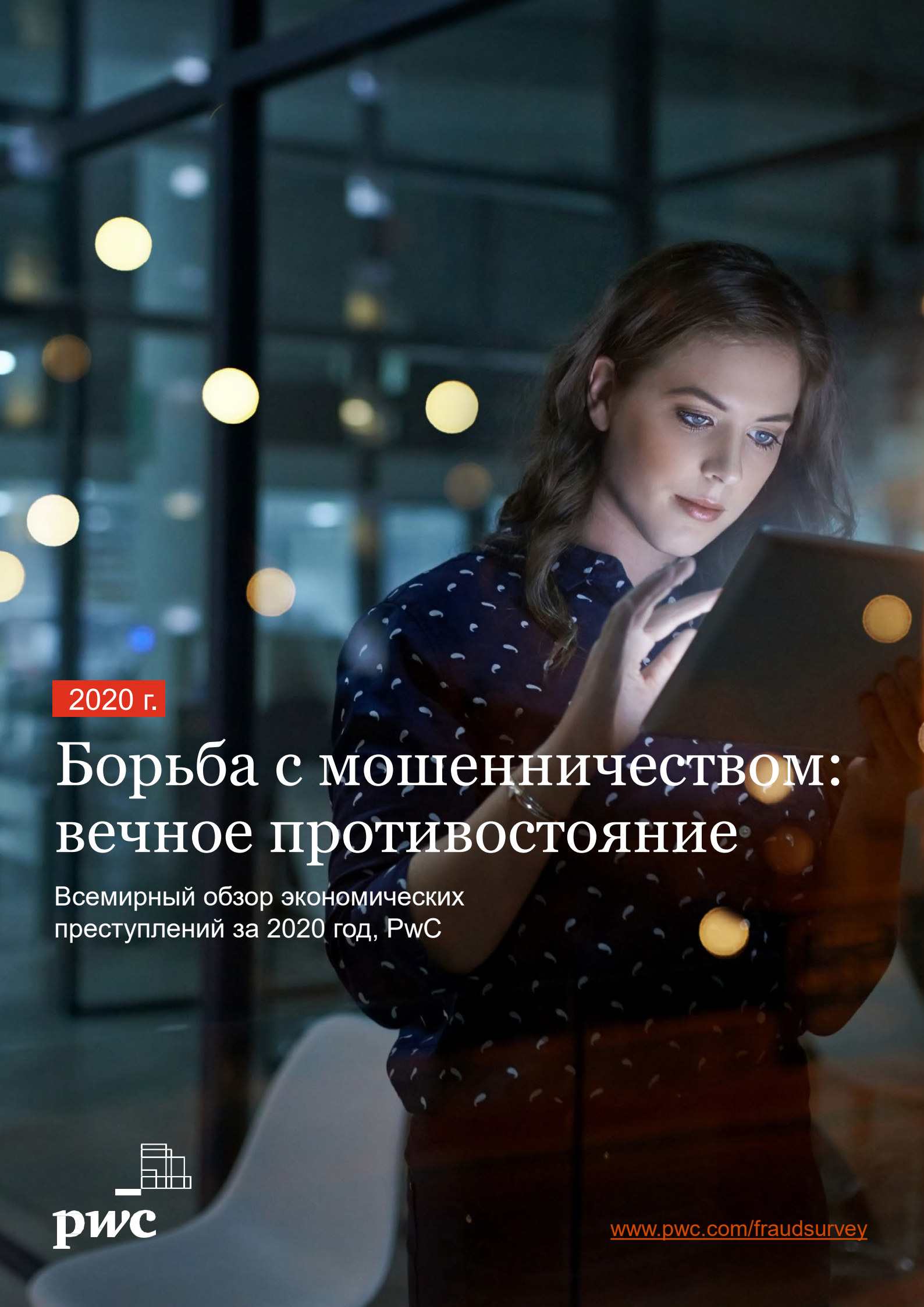


2020 г.

Борьба с мошенничеством: вечное противостояние

Всемирный обзор экономических преступлений за 2020 год, PwC

pwc

www.pwc.com/fraudsurvey

Включите новости или откройте газету – и вы наверняка узнаете о каком-то экономическом преступлении или мошенничестве:

«Причиной обрушения здания могли стать взятки на начальных этапах строительства... Хакерским атакам подверглись базы с медицинскими и платежными данными миллионов граждан... Причиной провала товара на рынке названы должностные злоупотребления в компании-производителе... Котировки акций рухнули из-за сообщений о манипулировании данными бухгалтерской отчетности компании...»

Уровень экономической преступности остается рекордно высоким, и все больше компаний несут убытки в самых разных сферах своей деятельности, чем когда бы то ни было. Учитывая данные тенденции, компании должны задаться такими вопросами:

Достаточно ли хорошо мы оцениваем уровень угрозы, или в нашей системе есть пробелы, из-за которых мы серьезно уязвимы? Справляются ли со своей задачей внедренные нами технологии защиты от экономических преступлений? Принимаем ли мы необходимые меры, столкнувшись с фактом мошенничества?

Мы постарались узнать ответы на эти и другие провокационные вопросы в нашем Всемирном обзоре экономических преступлений. Мошенничество сегодня представляет собой как никогда опасную угрозу, способную повлечь серьезные потери, и крайне важно оценить готовность вашей организации к быстрому обнаружению такой угрозы, выстраиванию систем защиты и оперативному ответу.

