишь 14% респондентов понесли такой значительный ущерб.

Реальные затраты, связанные с экономическими преступлениями, трудно оценить, особенно если учесть, что фактические финансовые убытки составляют лишь малую долю в общей структуре последствий от серьезного инцидента.

Рис. 3: Финансовые убытки в результате экономических преступлений

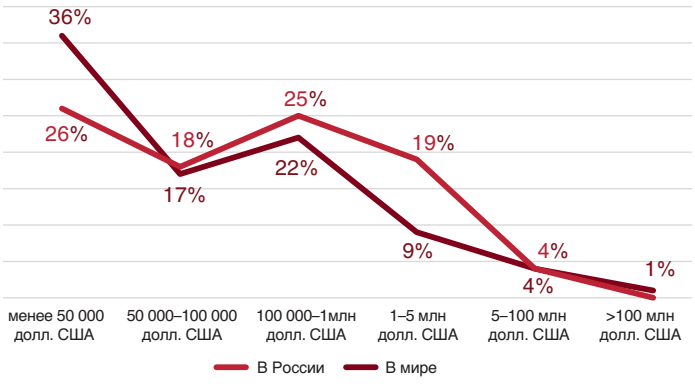
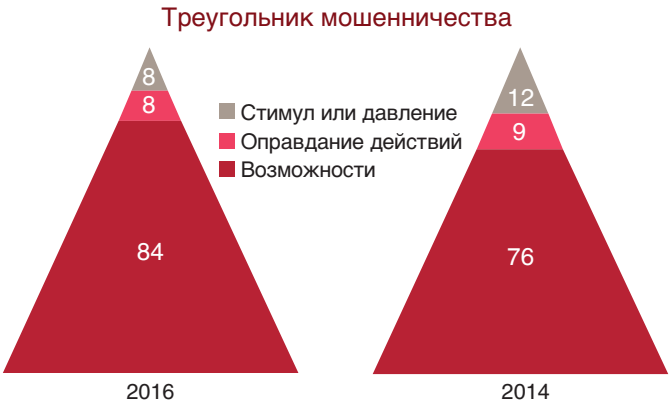


Рис. 4: Отрицательные последствия экономических преступлений (средний и высокий уровень влияния)

Участники нашего опроса неизменно отмечают, что на долгосрочные результаты деятельности существенное воздействие оказывает косвенный ущерб, который включает широкий спектр последствий: приостановка деятельности, следственные и превентивные мероприятия, меры по устранению причин правонарушений и, что особенно важно, ущерб, который наносится морально-психологическому климату в компании и ее деловой репутации.

В России 50% компаний, которые столкнулись с экономическими преступлениями за последние два года, отметили, что противоправные действия оказали значительное отрицательное влияние на морально-психологический климат в компании. На глобальном уровне лишь 44% респондентов отметили такое воздействие экономических преступлений на общее настроение сотрудников. При этом по сравнению с участниками опроса в других странах респондентов в России меньше беспокоит отрицательное влияние экономических преступлений на отношения с партнерами по бизнесу (35%) и на репутацию/имидж (34%).



Конечно, косвенный ущерб не всегда поддается количественной оценке. Тем не менее со временем его воздействие может стать более весомым по сравнению с непосредственными финансовыми потерями, которые носят относительно более краткосрочный характер.

Мотивы совершения экономических преступлений

Существует множество мотивов совершения экономических преступлений. Эксперты часто ссылаются на три самых распространенных фактора, обуславливающих совершение мошенничества (так называемый «Треугольник мошенничества»): возможность или способность совершить экономическое преступление; определенная мотивация или внешнее давление; и возможность обосновать совершенное экономическое преступление/самооправдание.

В России возможность или способность совершить преступление остается самым весомым фактором по мнению респондентов (84%). Его значимость выросла на 8% по сравнению с 2014 годом. Мотивация или внешнее давление, а также возможность обосновать совершенное экономическое преступление/самооправдание находятся на одном уровне по своей значимости (8%). В целом структура «треугольника мошенничества» в России схожа с его структурой на глобальном уровне, где возможность или способность совершить мошенничество является самым весомым фактором (69%).

Тенденция к увеличению доли этого фактора вызывает беспокойство. Это означает, что компании должны свести к минимуму такие «лазейки». Для этого необходимо применять упреждающий подход, с тем чтобы обеспечить эффективное управление существенными рисками мошенничества, используя механизмы выявления и предотвращения противоправных действий.

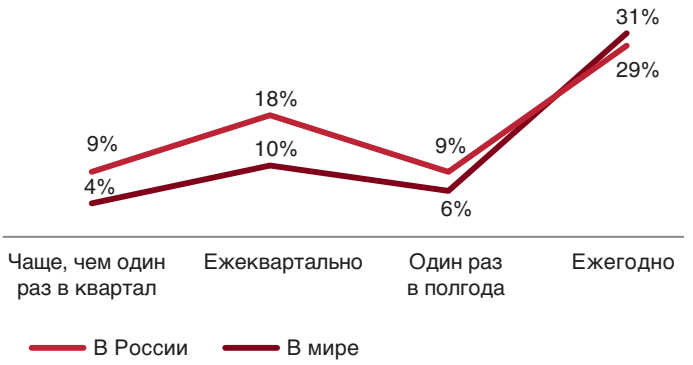
Выявление и расследование случаев мошенничества

Оценка рисков

Возможности совершить мошеннические действия возникают из-за наличия слабых мест в системе контроля, поэтому для выявления угроз и существующих недостатков крайне важно проводить оценку рисков мошенничества.

В России респонденты, как правило, регулярно выполняют оценку рисков (раз в полгода или один раз в год). По сравнению с общемировым показателем в России меньше компаний, которые никогда не выполняли оценку рисков или выполняли ее только один раз (32% и 23% соответственно). В целом, судя по ответам, российские респонденты гораздо чаще проводят оценку рисков мошенничества, чем участники опроса из других стран.

Рис. 5: Частота проведения оценки риска мошенничества в России и мире



Как уже отмечалось выше, респонденты в России и во всем мире считают возможность или способность совершить мошенничество самым весомым фактором, который способствует появлению таких преступлений. Таким образом, важность проведения оценки рисков возрастает, поскольку это мероприятие позволяет определить слабые места в системе контроля и, тем самым, предотвратить экономическое преступление или, по крайней мере, минимизировать его риск.

Выявление экономических преступлений

Результаты нашего опроса показывают, что в России службы внутреннего аудита и службы безопасности компаний первыми выявляют большинство экономических преступлений (20% и 15% соответственно). Общемировые результаты другие – 11% и 5% соответственно.

На глобальном уровне основным методом выявления экономических преступлений является информирование о подозрительных операциях.

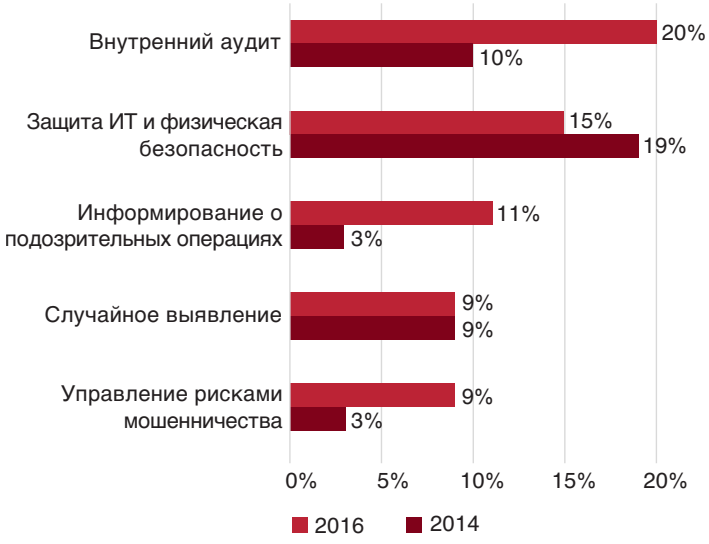
В России за последние два года произошли различные изменения в методах выявления случаев мошенничества.

Роль службы внутреннего аудита в выявлении экономических преступлений значительно усилилась: если в предыдущем опросе она была указана в 10% ответах респондентов, то в 2016 году уже в 20%. Роль службы корпоративной безопасности в выявлении случаев мошенничества ослабла в 2016 году.

Информирование о подозрительных операциях и управление рисками мошенничества становятся важными методами выявления экономических преступлений (20%).

Похоже, что российские компании реализовали надлежащие меры реагирования на риски, выявленные в ходе оценки рисков, и теперь они выявляют случаи мошенничества, используя более эффективные внутренние системы управления рисками.

Рис. 6: Методы обнаружения мошенничества в 2014 г. и в 2016 г.



