www.pwc.com/ua

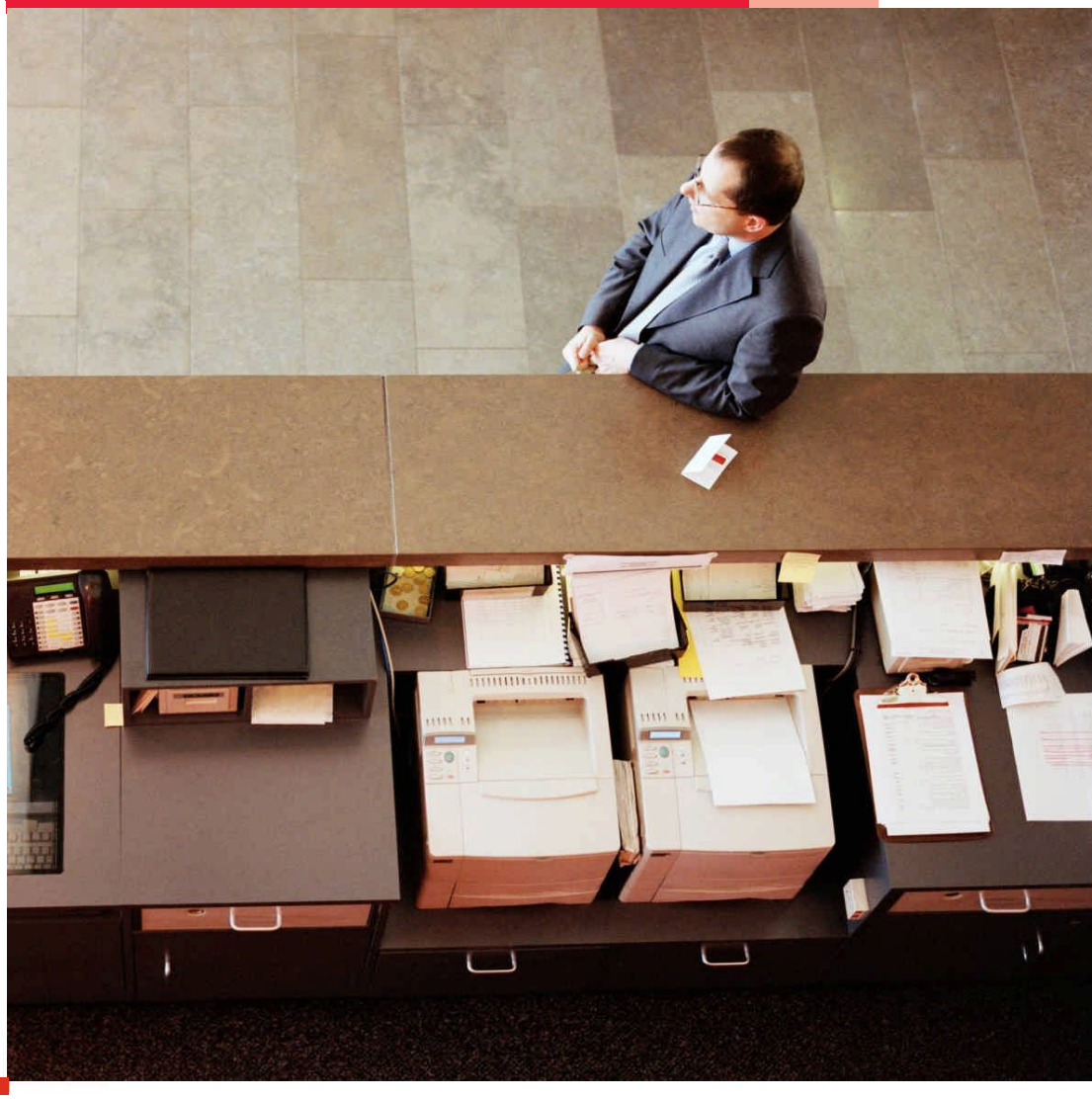
Украина

Всемирный обзор экономических преступлений

Киберпреступления в центре внимания

3 877 респондентов из 78 стран поделились своим мнением об экономической преступности в мире

Декабрь 2011



pwc

Содержание

Общие сведения

Экономическая преступность не имеет границ. Она влияет на организации во всем мире и ни одна отрасль экономики или компания не может чувствовать себя полностью защищенной от нежелательных последствий экономической преступности. Кроме непосредственных убытков, экономическая преступность может нанести серьезный ущерб имиджу организаций или ухудшить их репутацию, что в итоге может привести даже к потере доли на рынке. На сегодняшний день общество становится все менее толерантным к несоблюдению этических норм поведения, поэтому бизнесу необходимо завоевать общественное доверие и постоянно поддерживать его.