Мошенничество

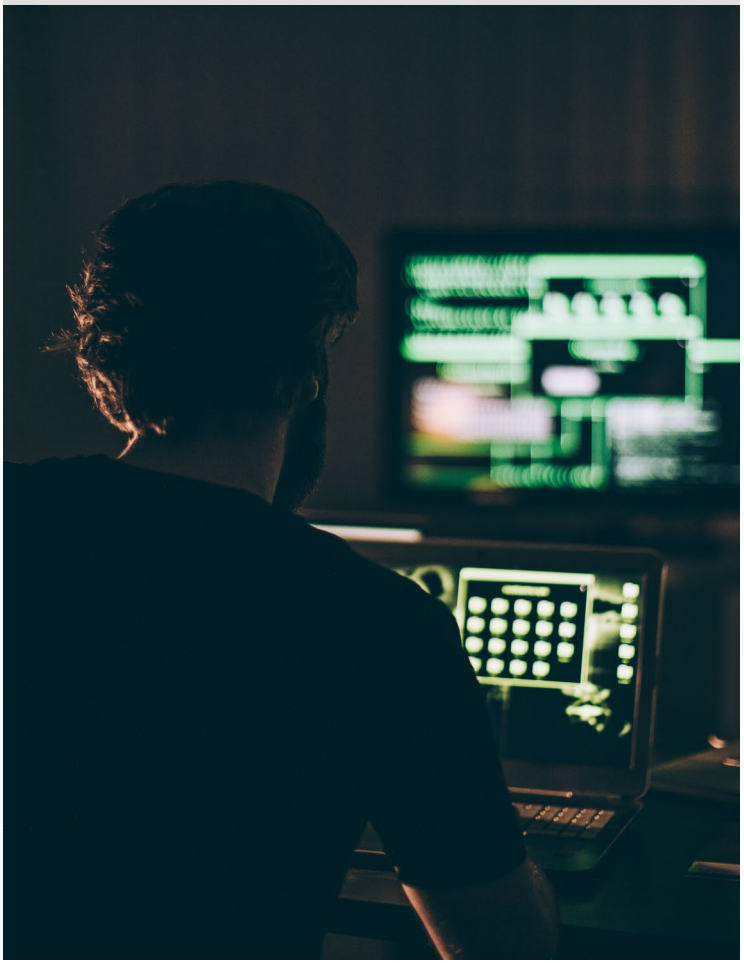
В рамках Всемирного обзора экономических преступлений специалисты PwC более 20 лет анализируют правонарушения в следующих сферах:

- Манипулирование данными бухгалтерского учета
- Нарушение законодательства о защите конкуренции и антимонопольного законодательства
- Незаконное присвоение активов
- Взяточничество и коррупция
- Мошеннические действия клиентов
- Киберпреступления
- Нарушение принципов делового поведения
- Мошенничество в сфере управления персоналом
- Неправомерное использование инсайдерской информации
- Нарушение прав интеллектуальной собственности
- Легализация доходов, полученных преступным путем, и нарушение санкционных режимов
- Мошенничество в сфере закупок товаров, работ и услуг
- Налоговое мошенничество

Основные выводы

Мошенничество: **Когда происходит преступление?**

На основе ответов более 5 000 респондентов, которые стали жертвами мошенников за последние два года, мы собрали самые свежие данные о распространенных видах мошенничества, типаже злоумышленника и опыте успешного противодействия экономическим преступлениям.



5 000+ респондентов

62% руководители высшего звена

72% Компаний с выручкой свыше 10 млн долл. США

99 стран и регионов

42 млрд долл. США убытков

47%

респондентов **стали жертвами экономических преступлений за последние два года.**
Это **второй по значению** уровень экономической преступности за последние 20 лет.

6 случаев мошенничества

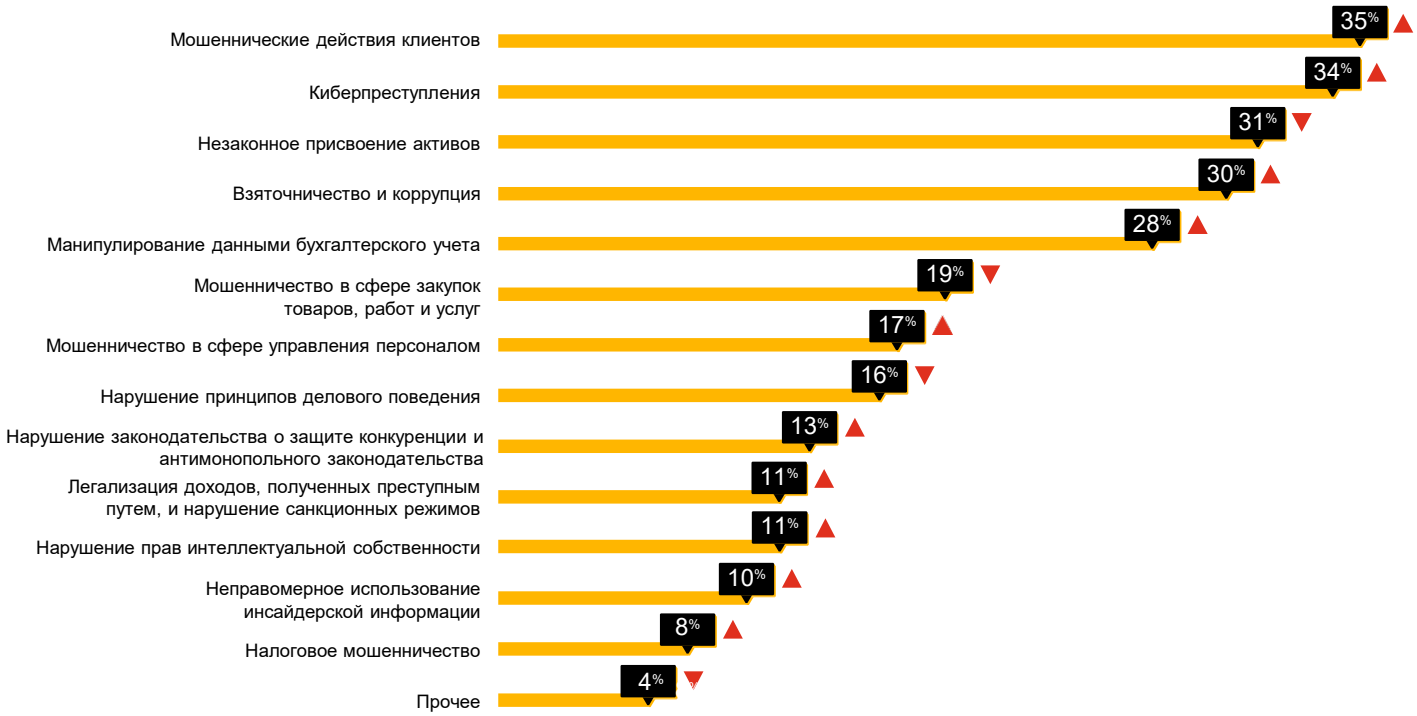
В среднем шесть раз **за последние два года** компании сталкивались с мошенническими действиями.