Расследование

При выявлении случая потенциального мошенничества большинство респондентов (85%) проводят внутреннее расследование с использованием собственных ресурсов. Общемировой показатель ниже – 72%. В нашем исследовании за 2014 год показатели были выше – 93% и 79% соответственно. Вместе с тем результаты опроса также свидетельствуют о том, что в рамках внутренних расследований, как правило, дополнительно используются и другие мероприятия. Мы считаем, что в некоторых ситуациях внешнее содействие может принести пользу (например, привлечение специалистов, имеющих соответствующую квалификацию и опыт; обеспечение независимости; вопрос ресурсов; и т.д.).

В целом респонденты в России используют такой же подход, что и участники опроса из других стран.

Восприятие деятельности правоохранительных органов

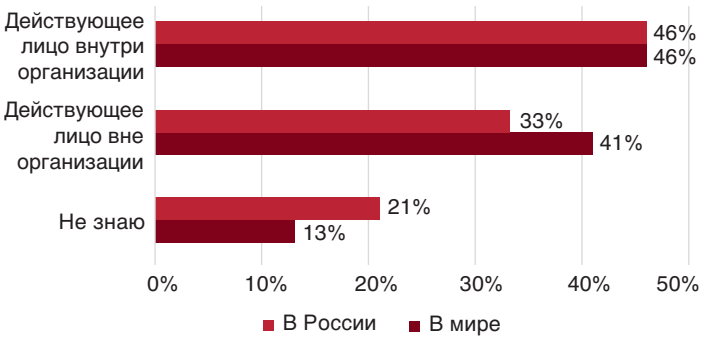
Мы попросили респондентов высказать мнение относительно уровня технической оснащенности и подготовки местных правоохранительных органов при расследовании экономических преступлений и преследовании за совершенные экономические преступления. Большинство респондентов выразили сомнения в том, что техническая оснащенность и подготовка правоохранительных органов находится на должном уровне, причем как во всем мире, так и в России (44% и 38% соответственно).

Рис. 7: Методы расследования мошенничества

Виновники экономических преступлений

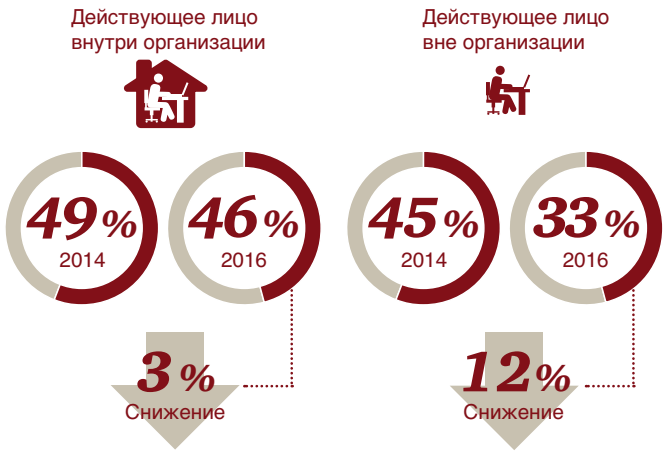
46% респондентов в России и по всему миру отметили, что среди лиц, совершивших экономические преступления, основная доля приходится на сотрудников компании.

Рис. 8: Виновники мошенничества



В России количество респондентов, указавших, что мошенниками оказались сотрудники их компаний, уменьшилось на 3% – с 49% в 2014 году до 46% в 2016 году. Общемировой показатель снизился еще более значительно – на 10%: с 56% в 2014 году до 46% в 2016 году.

В России количество респондентов, указавших, что мошенниками оказались внешние стороны, уменьшилось на 12% – с 45% в 2014 году до 33% в 2016 году. На глобальном уровне наблюдалась противоположная тенденция: количество таких респондентов увеличилось на 1 % – с 40 % в 2014 году до 41% в 2016 году.



Внутренние мошенники

Как в России, так и во всем мире экономические преступления совершают преимущественно руководители среднего звена (42% и 35% соответственно). Руководители младшего звена также составляют большую долю среди внутренних правонарушителей, совершивших мошеннические действия (31% в России и 32% во всем мире).

В России доля мошенников среди руководителей младшего звена увеличилась с 18% до 31% и почти сравнялась с общемировым показателем (32%).

Что касается руководителей высшего звена, то в России за последние два года их доля среди мошенников уменьшилась с 36% до 15% и стала соответствовать общемировому среднему показателю (16%).

Типичный портрет внутреннего мошенника

В России большинство мошенников из числа сотрудников компании составляют мужчины (77%) в возрасте от 31 года до 40 лет (62%), имеющие высшее образование (72%) и работающие в компании от 3 до 5 лет (62%). Этот портрет похож на портрет мошенника, который получился на основании ответов респондентов во всем мире.

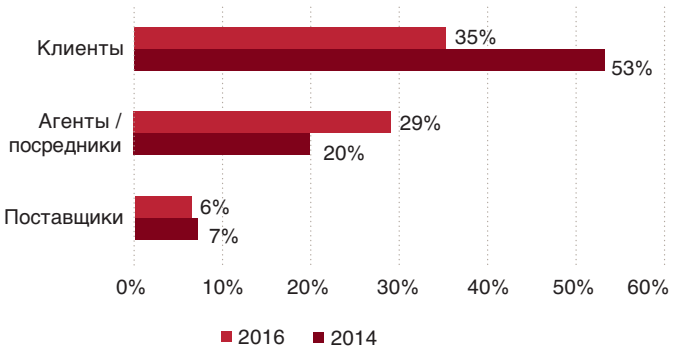
Наиболее вероятные характеристики мошенника внутри организации

Внешние (сторонние) мошенники

В России респонденты, компании которых столкнулись с экономическими преступлениями, отметили, что внешними правонарушителями оказались клиенты (35% случаев), агенты/посредники (29%) или поставщики (6%).

Результаты нашего опроса показывают, что за последние два года доля агентов/посредников, отношения с которыми представляют собой область риска, увеличилась на 9%.

Рис. 9: Внешние мошенники в России



По нашему мнению, в отношениях с клиентами распространенными видами мошенничества являются различные схемы откатов, связанные с получением взяток при осуществлении коммерческой деятельности (т.е. денег, заплаченных клиентами менеджерам по продажам с целью получения выгодных условий) и дачей взяток (т.е. денег, заплаченных клиентам с целью сохранения бизнеса с ними).

Действия против правонарушителей

В России в отношении правонарушителей из числа сотрудников компании чаще всего применяется увольнение (58%), что соответствует глобальной тенденции. По сравнению с результатами нашего предыдущего опроса (88%) этот показатель снизился. Такие действия, как гражданские иски и информирование правоохранительных органов, реже применяются к внутренним правонарушителям по сравнению с общемировой практикой.

Рис. 10: Меры, предпринимаемые организациями против мошенников внутри компании

Результаты нашего опроса также показывают, что в 15% случаях мошенничества с участием сотрудников компании никаких действий не предпринималось. Такая практика может иметь негативное влияние на корпоративную культуру, особенно на морально-психологический климат в компании.

В России увеличилось количество респондентов, указавших, что их компании обращались в правоохранительные органы в связи с экономическими преступлениями, в которых участвовали третьи стороны (67% в 2016 году и 60% в 2014 году). Обращение в правоохранительные органы остается самым распространенным действием в отношении внешних правонарушителей во всем мире (53%).

В России прекращение деловых отношений стало реже применяться в отношении внешних правонарушителей (56 % в 2016 году и 70% в 2014 году). Однако этот показатель все еще значительно превышает общемировой (25%). Такие действия, как гражданские иски и информирование правоохранительных органов, реже применяются к внутренним правонарушителям по сравнению с общемировой практикой.

Результаты нашего опроса также показывают, что в 15 % случаях мошенничества с участием сотрудников компании никаких действий не предпринималось. Такая практика может иметь негативное влияние на корпоративную культуру, особенно на морально-психологический климат в организации.

В России увеличилось количество респондентов, указавших, что их компании обращались в правоохранительные органы в связи с экономическими преступлениями, в которых участвовали третьи стороны (67 % в 2016 году и 60 % в 2014 году). Обращение в правоохранительные органы остается самым распространенным действием в отношении внешних правонарушителей во всем мире (53 %).

В России прекращение деловых отношений стало реже применяться в отношении внешних правонарушителей (56 % в 2016 году и 70 % в 2014 году). Однако этот показатель все еще значительно превышает общемировой (25 %).

Рис. 11: Меры, предпринимаемые организациями против внешних мошенников

[2] Под «увольнением» в этом контексте подразумевается любое прекращение трудовых отношений (например, по соглашению сторон).

Мошенничество в сфере закупок товаров и услуг

Возможность мошенничества в сфере закупок возникает, когда компания участвует в коммерческом или государственном тендере, или когда она приобретает товары и услуги для собственного пользования. В России компании чаще сталкиваются с мошенничеством в сфере закупок товаров и услуг по сравнению с общемировым средним показателем (33% и 23% соответственно).