В этом году Всемирный обзор экономических преступлений делает акцент на возрастающей угрозе киберпреступности. В наше время многие люди и организации используют различные технологии, включая Интернет. Таким образом, они подвержены риску потенциальных атак мошенников с любого уголка мира. На фоне проблем хищения данных и утечки информации, компьютерных вирусов и атак хакеров, особое внимание в нашем обзоре уделяется значимости этого вида экономической преступности и его влиянию на организации во всем мире.

В ходе нашего исследования проводился сбор мнений представителей различных организаций об экономической преступности. Также в опрос были включены специфические вопросы касательно киберпреступности, которые покрывают риски и угрозы киберпреступности и меры, которые организации предпринимают для реагирования на атаки с использованием компьютерных технологий.

В этом году отчет состоит из двух частей:

1. Киберпреступность и ее влияние на организации, уровень осведомленности о киберпреступности и меры по снижению рисков наступления нежелательных последствий.

2. Экономические преступления, мошенники и жертвы: виды мошенничества, методы обнаружения мошеннических действий, идентификация нарушителей и последствия.

Это уже шестой Всемирный обзор экономических преступлений. В Украине данное исследование проводится во второй раз.

Общее число участников опроса составило почти 4 000 человек из 78 стран, среди которых 53% – директора и топ-менеджеры организаций, 36% участников представляют организации, зарегистрированные на биржах разных стран, и 38% участников представляют организации с численностью персонала более 1 000 человек.

Число респондентов из Украины увеличилось на 23% по сравнению с прошлым опросом. В опросе приняли участие 84 руководителя и представителя высшего руководства организаций, работающих в 13 отраслях экономики.

Основные выводы

Киберпреступность в Украине

- Киберпреступность стала одним из пяти самых распространенных экономических преступлений в Украине.
- Каждый третий респондент (37%) считает, что риск киберпреступности повысился за последние 12 месяцев.
- Более 25% организаций не имеют соответствующих политик и механизмов реагирования на киберпреступления.
- 46% опрошенных не проходили обучения в области кибербезопасности в течение последних 12 месяцев.
- 58% респондентов в Украине ответили, что в их организациях отсутствует процесс мониторинга посещения социальных сетей.

Экономическая преступность в Украине

- 36% организаций сталкивались со случаями экономических преступлений за последние 12 месяцев.
- Треть организаций не проводят оценку рисков мошенничества.
- Незаконное присвоение имущества (73%), коррупция и взяточничество (60%) остаются наиболее распространенными видами экономической преступности в Украине.
- Количество внутренних мошеннических операций существенно выросло (на 22%) по сравнению с 2009 годом.
- Большинство украинских респондентов, которые сталкивались со случаями мошенничества, оценивают убытки до 5 млн. долл. США.
- 40% преступлений совершает высшее руководство.
- По отношению к каждому пятому сотруднику, совершившему экономическое преступление в организации, не было предпринято соответствующих мер.

Отсутствие четкого определения и описания киберпреступности приводит к тому, что организации до конца не осознают связанных с ней рисков. Это усложняет процесс выявления и предотвращения преступлений

Угроза киберпреступности

По мнению специалистов PwC существует 5 основных видов кибератак, цели и методы которых иногда совпадают:

Финансовые преступления и мошенничество. Совершаются организованными и хорошо финансируемыми группами лиц, занимающимися хищением средств и прочих активов с помощью современных технологий.

Шпионаж. На сегодня корпоративная почта и файлы, а также традиционные объекты интеллектуальной собственности, такие как результаты научных исследований и разработок, представляют большую ценность для любой организации. Хищение интеллектуальной собственности – это постоянная угроза. Жертвы могут даже не догадываться о случившемся до момента внезапного появления пиратских копий на рынке или регистрации патента на результаты исследований и разработок третьими лицами.