Самые распространенные виды мошенничества

1. **Мошеннические действия клиентов**
2. Киберпреступления
3. Незаконное присвоение активов
4. Взяточничество и коррупция

В этом году наблюдается значительный рост экономических преступлений следующих видов: мошеннические действия клиентов, манипулирование данными бухгалтерского учета, нарушения антимонопольного законодательства, мошенничество в сфере управления персоналом, взяточничество и коррупция.

Основные виды экономических преступлений



Источник: Всемирный обзор экономических преступлений за 2020 год, PwC

Наиболее значимые виды экономических преступлений - по отраслям

	Потребительские товары и услуги	ТЭК и сырьевой сектор	Финансовые услуги	Государственный сектор	Здравоохранение	Производство промышленных товаров	Информационные технологии, СМИ и теле-коммуникации
1	Мошеннические действия клиентов **18%**	Взяточничество и коррупция **17%**	Мошеннические действия клиентов **27%**	Киберпреступления **17%**	Киберпреступления **16%**	Незаконное присвоение активов **21%**	Киберпреступления **20%**
2	Незаконное присвоение активов **17%**	Незаконное присвоение активов **16%**	Киберпреступления **15%**	Манипулирование данными бухгалтерского учета **17%**	Манипулирование данными бухгалтерского учета **13%**	Киберпреступления **15%**	Манипулирование данными бухгалтерского учета **16%**
3	Киберпреступления **16%**	Манипулирование данными бухгалтерского учета **13%**	Манипулирование данными бухгалтерского учета **14%**	Взяточничество и коррупция **16%**	Мошеннические действия клиентов **13%**	Взяточничество и коррупция **14%**	Мошеннические действия клиентов **13%**

Источник: Всемирный обзор экономических преступлений за 2020 год, PwC

Мошенники: **Кто они?**

Риски мошенничества окружают организации со всех сторон: злоумышленник может оказаться одним из сотрудников компании или действовать извне, а во многих случаях внутренние и внешние мошенники действуют в сговоре. Взаимодействие с бизнес-партнерами по-прежнему представляет риск, и все чаще экономические преступления совершает само руководство компании.

Мошенники: внешние, внутренние, сговор внешних и внутренних

Почти половина выявленных экономических преступлений совершается привлеченными лицами (например, внутренними мошенниками, поставщиками).

Источник: Всемирный обзор экономических преступлений за 2020 год, PwC

Мошеннические действия клиентов (26%). Клиенты оказались не только самыми активными внешними мошенниками (26%), совершающими наиболее серьезные преступления, но и самыми частыми правонарушителями (35% - увеличение показателя с 2018 года).

- Вполне ожидаемо, что мошеннические действия клиентов чаще всего встречаются в сферах финансовых услуг и потребительских товаров и услуг. Это может стать серьезной проблемой, так как все больше компаний переходят на стратегию прямых продаж конечному потребителю.
- Однако есть и хорошая новость. Данный вид экономических преступлений эффективно предотвращается с помощью выделенных ресурсов, построения надежных процессов и технологий противодействия.

Третьи лица (19%). Все чаще компании передают непрофильные процессы внешним подрядчикам, чтобы сократить расходы. Однако такие подрядчики могут оказаться мошенниками. Многие компании пока еще не оценили этот риск надлежащим образом.

- Каждый пятый респондент считает наиболее серьезным случаем внешнего мошенничества мошенничество с участием поставщиков.
- Однако половина респондентов отметила, что в их компаниях отсутствует программа управления рисками при взаимодействии с контрагенами, а у 21% компаний полностью отсутствуют процедуры комплексной проверки благонадежности или мониторинга контрагентов.

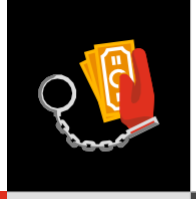
Руководители высшего звена (26%). Как правило, руководители совершают наиболее коварные экономические преступления ввиду того, что их положение (будь то делегированные полномочия, знание системы или влияние) позволяет им обойти (в том числе путем сговора) внутренние системы контроля.

А вас обвиняли в мошенничестве? В этом году мы впервые спросили наших респондентов, обвиняли ли их организацию в мошеннических действиях. Трое из десяти респондентов, пострадавших от мошенничества, сами сталкивались с обвинениями в противоправных действиях, коррупции или совершении другого экономического преступления.