По нашему мнению, мошенничество в сфере закупок представляет собой двойную угрозу. Оно наносит ущерб самим компаниям в отношении приобретения товаров и услуг. Кроме того, оно лишает компании возможности вести справедливую и успешную конкуренцию в коммерческих или публичных тендерах.

Мошенничество на разных этапах закупочного цикла

В России этапы закупочного цикла, на которых обычно совершаются мошеннические действия, несколько отличаются от этапов, указанных участниками нашего опроса в других странах.

Рис. 12: Этапы закупочной деятельности, на которых совершаются мошеннические действия

Результаты нашего опроса показывают, что как в России, так и во всем мире риск мошенничества наиболее высок на следующих этапах закупочной деятельности: отбор поставщика, процесс подачи заявки на участие в тендере и заключение/ведение договоров с поставщиками. Однако в России мошеннические действия на этих этапах совершаются чаще, чем в среднем во всем мире.

Следует отметить, что 95% респондентов в России указали в своих ответах, что большинство случаев мошенничества в сфере закупок связано с отбором поставщика. Мошенничество на этапах подачи заявок и анализа качества также чаще встречается в России, чем во всем мире.

Напротив, мошенничество на этапе оплаты довольно часто встречается во всем мире (41%), но редко в России (16%).

Похоже, что мошенничество в сфере закупок можно значительно минимизировать путем усиления контроля в следующих основных областях: проведение комплексной проверки поставщиков, проведение проверки на конфликт интересов и обеспечение наличия надлежащих средств контроля на этапе подачи заявок и заключения/ведения договоров с поставщиками.

Уделяя особое внимание рискам, связанным с проведением тендеров и отбором внешних поставщиков, важно не упускать из виду потенциальную угрозу со стороны внутренних действующих лиц. Сотрудник отдела закупок может иметь ранее установленные и часто непрямые отношения с определенным поставщиком. На выявление подобного конфликта интересов могут уйти месяцы и даже годы.

Минимизация рисков в сфере осуществления закупок

Одним из эффективных решений, позволяющих обеспечить надлежащую работу функции закупок, может быть детальный анализ процесса закупок. Для этого необходимо использовать современные методы анализа данных, а также проводить качественные оценки, результаты которых помогут определить риски мошенничества в сфере закупок и недостатки (неэффективные элементы) процесса.

Однако организация может иметь сотни и даже тысячи поставщиков. Что в этом случае необходимо делать, чтобы понять, кто из них не так надежен, как кажется? Одним из решений может быть комплексная проверка благонадежности и деловой репутации, которая поможет выявить негативную информацию и определить потенциальные конфликты интересов: а) между поставщиками и сотрудниками организации; и б) среди поставщиков или групп поставщиков. Такой анализ также поможет руководству компании очень оперативно сделать предварительные выводы.

Этапы анализа процесса закупок

Выявление

- Извлечение необходимых данных из ERP-системы с использованием ИТ-решений;
- Установление основных фактов о действующем в компании процессе закупок, используя результаты анализа данных и ответов на вопросы анкет или интервью с ответственными сотрудниками.

Анализ

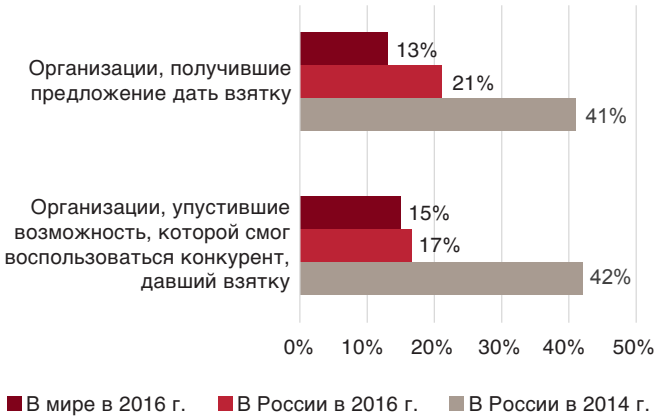
- Выявление необычных тенденций в данных;
- Выполнение детального анализа необычных тенденций и понимание их причин в результате использования аналитических тестов и методов визуализации данных.

Взяточничество и коррупция

В России 30% респондентов отметили, что их компании столкнулись со взяточничеством и коррупцией – это значение превышает общемировой средний показатель (24%). По сравнению с 2014 годом (58%) результаты за 2016 год свидетельствуют об уменьшении количества респондентов, отметивших этот вид экономического преступления.

В России 21% участников нашего опроса заявили, что их компаниям предлагалось дать взятку – это меньше по сравнению с 2014 годом, когда таких респондентов был 41%. В России и во всем мире 17% респондентов отметили, что их компании упустили коммерческую возможность, проиграв конкуренту, который, по их мнению, дал взятку. Этот показатель значительно ниже результатов нашего предыдущего опроса (42%).

Рис. 13: Организации, которые получили предложение дать взятку и которые упустили возможность из-за того, что взятку дал конкурент



Мы считаем, что эта положительная тенденция могла сформироваться в результате действия двух факторов. Во-первых, в последние годы в России был принят целый ряд законов и нормативных актов по противодействию коррупции. Вполне возможно, что сейчас мы видим положительные результаты этих инициатив. Во-вторых, доля публичных компаний, которые участвовали в нашем опросе, увеличилась с 40% в 2014 году до 59% в 2016 году. Публичные компании, как правило, стремятся разработать программы по соблюдению правил деловой этики и нормативно-правовых требований.

Согласно нашему последнему опросу руководителей крупнейших компаний в России 70% руководителей высшего звена указали, что взяточничество и коррупция являются одним из основных рисков для их организаций.

Мошенничество в будущем

Результаты нашего исследования показывают, что экономические преступления продолжают считаться значительной потенциальной угрозой.

Мы попросили респондентов высказать свое мнение о том, какие виды экономических преступлений представляют наиболее значительный риск для их компаний в ближайшие два года. Как минимум 41 % респондентов считают, что их компании, вероятно, столкнутся с экономическими преступлениями (мошенничеством в сфере закупок товаров и услуг) в ближайшие 2 года.

Рис. 14: Ожидания в отношении экономических преступлений в ближайшие два года

В целом похоже, что ожидания участников опроса в России отражают глобальные тенденции, но при этом есть следующие различия.

Во-первых, в России меньше респондентов, которые считают киберпреступления одной из серьезных угроз в будущем (25 % в России и 34 % во всем мире). Возможно, это свидетельствует о чрезмерной уверенности или неосведомленности, что приводит к недооценке потенциальной угрозы.

Во-вторых, в России больше респондентов, ожидающих, что в ближайшие два года их компании столкнутся с мошенничеством в сфере закупок товаров и услуг (41 % в России и 26 % во всем мире). Необычным является то, что по ожиданиям респондентов в России, в ближайшие два года их компании станут чаще сталкиваться с этим видом мошенничества, чем с незаконным присвоением активов. Такое мнение является еще одним подтверждением того, что мошенничество в сфере закупок товаров и услуг представляет значительную угрозу для российских компаний, поэтому его предотвращение должно быть в центре внимания их руководства.

[3] В апреле 2012 года Россия стала 39-м участником Конвенции ОЭСР по борьбе со взяточничеством.
В январе 2013 года вступила в силу статья 13.3 Федерального закона № 273-ФЗ «О противодействии коррупции».
В ноябре 2013 года Министерство труда и социальной защиты Российской Федерации выпустило «Методические рекомендации по разработке и принятию организациями мер по предупреждению и противодействию коррупции». В апреле 2014 года вступил в силу «Национальный план противодействия коррупции на 2014–2015 гг.».

Деловая этика и соблюдение нормативно-правовых требований

26%
компаний полагают, что столкнутся
с коррупцией и взяточничеством в будущем

... и 50%
или каждый второй респондент заявляют, что влияние
на моральное состояние сотрудников является самым
значительным последствием экономического преступления

Как стратегия вашего бизнеса соотносится с ценностями, принятыми в Вашей организации?

Приведение процесса принятия решений в соответствие с корпоративными ценностями

Обзор

Текущая бизнес-среда характеризуется растущей глобализацией, ужесточением контроля за соблюдением законодательства и повышенным требованием к ответственности перед обществом. Для решения задач в сфере деловой этики и соблюдения нормативно-правовых требований необходимо применять подход, основанный на оценке рисков. В рамках этого подхода первым шагом является понимание рисков экономических преступлений и недостатков в системе обеспечения соответствия внешним и внутренним нормативным документам. Используя этот подход, организации должны разработать эффективные программы, которые позволят не только минимизировать риски экономических преступлений, но и добиться поставленных бизнес-целей.