Военные действия. Сюда относятся военные конфликты между разными странами, а также попытки завладеть организациями частного сектора, в особенности такими важными инфраструктурными объектами национального масштаба, как энергетическая, телекоммуникационная и финансовая системы.

Терроризм. Перекликается с угрозой военных действий. Атаки совершаются террористическими группами (с возможной поддержкой со стороны государства) с целью завладения стратегически важными частными или государственными инфраструктурными объектами.

Активизм. По своей природе напоминает некоторые другие категории, но атаки при этом совершаются сторонниками идеализма.

Не существует общепринятого определения киберпреступности. Соответственно отсутствие четкого определения киберпреступности осложняет процесс выявления и реагирования на кибепреступления, тем более когда организациям даже неизвестно о существующей опасности. Более того, неполное понимание «концепции противника» может свести на нет все попытки борьбы с киберпреступностью.

Возникает вопрос: киберпреступность – это просто инструмент для совершения незаконных действий или отдельный вид экономической преступности?

Должны ли организации предпринимать специальные меры для управления этим риском в дополнение к обычным механизмам выявления и предотвращения мошенничества?

В нашем обзоре за 2011 год мы попытались детальнее разобраться с этими и другими

В нашем обзоре применялось следующее определение киберпреступности: «***Киберпреступность (или «преступление с использованием компьютерных технологий»)*** *– это экономическое преступление, совершенное с использованием вычислительной техники и сети Интернет. Примеры киберпреступности: распространение вирусов, незаконная выгрузка информации, фишинг и фарминг, а также хищение личной информации (например, реквизитов банковских счетов). К этой категории относятся только те экономические преступления, в которых основным (а не вспомогательным или сопутствующим) инструментом совершения преступления является компьютер, Интернет или электронные носители информации и устройства»*[1].

[1] Согласно определения во Всемирном обзоре экономический преступлений за 2011 год, подготовленном PwC при содействии нашего партнера по научным вопросам профессора Питера Соммера.

Киберпреступность – одно из пяти самых распространенных экономических преступлений в Украине

Киберпреступность – это пятый по значимости вид экономической преступности в Украине, вслед за незаконным присвоением имущества, взяточничеством и коррупцией, практикой подрыва конкуренции и манипуляцией с финансовой отчетностью (см. Рис. 1).

По результатам опроса на киберпреступность приходится 23% случаев мошенничества в мире, о которых сообщили участники опроса, и 17% в Украине.

Данные обзора в сфере информационной безопасности свидетельствуют о том, что киберпреступления становятся более изощренными, что усложняет их обнаружение и предотвращение. Это может привести к еще большим убыткам и потерям в будущем.

Новый риск или реальные случаи мошенничества, объемы которого неуклонно растут?

Не все из перечисленных ранее 5 видов кибератак являются типичными для Украины. Однако, совершенно точно можно утверждать, что угроза киберпреступности – это реальная проблема, которая может негативно повлиять на организации в Украине.

В предыдущем Всемирном обзоре экономических преступлений мы уже задавали вопросы по киберпреступности. Ввиду незначительного количества зафиксированных случаев киберпреступности результаты в данной области не были выделены в обзоре за 2009 год.

С учетом повышенной угрозы кибепреступности в обзоре за 2011 год мы акцентировали свое внимание именно на этом виде мошенничества и снова включили вопрос о том, сталкивались ли организации с киберпреступлениями на протяжении последних 12 месяцев.