- Примерно с одинаковой частотой поступали обвинения от конкурентов, регуляторов, сотрудников и клиентов.
- В некоторых странах и регионах данной тенденции способствовали программы поощрения корпоративного информирования и ужесточение нормативных требований.

Почти половина выявленных случаев мошенничества, причинивших компаниям **ущерб в размере 100 млн долл. США** или **более, была совершена инсайдерами.**

Источник: Всемирный обзор экономических преступлений за 2020 год, PwC



Оцените последствия:
Чем оборачиваются экономические преступления?

Ущерб от экономических преступлений – всегда комплексный. Некоторые потери можно легко измерить – это прямые финансовые потери или расходы на уплату штрафов, неустоек, ответные меры и меры по устранению нарушений. Однако другие потери оценить не так просто, в том числе ущерб бренду и репутации, ухудшение позиций на рынке, падение морального духа сотрудников, упущенные возможности.

42 млрд долл. США

Ущерба было нанесено действиями мошенников **за последние два года**

Некоторые мошеннические действия, такие как внешнее мошенничество, как правило, носят транзакционный характер и их можно эффективно отслеживать и предотвращать, снижая негативные финансовые последствия для организации.

Другие виды экономических преступлений, такие как взяточничество и коррупция или действия внутренних мошенников, спрогнозировать и отследить труднее; они могут повлечь серьезные штрафы и сопутствующие последствия, такие как потеря бизнеса или ущерб бренду и репутации. Здесь наиболее эффективной будет система управления рисками.

Около 13% респондентов, ставших жертвами экономических преступлений за последние два года, **в целом, потеряли более 50 млн долл. США.**

Топ-5 видов экономических преступлений, наносящих наибольший ущерб. Лидерами по прямым убыткам стали: нарушение антимонопольного законодательства, неправомерное использование инсайдерской информации, налоговое мошенничество, легализация доходов, полученных преступным путем, взяточничество и коррупция. Некоторые из этих видов экономических преступлений также повлекли затраты на устранение последствий и уплату штрафов.

Крупнейшие случаи мошенничества с участием инсайдеров могут иметь гораздо более разрушительные последствия, чем мошеннические действия внешних злоумышленников, и не только из-за более высоких финансовых потерь. 43% выявленных фактов мошенничества, причинивших компаниям ущерб в размере 100 млн долл. США или более, были совершены инсайдерами. Подобные преступления часто приводят к инициированию гражданских или уголовных исков против компании и участников преступления, наносят ущерб репутации. При этом руководство отвлекается от решения других важных задач, а упущенными бизнес-возможностями пользуются конкуренты.

Углубленный анализ

Взяточничество и коррупция также остаются серьезной проблемой. Одна треть респондентов заявили, что их либо просили дать взятку, либо они упустили бизнес-возможность из-за того, что, как они полагают, конкурент дал взятку.

Некоторые из этих ответов были **неожиданными и выявили слабые места:**

- **6 из 10 компаний не имеют программы реагирования на риски, связанные со взяточничеством и коррупцией.**
- Почти половина респондентов либо вообще не проводят процедуры по оценке рисков, либо проводят только неформальную оценку.
- Половина респондентов либо не проводят, либо проводят лишь неформальную оценку благонадежности контрагентов и осуществляют текущий мониторинг с учетом потенциальных рисков.
- Менее чем **3 из 10** компаний выполняют тестирование операционной эффективности имеющихся средств контролей в ограниченном объеме, а **12%** респондентов тестирование не проводят вообще.

Как подготовиться?

Что вы делаете для того, чтобы выявить и предотвратить экономические преступления? Какие программы, методы и технологии эффективны, а какие – нет? Что мешает вам выстроить эффективные меры противодействия, и какие возможности по усилению защиты можно использовать?

Борьба с мошенничеством окупается, но делаете ли Вы достаточно? В среднем компании реализуют четыре специальные программы снижения рисков мошенничества (в более крупных компаниях с численностью персонала свыше 10 тыс. человек таких программ в среднем реализуется больше). Почти две трети компаний имеют соответствующие политики и процедуры, а 6 из 10 респондентов также организуют обучение персонала и проводят мониторинг. **Тем не менее едва половина организаций выделяет специальные ресурсы для оценки и управления рисками и контроля за взаимодействием с контрагентами.**

Какие меры борьбы с мошенничеством наиболее эффективны?

1. **Выявляйте, приоритизируйте все возможные риски и принимайте соответствующие ответные меры.**
   Компании должны выполнять комплексный анализ рисков, собирать данные от заинтересованных лиц как внутри компании, так и за ее пределами, чтобы выявлять риски и оценивать варианты их минимизации. При таком анализе обязательно должны учитываться внешние факторы. В открытом доступе есть огромное количество информации, и игнорирование таких данных может привести к значительным потерям.
   Оценка рисков должна проводиться регулярно (не по принципу «сделал и забыл»).

2. **Усильте ваши технологические решения оптимальной системой управления, экспертизы и мониторинга.**
   Необходимо осознать, что один инструмент не может предотвратить все виды экономических преступлений и что технологии сами по себе не обеспечат надлежащий уровень защиты. Зачастую эффективность того или иного технологического решения целиком зависит от экспертных знаний пользователей, эффективности системы управления данными, обеспечения прозрачности информации, надежных средств контроля и регулярного мониторинга.