В последнее время многие компании сокращают затраты (как на содержание персонала, так и на программы обучения) или расширяют круг обязанностей специалистов, отвечающих за обеспечение нормативно-правового соответствия. Такая практика может оказаться стратегическим просчетом, поскольку взяточничество и коррупция по-прежнему представляют значительную угрозу для бизнеса в России. Хотя риски и угрозы постоянно меняются, эффективная программа по обеспечению нормативно-правового соответствия должна помогать руководству прогнозировать эти риски и управлять ими.

Похоже, что существует разрыв между тем, что происходит в компании на самом деле и тем, что члены правления/совета директоров и руководители думают о ситуации (особенно среди руководителей высшего и среднего звена). Согласно результатам нашего опроса, руководители среднего звена по-прежнему являются наиболее вероятными правонарушителями, считающими, что корпоративные ценности сформулированы нечетко или что программы стимулирования несправедливы.

Результаты нашего последнего опроса руководителей крупнейших российских компаний подтверждают наличие разрыва между намерением и исполнением. Например, 70% руководителей отметили взяточничество и коррупцию в качестве главных угроз для их организаций. Еще одной значительной угрозой является отсутствие доверия к бизнесу, что подчеркивает важность наличия в компании комплексной программы по вопросам корпоративной этики, которая заслуживала бы доверие.

Как убедиться в пригодности программы по обеспечению соответствия нормативно-правовым требованиям

Ниже перечислены четыре приоритетных направления, на которых следует сконцентрировать усилия, направленные на повышение эффективности программ по соблюдению правил деловой этики и нормативно-правовых требований:

- Персонал и корпоративная культура. Поддержка программы, в основе которой лежат корпоративные ценности, оценка и вознаграждение желаемого поведения сотрудников (в соответствии с целевыми моделями поведения);
- Роли и функциональные обязанности. Обеспечение их соответствия текущим рискам;
- Направления, связанные с высоким риском. Более эффективная/качественная реализация и тестирование программы на рынках и в подразделениях с высоким риском.
- Технологии. Более эффективное использование инструментов, предназначенных для выявления и предотвращения мошенничества (например, аналитического инструментария для работы с большим массивом данных).

Пять шагов к повышению эффективности программы по обеспечению соответствия нормативно-правовым требованиям

- Информирование о программе и позиционирование программы в соответствии с корпоративной стратегией Вашей компании;
- Оценка и возможное переосмысление характеристик функции по обеспечению соответствия нормативно-правовым требованиям в Вашей компании (комплаенс-функции);
- Обеспечение полного понимания всеми сотрудниками, ответственными за сферу комплаенса: (а) общей картины на уровне организации; и (б) круга их обязанностей;
- Помните, что недостаточно иметь внутренние политики и проводить обучение по корпоративным ценностям; крайне важно обеспечить убедительное и постоянное вовлечение сотрудников;
- Никогда не сокращайте персонал в условиях, когда риски растут.

Персонал и корпоративная культура: первая линия защиты Вашей организации

В основе каждого экономического преступления лежит решение, принятое человеком. Поэтому люди должны быть в центре внимания. Это означает, что компании должны не только формулировать принципы работы, которым должны следовать сотрудники, но и формировать корпоративную культуру, в которой существует прямая связь между соблюдением нормативно-правовых требований и корпоративными ценностями.

В России каждый второй респондент отметил, что самый большой ущерб, понесенный их компаниями в результате экономического преступления, связан с его негативным влиянием на морально-психологический климат в организации. 34% респондентов указали в своих ответах отрицательные последствия для деловой репутации и имиджа компании. В обоих случаях руководство компаний очень волнует восприятие их бизнеса (как сотрудниками компании, так и внешними сторонами). Это подчеркивает важную роль, которую играют корпоративные ценности в успехе бизнес-стратегии.

Основанная на корпоративных ценностях программа по обеспечению соответствия нормативно-правовым требованиям поможет привлечь в компанию лучших специалистов. Другими словами, ответственные люди хотят работать в ответственных компаниях.

Компания может получить очевидное стратегическое преимущество, если у нее есть тщательно продуманная программа по обеспечению соответствия нормативно-правовым требованиям, и она уделяет особое внимание этическим нормам поведения.

При этом эффективная программа по обеспечению соответствия нормативно-правовым требованиям включает в себя больше, чем новую редакцию кодекса поведения, политику и несколько часов обучения. По сути, она должна также обеспечить тесную взаимосвязь между корпоративными ценностями, моделями поведения и процессом принятия решений.

Учет и оценка различий в восприятии

В России 85% респондентов подтвердили, что в их компаниях есть четко сформулированные и понятные корпоративные ценности.

Однако только 70% респондентов считают, что система вознаграждения является справедливой и основана на едином подходе, независимо от уровня, роли, департамента или местонахождения. Более того, только 64% респондентов считают, что дисциплинарные процедуры и взыскания применяются последовательно. Таким образом, результаты нашего исследования, возможно, указывают на несоответствие в восприятии ценностей, особенно речь идет о несоответствии между заявлениями, которые делают руководители высшего звена, и фактической картиной, которую видят сотрудники.

Чтобы добиться успеха в условиях сильнейшей конкуренции, компании должны внедрять принципы этического поведения во всех операционных подразделениях на каждом без исключения уровне.

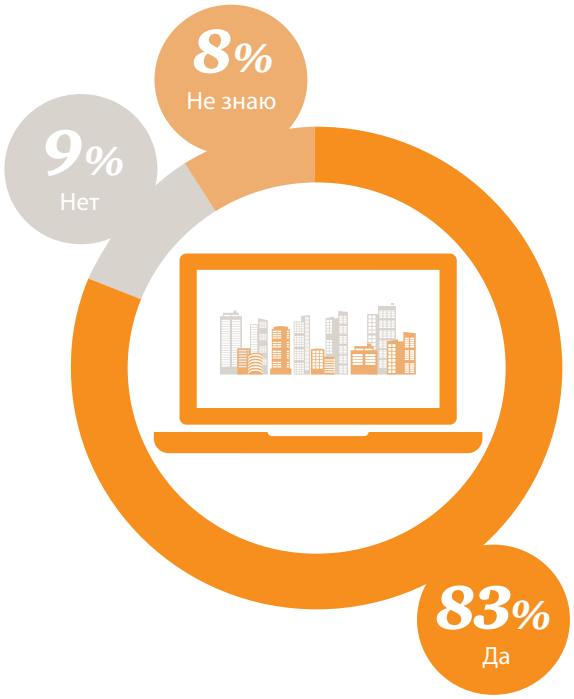
Рис. 15: Восприятие корпоративной этики

Приведение в соответствие функций и обязанностей: на ком лежит ответственность?

Результаты нашего опроса показывают, что 17% респондентов не осведомлены о наличии в их компаниях официальной программы по соблюдению правил деловой этики и нормативно-правовых требований.

В России 83% респондентов отметили, что в их компаниях созданы официальные программы по соблюдению правил деловой этики и нормативно-правовых требований. Этот результат почти соответствует общемировому показателю (82%).

Рис. 16: Сколько компаний имеют официальную программу по соблюдению правил деловой этики и нормативно-правовых требований?



На ком лежит ответственность? Применение подхода с учетом рисков

Результаты нашего исследования показывают, что в большинстве компаний ответственность за выполнение программ по соблюдению правил деловой этики и нормативно-правовых требований лежит на директоре по соблюдению нормативно-правовых требований и директоре по персоналу.

Рис. 17: Кто отвечает за реализацию программ по соблюдению деловой этики и обеспечению нормативно-правового соответствия?

Важно, чтобы сотрудники всех подразделений, а не только специалисты в области комплаенс, понимали свои функции и обязанности, связанные с обеспечением соответствия бизнес-целей и задач с программой по соблюдению правил деловой этики и нормативно-правовых требований. Однако во многих компаниях существует некоторое непонимание относительно того, кто за что отвечает.

«Владельцами» программы должны быть руководители бизнес-подразделения, поскольку именно они отвечают за понимание рисков и определение «риск-аппетита» для подразделения. С другой стороны, роль функции комплаенса заключается в том, чтобы осуществлять контроль и давать руководящие указания. Однако некоторые организации склонны рассматривать функцию комплаенса как вид страхового полиса, который позволяет сотрудниками другим подразделений пассивно исполнять обязанности.

В конечном итоге все сотрудники компании должны работать для достижения общих целей в области соблюдения нормативно-правовых требований.

Возможности для совершения экономического преступления становится больше

Результаты нашего опроса показывают, что 84% респондентов считают наличие возможности основным фактором, способствующим совершению экономических преступлений сотрудниками компании. Этот фактор перевешивает два других элемента «треугольника мошенничества» – мотивацию/внешнее давление и возможность обосновать совершенное экономическое преступление/самооправдание.

В России подавляющее большинство респондентов (81%) отметили, что в их компаниях оценкой эффективности программ по обеспечению соответствия нормативно-правовым требованиям занимается функция внутреннего аудита. Этот результат превышает общемировой средний показатель (76%).