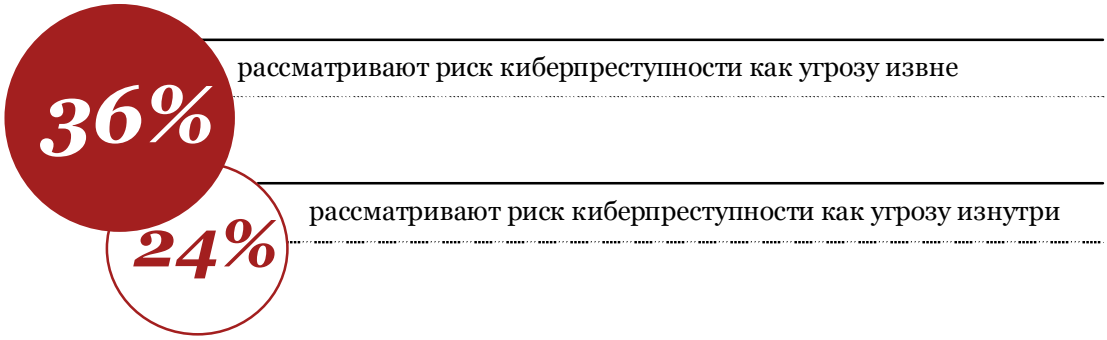
Более трети (37%) опрошенных в Украине подтвердили, что количество случаев киберпреступности в их организациях увеличилось. Около 4% заявили о снижении данного показателя и 59% ответили, что ситуация не изменилась.

Увеличение риска киберпреступности можно объяснить следующими факторами:

- Частое упоминание о случаях кибератак в средствах массовой информации вызвало повышенное внимание к данному виду мошенничества и вынудило организации внедрить дополнительные механизмы контроля, которые и позволили обнаружить большее количество таких экономических преступлений;
- Неоднозначное определение понятия киберпреступности, из-за чего многие респонденты реклассифицировали некоторые традиционные виды экономических преступлений как киберпреступность, поскольку они были совершены с использованием компьютера, электронных устройств или сети Интернет;
- Повышенное внимание со стороны регулирующих органов;
- Использование новейших технологий, «облегчающих» совершение киберпреступлений.

Рис. 1: Пять наиболее распространенных экономических преступлений в Украине и мире в 2011 году

Респонденты, столкнувшиеся с экономической преступностью на протяжении последних 12 месяцев



Киберпреступность – внешняя или внутренняя угроза?

36% респондентов в Украине полагают, что киберпреступность это внешняя угроза, 24% – внутренняя угроза. 34% – считают, что угроза может исходить как извне, так и изнутри организации.

Эти показатели немного отличаются от результатов Всемирного обзора, поскольку 46% респондентов в других странах отмечают, что риск киберпреступности в основном исходит извне, и только 13% полагают, что преступления были совершены сотрудниками организаций. 29% опрошенных считают, что угроза киберпреступности является одновременно внутренней и внешней угрозой.

Каковы источники киберпреступности?

Организациям было предложено ответить на вопрос: риск внешней киберпреступности преимущественно исходит изнутри их страны или из других стран?

Более половины (53%) опрошенных в Украине утверждают, что внешние угрозы киберпреступности возникают внутри страны. Основными кибермошенниками были признаны клиенты и поставщики. При этом более 40% участников опроса сошлись во мнении, что угрозы могут возникать как извне, так и изнутри страны, в которой они осуществляют свою деятельность.

Среди основных предполагаемых стран происхождения киберпреступности украинские респонденты отметили Гонконг (и Китай), Россию и США. Однако значительное количество украинских организаций считают, что угроза киберпреступности может исходить из любой страны мира, включая Украину.

Статистика в мире подтверждает результаты опроса в Украине. В список предполагаемых стран происхождения киберпреступности попали: Гонконг (и Китай), Индия, Нигерия, Россия, США и Украина[1].

На сегодня киберпреступность – это реальная глобальная угроза, которая может исходить из любой страны мира, выходит за рамки конкретной юрисдикции в отличие от многих других традиционных видов экономических преступлений

Каковы внутренние источники киберпреступности?

По мнению 67% опрошенных в Украине отдел информационных технологий (ИТ) является наиболее рисковым подразделением с точки зрения киберпреступности как внутренней угрозы. И это неудивительно, поскольку предполагается, что именно сотрудники отдела ИТ имеют необходимые навыки и возможности для совершения подобного рода преступлений (например, излишние права доступа к системам с возможностью удаления журнала записей событий, что усложняет процесс выявления незаконных действий).

Однако, следует отметить еще один интересный факт: среди других подразделений, подвергающих организации риску киберпреступности, респонденты отметили отдел финансов (47%), отдел маркетинга и продаж (37%), юридический отдел (27%), подразделения вертикали операционной деятельности (22%), а также представителей высшего руководства (29%). Похожая тенденция наблюдается и в других странах.