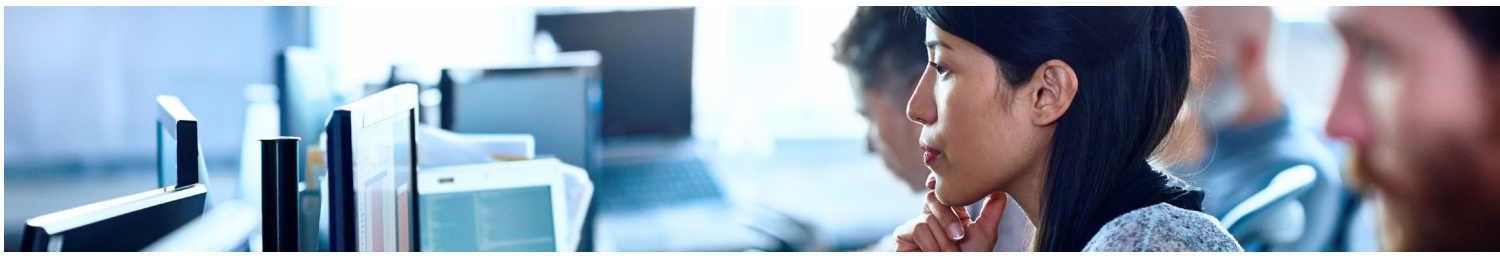
3. **Будьте начеку.**
   Способность быстро реагировать на выявленный факт мошенничества – критически важная составляющая эффективной программы противодействия мошенничеству.
   Способность быстро мобилизовать необходимых специалистов, настроить процессы и технологические решения поможет снизить потенциальный ущерб. Наиболее резонансные преступления, как правило, дают повод задуматься о смене стратегии компании и запуске более масштабной трансформации организации.

Технологии – не лекарство от всех болезней

В последние годы многие компании щедро инвестируют в разработку новых инструментов и технологий, однако на этапе внедрения и развертывания технологических решений значительная часть респондентов сталкивается с затруднениями:

- Менее **3 из 10 компаний** смогли внедрить новые или модернизировать имеющиеся технологии. Среди перечисленных препятствий – высокие затраты, ограниченные ресурсы, отсутствие необходимых систем.
- Что касается альтернативных технологий и подходов, только 25% опрошенных используют искусственный интеллект (ИИ) - столь популярную сегодня технологию. Тем не менее почти 40% компаний, использующих ИИ, пока не видят ощутимых преимуществ от данной технологии для повышения эффективности борьбы с мошенничеством.

Один единственный инструмент или технологическое решение нельзя назвать полноценной программой противодействия мошенничеству. Собираете ли вы необходимые данные в соответствии со всеми правилами и требованиями? Как вы анализируете эти данные? Корректируете ли вы систему в зависимости от результатов анализа, чтобы повысить ее надежность и эффективность? Внедрение новых технологий борьбы с мошенничеством многим компаниям дается нелегко, однако те, кто использует современные инструменты (например, искусственный интеллект), все же получают преимущества при условии, что внедрение таких инструментов прошло корректно.



Действуйте: **делайте то, что нужно**

Как вы поступаете, когда ваша организация сталкивается с экономическим преступлением? **Почти 60% компаний, проводивших расследование фактов мошенничества, удавалось улучшить ситуацию,** однако при этом почти половина респондентов заявили, что вообще не проводили расследований. Треть участников опроса довели информацию о факте мошенничества до сведения совета директоров.

Контролирующие органы, а еще в большей степени, общественность, требуют большего. Слишком медленное реагирование может усугубить текущую ситуацию и привести к более масштабному кризису. Согласно результатам Глобального обзора готовности компаний к кризисным ситуациям, компании, в штате которых числится 5 тысяч сотрудников или более, чаще всего сталкиваются с кризисными ситуациями, возникающими из-за **киберпреступности (26%), стихийных бедствий (22%), неправомерных действий руководства (17%) и нарушений этических норм (16%),** включая мошенничество, коррупцию и злоупотребление служебным положением в компании.

Опрос руководителей крупнейших компаний мира, проведенный PwC в 2020 году, показал, что 58% респондентов обеспокоены своей готовностью к реагированию на кризис

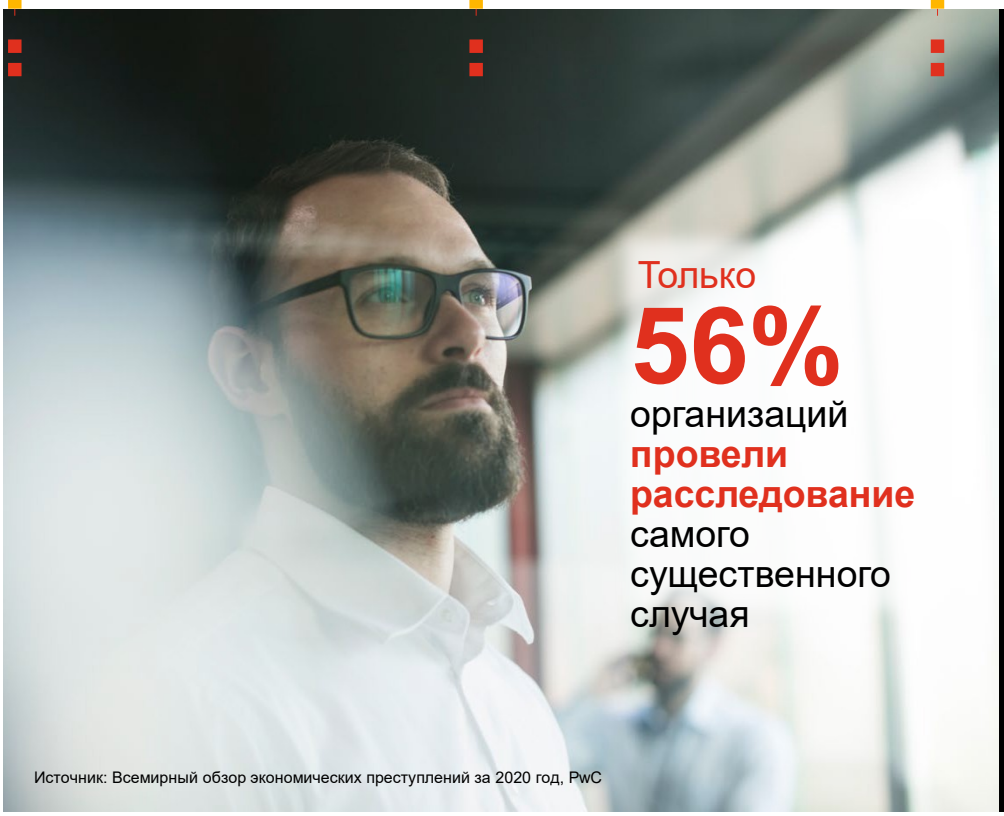
Как организациям удалось преодолеть кризис и улучшить свое положение?