Для обеспечения эффективности работы функций по соблюдению этических норм и нормативно-правовых требований в России чаще, чем в других странах используется мониторинг сообщений о совершении/подозрении в совершении неправомерных действий, получаемых через «горячую линию» (60% и 42% соответственно). На глобальном уровне второе место по популярности среди подходов, обеспечивающих эффективность работы этих функций, занимает коммуникация руководства. Этот подход – направление дальнейшего развития для компаний в России.

Хотя функция внутреннего аудита является важной частью системы оценки эффективности программы по обеспечению соответствия нормативно-правовым требованиям, сама по себе она не может быть достаточным средством, обеспечивающим уверенность в соблюдении установленных требований, поскольку выполняемые ею мероприятия носят периодический и исторический характер.

Поскольку в идеале мошенничество должно предотвращаться на этапе принятия решений, необходимо интегрировать механизмы внутреннего аудита, коммуникацию руководства и мониторинг в режиме реального времени, и с целью своевременного выявления и предотвращения проблем.

Рис. 18: Как в вашей организации обеспечивается эффективность программы в области соблюдения требований законодательства и деловой этики

Внедрение в зонах с высоким риском

В России 87% респондентов отметили, что в их организациях есть кодекс поведения, но только 68% из них подтвердили, что в их компаниях регулярно проводится соответствующее обучение и что вопросы, связанные с кодексами поведения, регулярно доводятся до сведения всех сотрудников.

Такой разрыв свидетельствует о том, что недостаточно иметь четко сформулированные политики и процедуры и тщательно разработанные средства контроля. Громкие слова должны подкрепляться действиями и практическими решениями.

Очевидно, что тщательно проработанная программа по обеспечению соответствия нормативно-правовым требованиям должна включать в себя больше, чем новую редакцию кодекса поведения, политику и несколько часов обучения.

Соблюдение установленных требований эффективно только тогда, когда оно не ограничивается мероприятиями «для галочки». Крайне важно, чтобы сотрудники на всех уровнях компании разделяли одни ценности.

Использование технологий с целью обеспечения соответствия установленным требованиям

В настоящее время существует целый ряд высокотехнологичных инструментов (например, методы анализа больших массивов данных для обеспечения эффективного мониторинга операций), которые предназначены для обработки различных структурированных и неструктурированных данных. Использование этих инструментов позволяет сделать инициативы в сфере соблюдения нормативно-правовых требований актуальными и для операционных подразделений.

Однако результаты нашего опроса показывают, что очень мало компаний применяют эти технологии для выявления и предотвращения экономических преступлений (исключение составляют системы мониторинга операций, которые используются в основном организациями финансового сектора).

Некоторые компании уделяют слишком много внимания мониторингу одних вопросов и при этом полностью игнорируют другие важнейшие проблемы. Другие компании дублируют свои затраты на различные инструменты. При этом к сфере комплаенса компании применяют подход «для галочки» и не всегда собирают или используют правильные данные.

Наш опыт показывает, что целесообразнее всего надо начинать не с больших массивов данных, используемых для мониторинга операций, а с малых данных о результатах оценки рисков. Самое важное – собрать непротиворечивые и сопоставимые данные.

Оптимальная модель должна охватывать весь спектр рисков, с которыми сталкивается организация, и предусматривать составление отчетности по бизнес-подразделениям, географическому расположению или третьим сторонам. Для решения этой задачи необходимо иметь:

- единый подход к определению рисков;
- понятную систему количественной оценки рисков;
- общую платформу данных.

Данные сами по себе никогда не бывают панацеей. Тем не менее если их использовать эффективно, компании могут получить дополнительное преимущество, чтобы быть на шаг впереди в части управления комплаенс-рисками.

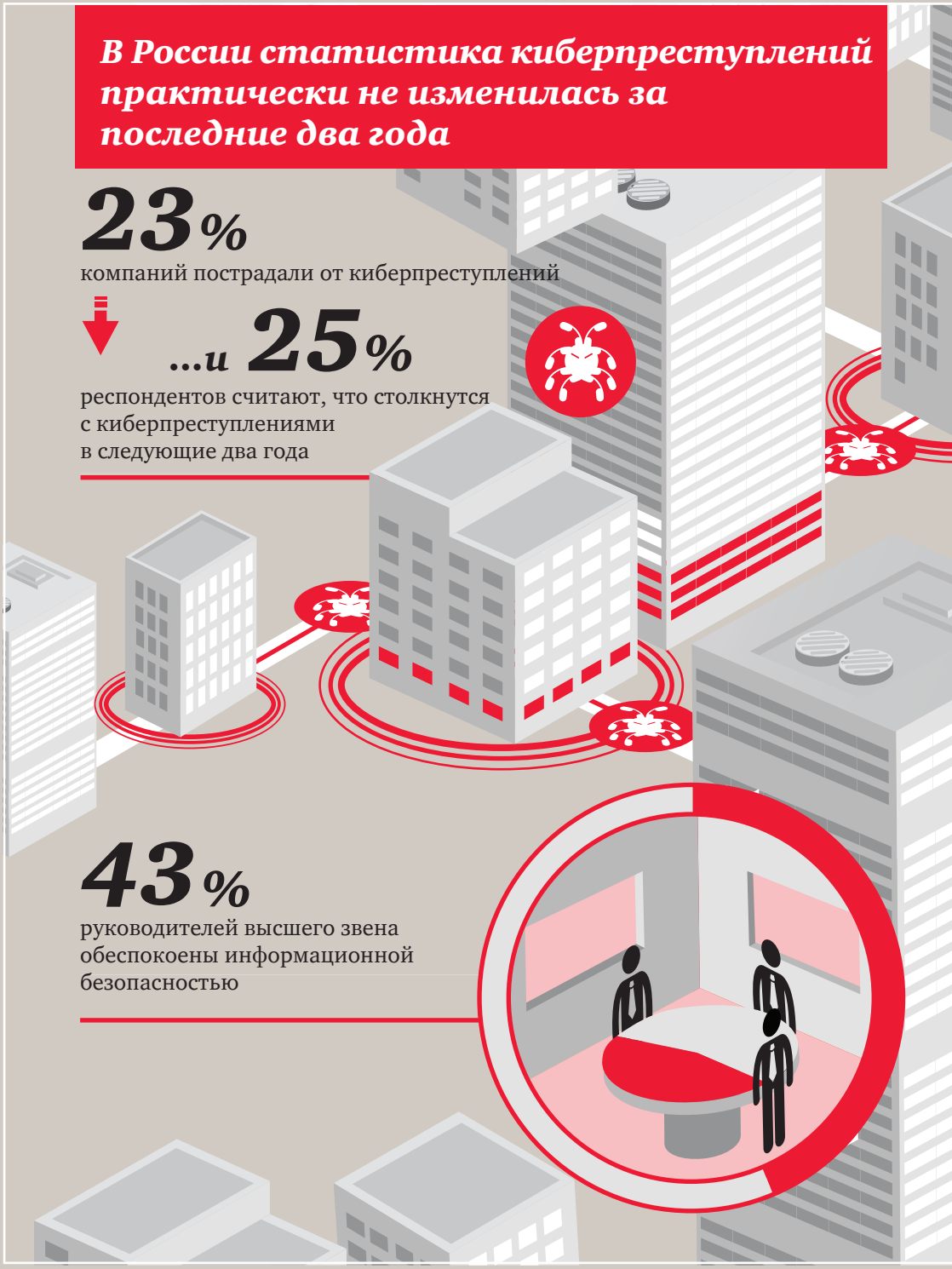
Киберпреступность

Киберпреступность заняла второе место среди экономических преступлений в мире

В России статистика киберпреступлений практически не изменилась за последние два года

23%
компаний пострадали от киберпреступлений

...и 25%
респондентов считают, что столкнутся с киберпреступлениями в следующие два года



43%
руководителей высшего звена обеспокоены информационной безопасностью

Только 26%
компаний имеют действующий план реагирования на киберпреступления

Большинство компаний недостаточно подготовлены и не всегда осознают риски, а состав команды реагирования значительно варьируется

Насколько Ваш план реагирования на киберпреступления соотносится с реальностью?

Безграничные угрозы

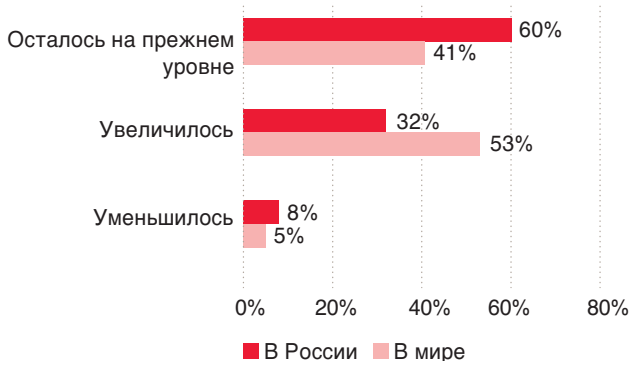
Обзор

Цифровые технологии продолжают коренным образом изменять мир бизнеса, в результате чего перед компаниями не только открываются новые возможности, но и возникают новые угрозы. Поэтому совсем неудивительно, что в мире наблюдается рост киберпреступлений (например, в рейтинге за 2016 год они занимают второе место среди преступлений, с которыми чаще всего сталкиваются компании во всем мире).