Наименее рисковыми были признаны отделы информационной и физической безопасности (16%), а также отдел управления персоналом (10%). При этом не следует забывать о том, что мошенниками могут оказаться сотрудники любого отдела.

[1] Страны перечислены в алфавитном порядке

58% опрошенных заявили, что в их организациях отсутствует процесс мониторинга посещения социальных сетей или им неизвестно о наличии такового

Действительно ли социальные сети так опасны?

58% опрошенных в Украине и 60% в мире заявили, что в их организациях отсутствует процесс мониторинга посещения социальных сетей или им неизвестно о наличии такового. Данная статистика настораживает, поскольку такие сайты могут привести к существенным рискам безопасности в случае злоупотреблений со стороны сотрудников.

Молодое поколение активно посещает социальные сети во многом из-за навязанной обществом необходимости делиться информацией с другими. Следовательно, отсутствие мониторинга сайтов социальных сетей может вызвать определенные проблемы для организаций с точки зрения киберпреступности.

При этом следует признать тот факт, что нынешнее поколение выросло вместе с этими сайтами, и практика обмена личной информацией уже давно стала нормой для всего поколения.

Организации должны осознавать, что у молодых специалистов может быть абсолютно другое представление о рисках, которым такие сайты подвергают организации, и для них необходимо организовывать и проводить соответствующие тренинги.

Как снизить риск?

Учитывая признанную во всем мире возрастающую тенденцию кибепреступности, тот факт, что за последние 12 месяцев 46% опрошенных в Украине (42% в мире) не проходили никаких тренингов по кибербезопасности, вызывает беспокойство. Это может свидетельствовать лишь о том, что им неизвестно о рисках, которым киберпреступность подвергает их организации.

Насколько эффективны тренинги в процессе предотвращения киберпреступлений?

Мы задали вопрос о том, какие тренинги по борьбе с киберпреступностью проводились в организациях. Лишь одна шестая опрошенных, прошедших тренинг, заявили, что соответствующее обучение проводилось в формате семинаров или практических занятий. 62% проходили тренинги в удаленном режиме, например, посредством электронных тренингов и т.д.

Незначительное количество тренингов в формате семинаров и практических занятий объясняется значительными временными и финансовыми затратами на их проведение.

Однако 56% опрошенных заявили, что такого рода тренинги являются наиболее эффективными для повышения уровня осведомленности о киберпреступности.

Что делать, если преступление произошло?

Ниже представлены три наиболее популярных варианта реагирования украинских организаций на киберпреступления:

- Обращение к опытным сотрудникам внутри организации для решения вопроса;
- Обращение за помощью к внешним экспертам;
- Информирование правоохранительных органов.

При обнаружении мошенничества, совершенного третьими лицами, организации, как правило, информировали правоохранительные и другие компетентные органы надзора, а также подавали гражданские иски, включая требования о возмещении ущерба или прекращения деловых отношений.

Сотрудники, причастные к мошенническим действиям, были уволены в 73% случаев.

Социальные сети могут и не быть источником киберпреступности, однако они могут использоваться для повышения эффективности средств социальной инженерии, направленных на совершение киберпреступлений или способствующих фишингу. Например, использование социальных сетей для сбора информации о конкретном человеке или сотруднике (так называемая техника «точечного фишинга»), либо для установки вредоносных программ на компьютер пользователя с целью облегчения дальнейшего совершения киберпреступления.

Руководство приходит к пониманию, что безопасность в первую очередь стратегически важный вопрос бизнеса, нежели ИТ

Какие меры реагирования, предпринимают организации?

Как сказано выше, около половины опрошенных, которые столкнулись с экономическими преступлениями за последние 12 месяцев, заявили, что риск киберпреступности увеличивается.

Согласно опроса, киберпреступность – это один из пяти самых распространенных видов мошенничества. С целью снижения риска мошенничества многие украинские организации (50%) внедряют дополнительные технические средства и набирают квалифицированные кадры для предотвращения и обнаружения киберпреступлений, а также проведения служебных расследований.

Как правило, внешние консультанты привлекаются по факту возникновения инцидента (57%). И только 21% организаций в Украине обращаются к внешним экспертам в целях предотвращения киберпреступлений.