Провели расследование (71%). Для предотвращения дальнейшего ущерба крайне важно добраться до сути проблемы. Компании часто обращаются к внешним организациям за помощью в расследовании фактов мошенничества, когда важна объективность или когда им не хватает ресурсов и знаний для самостоятельного проведения расследований.

Усилили внутренние контроли, регламенты и процедуры (более 50%). Возможно, создание некоторых регламентов и процедур не вызовет затруднений, однако важно оценить операционную деятельность в целом и понять, чего не хватает.

Приняли меры дисциплинарного воздействия в отношении своих сотрудников (44%). Согласно рекомендациям регуляторов, комплаенс-программы должны применяться ко всем без исключения.

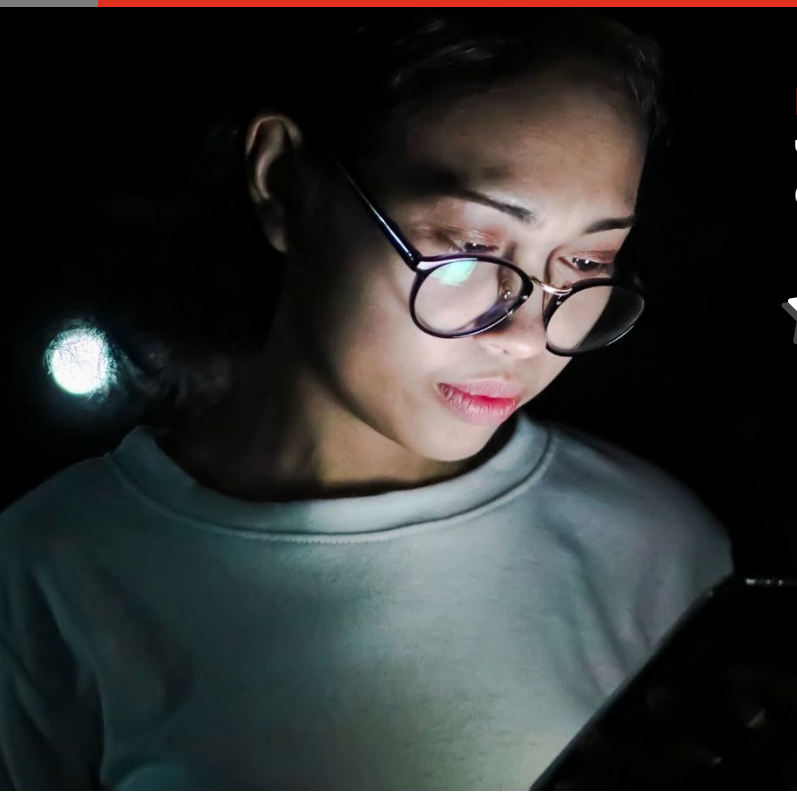
Никого нельзя считать настолько ценным сотрудником, что на него не будут распространяться дисциплинарные меры. Неукоснительное исполнение комплаенс-программ – одно из главных условий их эффективности.



Только **56%** организаций **провели расследование** самого существенного случая

Источник: Всемирный обзор экономических преступлений за 2020 год, PwC

Только треть участников опроса довели эту информацию до сведения совета директоров



Почти 90% опрошенных сообщили, что испытали негативные эмоции, столкнувшись с мошенничеством

42%
испытали положительные чувства и эмоции

89%
испытали негативные чувства и эмоции

Источник:
Всемирный обзор экономических преступлений за 2020 год, PwC

Сообщили о факте мошенничества органам власти (37%). Если сразу сообщить о факте мошенничества, то можно добиться более благоприятных взаимоотношений с регулятором.

Провели обучение (32%). Тренинги позволяют не только повысить информированность сотрудников о новых регламентах и процедурах, но и сформировать культуру борьбы с экономическими преступлениями.

Неудивительно, что большинство опрошенных (**89% к 42%**) сообщили, что испытали отрицательные эмоции в результате факта мошенничества. Однако респонденты, сообщившие о более выгодном положении их организаций после расследования случаев мошенничества, указали, что:

- основной злоумышленник – человек со стороны («мы подверглись атаке»), а не сотрудник организации («один из нас») (**48%**);
- компании выразили уверенность в том, что им удалось сохранить верность своим ценностям, стать одной командой, подготовить и реализовать план действий.

Работа над ошибками

Никто не хочет стать жертвой мошенничества (или быть обвиненным в мошенничестве). Но к серьезным потрясениям можно отнестись иначе: как к переломному моменту, стимулу для организационной трансформации. Приведет ли такая трансформация к отрицательным или положительным результатам (полный крах или укрепление рыночной позиции), зависит от степени готовности бизнеса и от подхода к управлению.