Киберпреступления – это не просто проблема, связанная с информационными технологиями. Сегодня информационные технологии настолько широко распространены (как внутри, так и за пределами компаний), что киберпреступления могут считаться одной из основных бизнес-проблем.

Однако результаты нашего опроса показывают, что в России ситуация с киберпреступлениями несколько иная. Почти четверть (23%) респондентов отметили, что за последние два года их компании пострадали от киберпреступлений. По сравнению с предыдущим опросом за 2014 год (25%) значительных изменений не произошло.

Рис. 19: Изменение восприятия рисков киберпреступлений



В России за последние два года восприятие рисков киберпреступлений не изменилось у 60% респондентов. Наоборот, на глобальном уровне 53 % респондентов считают, что этот риск вырос за последние два года, тогда как в России лишь 32% респондентов ощутили его рост.

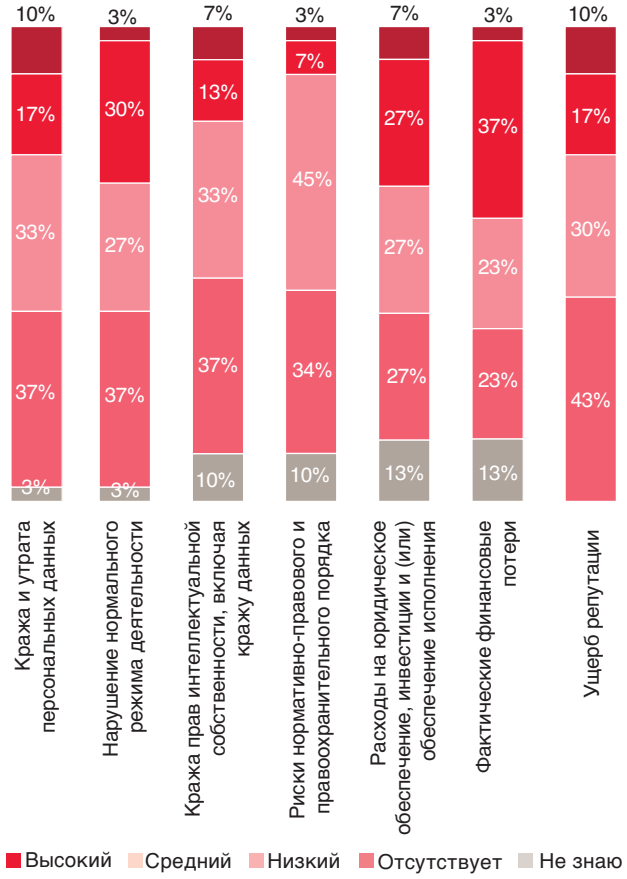
Означает ли это, что российские компании менее подвержены риску киберпреступлений? Скрытый характер данной угрозы проявляется в том, что определенная часть респондентов, заявивших, что их компании не столкнулись с киберпреступлениями, на самом деле пострадали от них, даже не зная об этом. Иногда хакерам удается оставаться в сети компаний не обнаруженными в течение длительного периода времени.

Руководители компаний склонны беспокоится, что киберпреступления могут сдерживать развитие их компаний. Результаты нашего последнего опроса руководителей крупнейших компаний, работающих в России, показали, что 43 % руководителей выразили беспокойство по поводу растущей угрозы киберпрестпулений, при этом 52 % из них считают ускорение технологических изменений еще одной проблемой.

Воздействие киберпреступлений

Респонденты в России отметили, что ущерб репутации и хищение персональных данных являются наиболее разрушительными последствиями киберпреступления. Далее идут утрата интеллектуальной собственности и расходы на юридическое обеспечение и принудительное исполнение. На глобальном уровне респонденты отметили сбои в работе/обслуживании, регуляторные риски и непосредственные финансовые потери.

Рис. 20: Уровень влияния киберпреступлений



В России 47% респондентов указали в ответах, что их компании потеряли до 1 миллиона долларов в результате киберпреступления, совершенного против них за последние два года. 6% респондентов указали еще более существенный убыток, который они понесли в результате киберпреступлений. Стоит отметить, что значительная доля респондентов (23%), компании которых столкнулись с киберпретспулениями, не могли оценить размер ущерба от них.

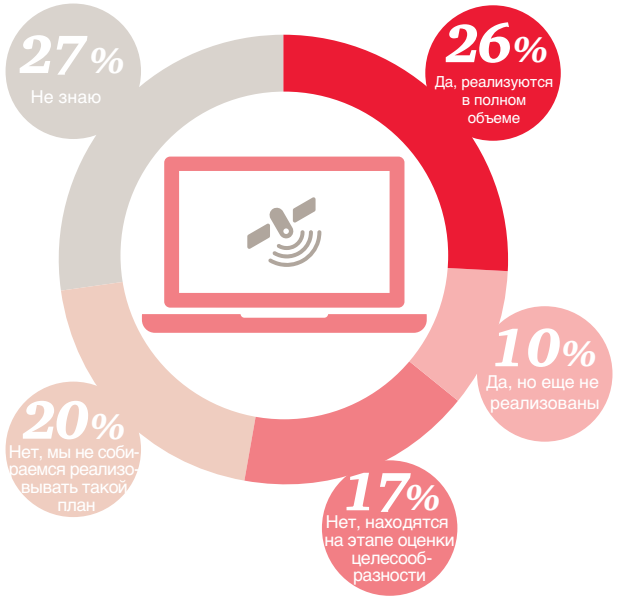
Меры реагирования на киберпреступления

В России только 26% респондентов отметили наличие в их компаниях полностью действующего плана реагирования на инциденты. Среди участников опроса во всем мире такой ответ дали 37% респондентов. Более того, 20% организаций не имеют плана и не рассматривают возможность его внедрения.

Похоже, что в случае с киберпреступлениями только в 45% организаций есть «полностью обученные» сотрудники, готовые действовать в качестве первого эшелона реагирования, при этом сотрудники отдела ИТ-безопасности составляют подавляющее большинство (74%) из них.

Корпоративные киберпреступления – одна из самых сложных и трудных проблем, с которой может столкнуться организация. Для принятия эффективных мер реагирования необходима совместная работа специалистов из различных функций, которые имеют соответствующие навыки, знания и опыт (например, юридического отдела, отдела кадров, отдела по работе со СМИ и связям с общественностью, отдела коммуникаций, юридического консультанта по вопросам защиты конфиденциальной информации, аудита и управления рисками, финансового отдела, службы корпоративной безопасности и др.).

Рис. 21: Имеются ли у организации планы реагирования на инциденты для решения проблем, связанных с кибератаками?



Определение угроз в сфере информационных технологий и их минимизация входят в круг обязанностей всех подразделений компании.

ИТ-угрозы и их минимизация входят в круг обязанностей всех подразделений компании

Уровень руководства

- Разработка стратегии информационной безопасности
- Обеспечение получения и передачи качественной информации
- Внедрение программ осведомленности о безопасности
- Поддержка стратегии расходов на безопасность

Юридическая поддержка

- Отслеживание изменения законодательства
- Мониторинг решений регулирующих органов в отношении инцидентов
- Уведомление о факторах, которые могут аннулировать страховые выплаты

Аудит и риски

- Обеспечение должного понимания и покрытия ИТ рисков
- Проведение проверки на благонадежность в целях минимизации рисков, связанных с третьими лицами
- Реагирование на риски, связанные с операционными системами
- Реагирование на основные проблемы, выявленные в ходе ИТ аудита

Информационные технологии

- Проведение оценки готовности реагирования
- Уведомления об изменении общей картины и направления кибератак
- Тестирование плана реагирования на инциденты
- Внедрение эффективного процесса мониторинга
- Проведение учебных кибератак, тренингов по безопасности и повышение осведомленности

Противодействие легализации доходов, полученных преступным путём

Темпы изменения режима регулирования возросли

29%
респондентов финансового сектора сталкивались с правоприменительными мерами со стороны регулирующих органов

В России **52%**
респондентов финансового сектора выделяют сложность внедрения и модернизации информационных систем

***...только* 57%**
операций по легализации доходов, полученных преступным путем, было выявлено по средствам мониторинга операций

Как Ваша организация отреагирует в случае проверки со стороны регулирующих органов?

Обзор

Легализация денежных средств, полученных преступным путем («отмывание денег») разрушает ценности. Это способствует совершению экономических преступлений и безнравственных действий, таких как коррупция, терроризм, уклонение от уплаты налогов, наркоторговля и торговля людьми. Эти преступления совершаются в результате хранения или перевода необходимых денежных средств. Легализация денежных средств, полученных преступным путем, может нанести ущерб репутации компании и оказать негативное влияние на ее итоговые результаты деятельности.