Таблица 1: Механизмы реагирования украинских организаций на киберпреступления в 2011 году

Использование внутренних ресурсов для предотвращения и обнаружения преступлений	51%
Использование внутренних ресурсов для проведения служебных расследований	50%
Привлечение форензик-экспертов	45%
Медийные и PR планы менеджмента	38%

% от общего количества участников опроса

Как защитить свою организацию?

1. Заручиться поддержкой генерального директора – правление и генерального директора необходимо проинформировать об угрозе кибепреступности. Необходимо, чтобы высшее руководство располагало полной информацией о рисках, связанных с компьютерными преступлениями.

2. Пересмотреть работу службы безопасности – в отличие от традиционных экономических преступлений, киберпреступность динамично изменяется, постоянно возникают новые риски, и, как следствие, организациям необходимо постоянно адаптировать свои процедуры с учетом этих рисков.

3. Информированность – организациям необходима вся информация о своей текущей и будущей компьютерной среде. Если организация надлежащим образом информирована, она может принимать информированные решения и на их основе реализовать соответствующие меры.

4. Создать группу оперативного реагирования на киберпреступления. Хорошо подготовленная группа оперативного реагирования обеспечит выявление инцидента на любом участке бизнеса, оценку риска и доведение его до сведения руководства.

5. Обучение всех сотрудников – организациям необходимо внедрение культуры «информированности о киберпреступности». Для этого необходимо предусмотреть в штате персонал с соответствующими знаниями, который сможет обеспечить обучение всех сотрудников для создания достаточной информированности о риске киберпреступности в организации.

6. Активная и прозрачная позиция организации по отношению к преступлениям с использованием компьютерных технологий - организация должна активно преследовать нарушителей и информировать общественность об угрозах, фактах нарушений и мерах, принимаемых организацией.

Киберпреступность – это не только ИТ-проблема

Традиционно кибербезопасность относят к сфере ИТ вопросов, что создает недостаточное взаимодействие между сотрудниками бизнес-подразделений и специалистами по информационной безопасности.

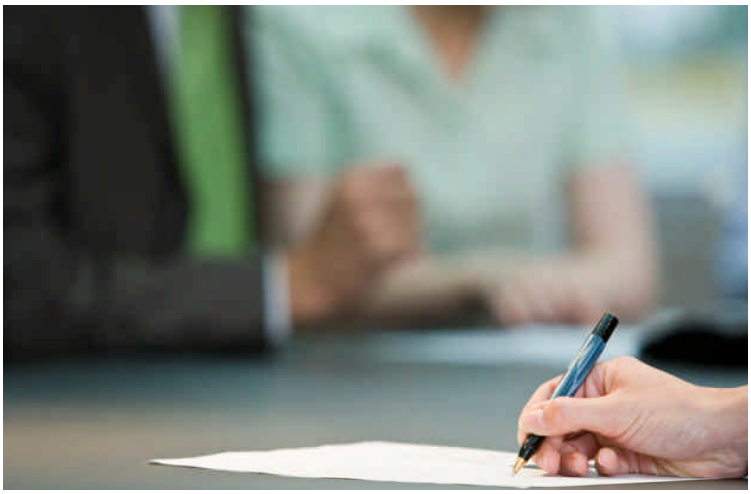
Результаты Всемирного обзора состояния информационной безопасности в 2011 году, подготовленного PwC, свидетельствуют о том, что обеспечение кибербезопасности – это не только вопрос технического характера, но и одна из обязанностей бизнес-подразделений.

На вопрос о том, кто должен нести общую ответственность за устранение угроз киберпреступности, больше половины опрошенных (67%) указали директора по ИТ или директора по технологиям и только 13% назвали генерального директора или членов правления организации. Это значит, что независимо от того, входит ли директор по ИТ в состав правления организации или нет, он не совмещает общую ответственность с генеральным директором или правлением в целом.

Только 20% респондентов заявили, что генеральный директор и члены правления обсуждают оценку таких рисков по меньшей мере 1 раз в год. 32% опрошенных ответили, что данное обсуждение проводится по мере необходимости, в то время как 25% отметили, что оценка этих рисков в их организации вообще не проводится.

Мы предполагаем, что в будущем генеральные директора и члены правлений организаций будут рассматривать вопросы, связанные с риском киберпреступности, на регулярной основе.