Данные свидетельствуют о больших преимуществах проведения работы над ошибками по итогам рассмотрения инцидентов. **Почти половина (45%) всех респондентов, столкнувшихся с мошенничеством, говорят, что в результате усилили свои позиции:** например, укрепили систему контроля, оптимизировали операционную деятельность, сократили потери, улучшили моральный дух сотрудников. Крупные компании еще чаще (52%) говорят об укреплении своего положения, приводя в пример не только более хорошую атмосферу и прозрачные процессы, но и внедрение новых технологий и сокращение числа повторных инцидентов.

Стать сильнее: **оцените достигнутые успехи**

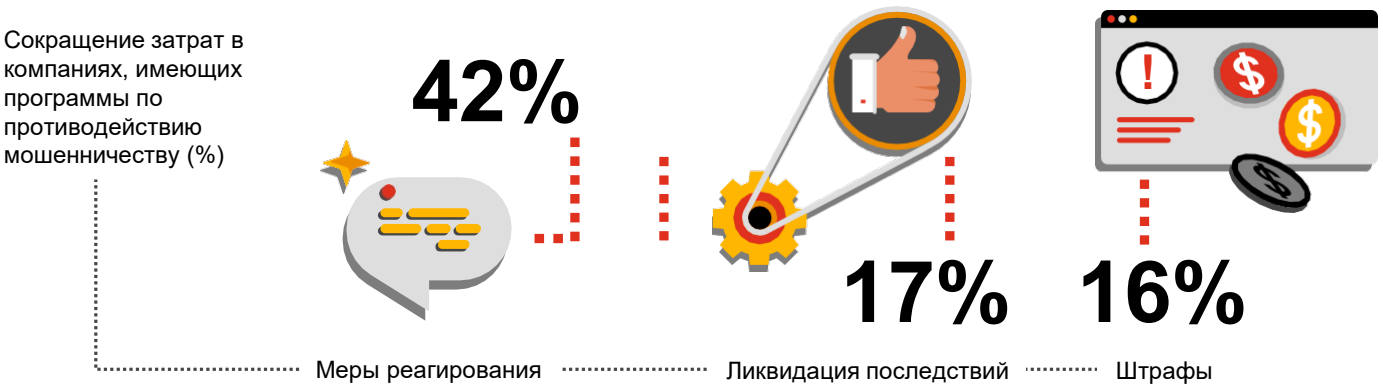
Подразделениям компаний, ответственным за противодействие экономическим преступлениям, зачастую приходится отстаивать увеличение бюджета на новые технологии, программы и увеличение штата. **Почти 40% наших респондентов планируют увеличить расходы на предотвращение мошенничества** в ближайшие два года. Однако, сработают ли эти меры и окупятся ли инвестиции? И как обосновать расходы перед руководством?

Количественная оценка эффекта от применения того или иного инструмента по борьбе с мошенничеством – задача непростая. Здравый смысл подсказывает, что эффективные меры по предотвращению экономических преступлений приводят к сокращению числа и масштабов мошенничества в будущем. Однако посмотрим на еще более интересную статистику: **прослеживается четкая связь между размером инвестиций, заблаговременно направленных на противодействие мошенничеству, и снижением затрат на устранение последствий экономического преступления.**

Компании, где реализуется специальная программа по противодействию мошенничеству, как правило, тратят меньше средств (относительно выручки) на меры реагирования, ликвидацию последствий и уплату штрафов:

- Компании, внедрившие специальную программу по противодействию мошенничеству, потратили на меры реагирования на 42% и на ликвидацию последствий на 17% меньше средств соответственно, чем компании, у которых не было подобных программ.
- Компании, имеющие программы по борьбе со взяточничеством и коррупцией, потратили на ликвидацию последствий выявленных фактов взяточничества и коррупции на 58% меньше средств, чем компании, у которых подобные программы отсутствуют.

Компании, которые инвестировали в программы по противодействию экономическим преступлениям, потратили меньше денег при наступлении случаев мошенничества



Источник: Всемирный обзор экономических преступлений за 2020 год, PwC

Однако, даже при наличии специальной программы важно проводить ее регулярную оценку и доработку. Почему?

- Бизнес-модели часто динамичны и могут измениться еще до того, как будут разработаны или усовершенствованы соответствующие программы управления рисками. В таком случае компания будет подвержена непредвиденным рискам.
- В некоторых отраслях наблюдается сближение: так, технологические компании предлагают финансовые услуги, а медицинские компании выходят на рынки потребительских товаров и услуг. Поэтому программы управления рисками необходимо доработать таким образом, чтобы они охватывали новые области и соответствующие им риски.
- По результатам сообщения на горячую линию или аудиторской проверки может быть выявлен риск, который раньше не учитывался.

Возможно, самое главное – повышенное внимание регуляторов к комплаенс-программам. Некоторые регуляторы требуют от компаний предоставить доказательства эффективности таких программ.

Многие регуляторы признают, что комплаенс-программы должны строиться на основе имеющихся рисков и охватывать релевантные области и что ни одна программа не гарантирует выявления всех недобросовестных действий. Не существует стандартного подхода к соблюдению нормативно-правовых требований. Программа крупной телекоммуникационной компании, несомненно, будет отличаться от программы мелкого ретейлера. Но несмотря на это, обе программы могут надлежащим образом учитывать конкретные риски, с которыми сталкивается каждая организация.

Единого предписанного метода оценки эффективности программ также нет. Есть множество научных статей об оценке эффективности обучения персонала, в которых содержится много полезной информации, но статей, посвященных, к примеру, оценке эффективности программы управления отношениями с контрагентами, не так много.