По оценкам, объем операций по легализации денежных средств, полученных преступным путем, во всем мире составляет от 2 до 5 процентов мирового ВВП, т.е. порядка 1–2 триллионов долларов США ежегодно. При этом, согласно данным Управления ООН по наркотикам и преступности, властям удается перехватить менее 1% нелегальных финансовых потоков в мире[3].

Почти во всех странах растет обеспокоенность правительств по поводу увеличения объема операций по легализации денежных средств, полученных преступным путем, и финансированию терроризма. В течение последних нескольких лет регулирующие органы наложили на международные финансовые организации крупные штрафы (размер которых составляет сотни миллионов и даже миллиарды долларов США) за операции по легализации денежных средств, полученных преступным путем.

Законодательство касается не только организаций, работающих в сфере финансовых услуг. Любая компания, осуществляющая финансовые транзакции, включая небанковские организации, которые предоставляют услуги по работе с денежными средствами (такие как поставщики услуг цифровых/мобильных платежей, компании по страхованию жизни и ритейлеры), также находится в центре внимания законодательства по противодействию отмыванию денег (ПОД) по всему миру. Многие из этих новых участников пока еще не соответствуют требованиям регулирующих органов.

По мере развития и усложнения нормативно-правового регулирования растут затраты на соблюдение требований законодательства ПОД. Согласно новым данным компании WealthInsight, к 2017 году расходы на соблюдение требований законодательства ПОД увеличатся до 8 миллиардов долларов США (совокупные темпы годового роста составят почти 9%)[4] . Однако крупные штрафы за несоблюдение этих требований превышают растущие затраты на обеспечение соответствия.

[3] Из доклада «Оценка нелегальных финансовых потоков, порождаемых торговлей наркотиками и другими видами транснациональной организованной преступной деятельности», подготовленного Управлением ООН по наркотикам и преступности © 2011 Организация объединенных наций. Перепечатано с разрешения ООН.
[4] Статистические данные любезно предоставлены компанией WealthInsight.

Оценка рисков имеет важнейшее значение

За последние 10 лет меры контроля за операциями по легализации денежных средств, полученных преступным путем, стали более эффективными, что заставило мошенников и преступников искать новые способы для перевода денежных средств. Поэтому крайне важно регулярно проводить оценки рисков, поскольку они позволят организациям определить риски в сфере ПОД/ФТ и управлять ими.

Оценка рисков должна проводиться регулярно и с учетом различных обстоятельств, таких как операционная среда, международные стандарты и национальное законодательство.

Результаты нашего опроса показывают, что подавляющее большинство респондентов из компаний финансового сектора (88% в России и 74% в мире) выполняют проверки рисков в сфере ПОД/ФТ во всех своих бизнес-подразделениях и в странах, где они осуществляют операционную деятельность.

Рис. 22: Организации, которые проводят оценку рисков, связанных с требованиями по противодействию легализации доходов/финансирования терроризма

Однако результаты нашего опроса показывают, что 29% финансовых организаций в России и 18% финансовых организаций во всем мире подверглись мерам воздействия со стороны регулятора (либо в виде принудительной программы устранения недостатков, либо в виде серьезного замечания с требованием решить актуальные вопросы).

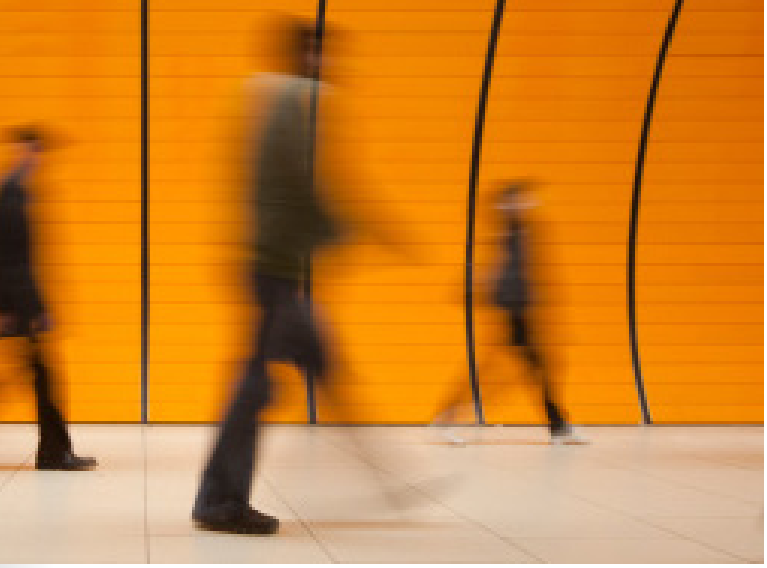


Рис. 23: Сталкивались ли вы на своем опыте с правоприменительными мерами со стороны органов регулирования?

Проблемы и трудности, с которыми сталкиваются организации

Участники нашего опроса отметили, что применение мер ПОД/ФТ создает проблемы даже для наиболее передовых финансовых организаций.

В России 58% респондентов указали в ответах, что самой большой проблемой для них в рамках соблюдения требований ПОД/ФТ является скорость изменения нормативно-правовой базы. На глобальном уровне лишь 19% респондентов считают это проблемой.

Участники опроса из других стран также указали следующие значительные проблемы (которые не были особо отмечены респондентами в России): возможность нанять на работу опытных специалистов в области ПОД/ФТ (19% во всем мире и лишь 4% в России) и технологические требования (19% во всем мире и лишь 4% в России).

Рис. 24: Наиболее значительные трудности в соблюдении требований по предотвращению легализации доходов/ финансирования терроризма

Результаты исследования показывают, что самой большой проблемой в связи с организацией систем ПОД/ФТ в компаниях является сложность внедрения или модернизации информационных систем, качество данных, сохранение информации о клиентах в электронных форматах и мониторинг систем, которые генерируют большое количество ложных тревог.

В России большинство респондентов отметили, что самой большой проблемой для них является сложность внедрения или модернизации информационных систем. Возможно, это связано с использованием старых систем мониторинга, которые тяжело и очень дорого эксплуатировать, обслуживать и модернизировать по мере изменения нормативно-правовой базы в России.

Рис. 25: Системы предотвращения легализации доходов/ финансирования терроризма: наиболее значительные трудности

Эффективность применяемых методов

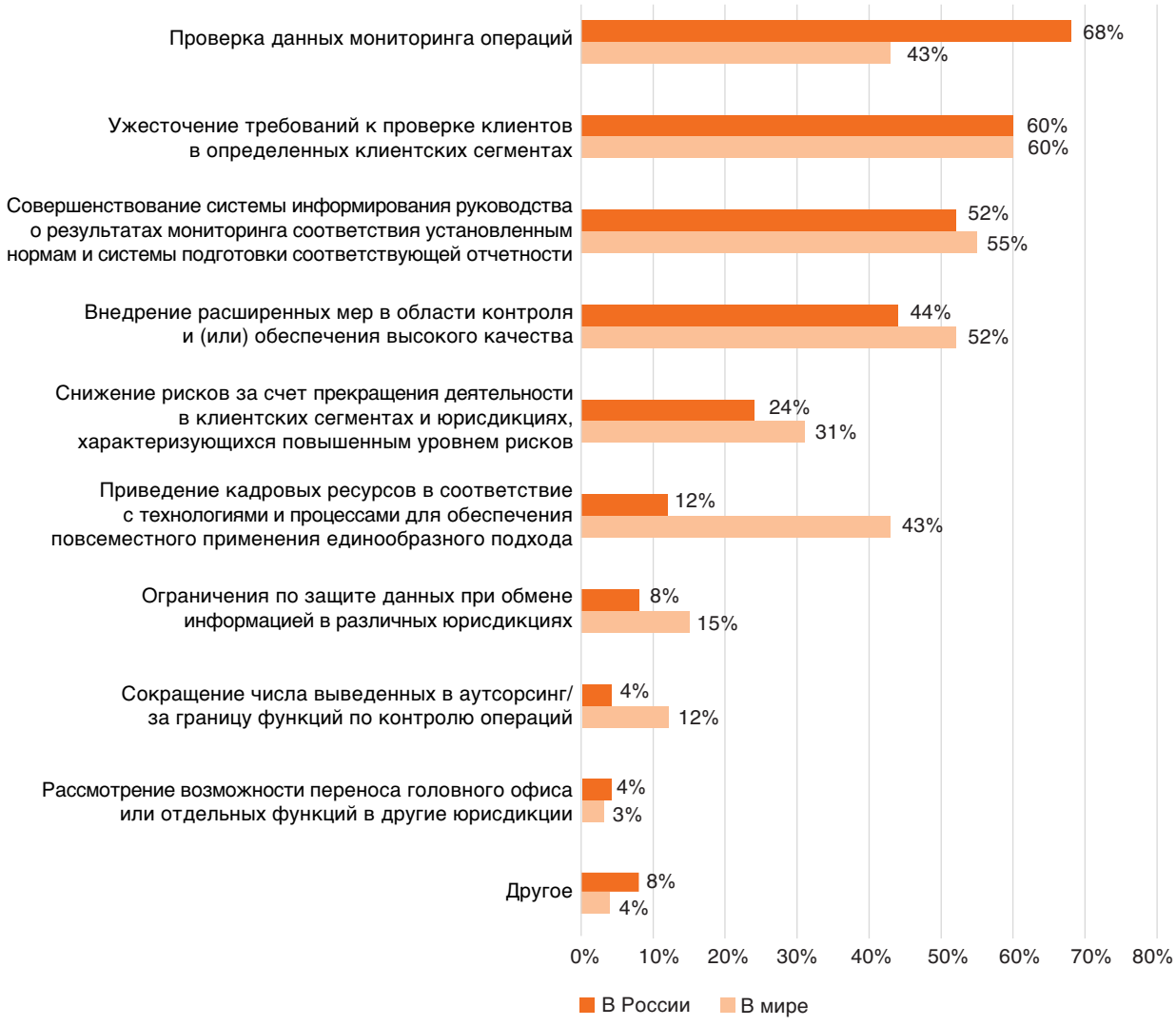
Результаты нашего опроса показывают, что российские финансовые организации чаще используют мониторинг операций в качестве основного метода выявления подозрительных операций по легализации денежных средств, полученных преступным путем, или финансированию терроризма.

Результаты нашего исследования также свидетельствуют о том, сотрудники финансовых организаций в России чаще используют внутреннюю отчетность, чем их коллеги в других странах (24% и 10% соответственно).

Рис. 26: Методы выявления подозрительной деятельности

Результаты нашего исследования показывают, что компании выполняют различные мероприятия с целью минимизации рисков ПОД/ФТ. Чаще всего они используют мониторинг операций, проверку (валидацию) данных, ужесточение требований «Знай своего клиента» (ЗСК) к некоторым клиентским сегментам, а также повышают эффективность программ по обеспечению соответствия нормативно-правовым требованиям в части мониторинга систем отчетности и информирования руководства о проблемах.

Рис. 27: Меры, направленные на снижение рисков, связанных с требованиями по противодействию легализации доходов/финансирования терроризма



Как уже отмечалось выше, финансовые организации в России больше сосредоточены на выявлении подозрительных операций и их дальнейшей проверке (68% в России и 43% во всем мире). Мы также получили данные, свидетельствующие об отсутствии единого подхода к увязке кадровых ресурсов, технологий и процессов в разных юрисдикциях (12% в России и 43% во всем мире). Компаниям в России необходимо развивать такой подход.

Терминология

В нормативно-правовых актах различных государств отдельные виды экономических преступлений описываются по-разному. В связи с этим для целей данного исследования мы выделили следующие категории. Приведенное ниже описание соответствует определениям, содержащимся в нашем Интернет-опросе.

Манипулирование данными бухгалтерского учета

Изменение данных финансовой отчетности и (или) иных документов, равно как и такое их представление, при котором они перестают отражать реальную оценку стоимости или реальные результаты финансовой деятельности организации. К таким действиям могут относиться манипулирование данными бухгалтерского учета, мошенничество при получении кредитов / привлечении финансирования, мошеннические заявления на получение кредита и неавторизованные операции / мошеннические торговые операции.

Незаконное присвоение активов, включая хищение/обман со стороны сотрудников

Хищение имущества (включая монетарные активы/ денежные средства или ТМЦ и оборудование) руководителями, доверенными лицами или сотрудниками в целях личной выгоды.

ПОД

Противодействие легализации (отмыванию) доходов, полученных преступным путем

Взяточничество

Злоупотребление должностными полномочиями для совершения действий, входящих в круг служебных обязанностей, вопреки интересам службы и в личных интересах. К таким действиям могут относиться обещания экономической или иной выгоды (предложение взятки), применение запугивания или шантажа. А также согласие (обещание) на получение взятки в обмен на предоставление определенной услуги. В качестве конкретных примеров можно привести откаты, вымогательство, подарки (с определенными условиями), стимулирующие платежи и др.

Коррупция

Нечестное или мошенническое поведение лиц, облеченных властью, как правило, предполагающее дачу взятки.

ПФТ

Противодействие финансированию терроризма

Киберпреступление

Известное также как компьютерное преступление, киберпреступление – это экономическое правонарушение, совершенное с использованием компьютера и (или) Интернета. Типичные примеры киберпреступлений включают распространение вирусов, несанкционированное копирование информации с носителей информации, фишинг и фарминг, а также хищение персональных данных, таких как реквизиты банковских счетов. К киберпреступлениям не относятся обычные противоправные действия, для совершения которых компьютерные технологии были использованы как вспомогательный инструмент. К ним относятся экономические преступления, в совершении которых компьютерные технологии, Интернет, равно как и электронные носители и устройства были использованы как основной, а не сопутствующий элемент.

Экономическое преступление

Намеренное введение в заблуждение с целью завладения чужими денежными средствами, имуществом или правами.

Финансовые убытки

При оценке финансовых потерь в результате мошенничества участники должны учитывать как прямые, так и косвенные убытки. Прямые убытки – это непосредственная сумма потерь от мошенничества, а косвенные убытки, как правило, включают затраты на расследование и устранение проблемы, наложенные регулирующими органами штрафы, а также затраты на судебные разбирательства. В эту величину не входит расчетная сумма потерь в результате «упущенной возможности для бизнеса».

Оценка рисков мошенничества

Оценка выполняется, с тем чтобы определить, предприняла ли организация инициативы для:

a. Анализа рисков мошенничества, которым подвержена ее операционная деятельность;

b. Оценки рисков, представляющих наибольшую угрозу (т.е. оценки рисков по их значимости и вероятности наступления);

c. Определения и оценки эффективности средств контроля (при наличии таковых), предназначенных для минимизации основных рисков;

d. Оценки общих программ по борьбе с мошенничеством и системы контроля, существующей в организации;

e. Разработки мероприятий по устранению недостатков, имеющихся в системе контроля.

Мотивация/внешнее давление

Существование у человека некоторой финансовой проблемы, которую он (она) не может решить, используя законные средства, и поэтому рассматривает возможность совершения противоправного действия в качестве способа решения проблемы. По своему характеру финансовая проблема может быть профессиональной (например, риск потерять работу) или личной (например, личный долг).

Нарушение прав интеллектуальной собственности (ИС)

Нарушение прав ИС распространяется на торговые марки, патенты, контрафактную продукцию и услуги. Данный вид нарушений включает незаконное копирование и (или) распространение поддельной продукции в нарушение патентного или авторского права, а также выпуск фальшивых банкнот и монет с намерением их использования в качестве подлинных денежных знаков.

ЗСК

Знай своего клиента

Легализация денежных средств, полученных незаконным путем («отмывание денег»)

Умышленные действия для легализации незаконно полученных доходов путем сокрытия истинного источника их происхождения.

Возможность или способность

Обнаружение отдельным лицом способа, с помощью которого оно может использовать свою ответственную должность (злоупотреблять своей должностью) с целью решения финансовой проблемы, при этом риск быть пойманным воспринимается как низкий.

Мошенничество при организации и проведении подрядных работ и закупок

Незаконные действия правонарушителя, за счет которых он получает преимущество, избегает выполнения обязательств или причиняет ущерб своей организации. Правонарушителем может быть сотрудник, собственник, член законного органа управления, должностное лицо, общественный деятель или поставщик, участвующий в приобретении услуг, товаров или активов для пострадавшей организации

Самооправдание

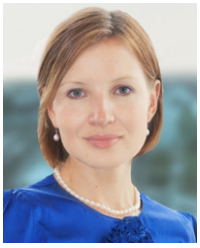
Попытка человека обосновать для себя преступление таким образом, что оно становится приемлемым или оправданным действием.

Контактная информация

Общее руководство исследованием

Джереми Оутен
PwC | Партнер
Тел.: +7 495 967 6011
Email: jeremy.outen@ru.pwc.com

Ирина Новикова
PwC | Партнер
Тел.: +7 495 232 5735
Email: irina.n.novikova@ru.pwc.com



Инна Фокина
PwC | Партнер
Тел.: +7 495 967 6382
Email: inna.fokina@ru.pwc.com

Методология и подготовка исследования

Илья Мушкет
PwC | Старший менеджер
Тел.: +7 495 223 5105
Email: ilya.mushket@ru.pwc.com

Антон Ульякин
PwC | Младший менеджер
Тел.: +7 495 967 6000
Email: anton.ulyakin@ru.pwc.com

www.pwc.ru/ru/forensic-services