У компаний есть возможность разработать собственную продуманную систему оценки, охватывающую такие области, как статистика по обоснованию выбора поставщиков, статистика по отказам поставщикам, участие поставщиков в программах обучения, сертификация поставщиков, сокращение числа отклонений/несоответствий, выявленных по результатам внешних проверок операций контрагентов.
Залог успеха – обоснованная оценка, которая сможет показать, что та или иная область программы прошла проверку, и продемонстрировать, каким образом программа позволит предотвратить или выявить случаи неправомерного поведения в будущем.

Заключение

Итак, в каком положении находитесь вы? Можно ли назвать вас лидером с точки зрения предотвращения, выявления случаев мошенничества и реагирования на них? Или вам есть что улучшить в срочном порядке?

В любом случае, нужно действовать. Даже «лучшие» программы по противодействию мошенничеству необходимо регулярно оценивать и пересматривать. Потому что действующие лица и их методы меняются, и ваши системы защиты необходимо корректировать в соответствии с новыми рисками.

В противном случае, если в вашей системе защиты от мошенничества имеются пробелы или недостатки, вы подвергаетесь рискам, а любое экономическое преступление обходится вам все дороже.

От мошенничества нет иммунитета ни у одной компании. И когда после инцидента поднимаются непростые вопросы, то неосведомленность и отсутствие информации не будут служить оправданием.

Пора понять, насколько хорошо вы готовы. Индивидуальное исследование позволит вам оценить свое положение относительно других компаний рынка, отрасли или других стран и определить, какие шаги следует предпринять сейчас, чтобы противостоять мошенничеству в будущем.

Узнать больше

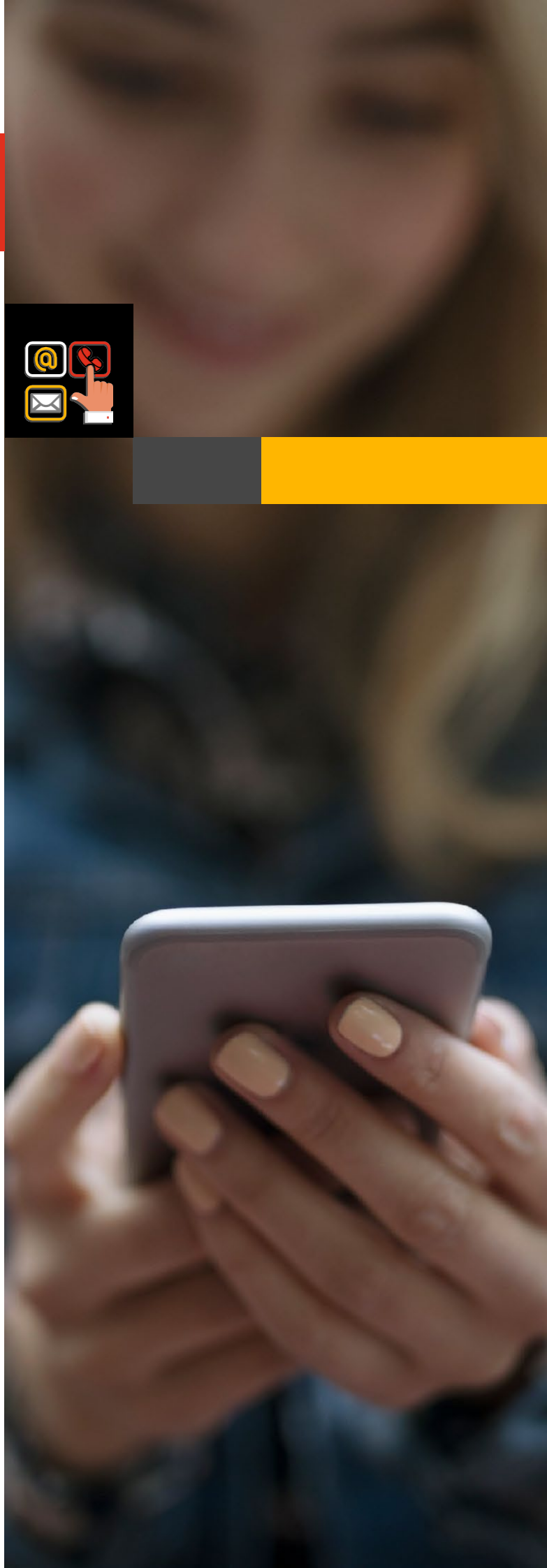
Узнайте больше о рисках экономических преступлений и мошенничества, присущих вашей компании, и оцените свои программы по сравнению с другими компаниями и нашими респондентами из различных стран мира.

Кристин Ривера
Руководитель международной практики по предоставлению услуг в области независимых финансовых расследований – форензик, PwC в США
kristin.d.rivera@pwc.com
+1 415 302 3428м

Лев Виляев
Партнер, Форензик, PwC в России
lev.vilyaev@pwc.com
+7 (495) 232 5703

Инна Фокина
Партнер, Форензик, PwC в России
Inna.fokina@pwc.com
+7 (495) 967 6382

Владимир Нефедьев
Партнер, Форензик, PwC в России
vladimir.nefediev@pwc.com
+7 (495) 232 5587



В PwC наша цель заключается в том, чтобы заручиться доверием общества и решать серьезные задачи. PwC представляет собой сеть фирм в 158 странах, объединяющую свыше 236 000 специалистов, которые готовы оказывать услуги в области аудита, бизнес-консультирования и налогообложения на качественном уровне. Ознакомьтесь с более подробной информацией и расскажите нам о том, что важно для вас, на нашем сайте www.pwc.com.

WLT127074948