36% организаций в Украине столкнулись со случаями экономических преступлений за последние 12 месяцев



Обзор экономических преступлений в Украине

36% из 84 респондентов в Украине сообщили о том, что за последний год они столкнулись хотя бы с одним случаем экономического преступления. Этот показатель выше, чем в мире (34%), однако он ниже по сравнению с данными по Украине за 2009 год (45%).

Мы можем предположить, что результаты обзора за 2009 год находились под влиянием экономической рецессии, следствием которой являлся рост числа мошеннических действий.

В 2011 году снижение уровня мошенничесива в украинских компаниях можно объяснить неэффективностью его обнаружения, а не фактическим сокращением количества таких случаев.

В свете этого мы сравнили число случаев мошенничества, о которых сообщили организации, регулярно проводящие оценку рисков, с данными организаций, которые не проводят такой оценки.

В результате, организации, регулярно проводящие оценку рисков, заявляют о большем числе злоупотреблений и высокой частоте таких случаев.

Однако, мы ожидаем, что топ-менеджмент должен быть информирован об экономических преступлениях. Так в 2011 году топ-менеджмент оказался более осведомленным о случаях злоупотреблений в своих организациях по сравнению с 2009 годом: только 10% респондентов, которые являются представителями топ-менеджмента, сообщили о том, что они не знали о случаях мошенничества в своих организациях (55% в 2009 году).

Для обеспечения эффективности деятельности организациям необходимо уделять больше внимания процедурам предотвращения мошенничества и управления рисками мошенничества.

Организации, которые проводят оценку рисков, отмечают большее количество случаев мошенничества и сталкиваются с такими случаями чаще.

Статистика мошенничества по видам организаций

Большинство участников обзора в Украине – это представители частных (69%) и публичных организаций (24%).

Представители правительственных, государственных и неприбыльных организаций, которые составляют 7% участников обзора, ответили, что они не сталкивались со случаями злоупотреблений за последний год или им не известно о таких случаях.

Однако частные компании сталкивались со случаями экономических преступлений почти в 3 раза чаще, чем публичные организации. Наиболее распространенными видами злоупотреблений в частных компаниях являются:

- незаконное присвоение имущества (31%);
- коррупция и взяточничество (29%);
- манипуляции с финансовой отчетностью (14%).

Статистика для публичных компаний:

- незаконное присвоение имущества (37%);
- коррупция и взяточничество (21%);
- киберпреступность (16%).

Рис. 2: Виды мошенничества в Украине в 2009 и 2011 годах

% респондентов, столкнувшихся с экономической преступностью в 2009 и 2011 годах

С какими видами экономических преступлений сталкиваются организации в Украине?

Существует много видов экономических преступлений, причем некоторые из них более распространены и встречаются систематически. В 2011 году наиболее распространенным видом экономических преступлений в Украине было незаконное присвоение имущества (73%), на втором месте оказалось взяточничество и коррупция (60%), на третьем – манипуляции с финансовой отчетностью (30%).

Результаты опроса свидетельствуют о том, что украинские компании гораздо больше страдают от «взяточничества и коррупции» и «практики недобросовестной конкуренции», чем другие страны в Центральной и Восточной Европе и мире (см. Таблицу 2).

Значительное количество инцидентов злоупотреблений, о котором сообщают наши респонденты, также означает, что эти виды злоупотреблений не только наиболее распространенны, но и могут быть выявлены проще, чем другие виды экономических преступлений.

Количество случаев «незаконного присвоения имущества» и «практики недобросовестной конкуренции» выросло почти на 15% по сравнению с 2009 годом. В то же время, «взяточничество и коррупция» и «манипуляции с финансовой отчетностью» остались на том же уровне.

Это побуждает мошенников разрабатывать все более изощренные схемы мошенничества, которые могут остаться невыявленными. В наши дни мошенники располагают широким арсеналом приемов, в то время как специалисты по внутренним расследованиям только начинают разрабатывать механизмы предотвращения и выявления злоупотреблений. Экономическая рецессия привела к тому, что организации с неохотой инвестируют в такие услуги, как внутренний аудит или внутренние финансовые расследования.

Таблица 2: Виды злоупотреблений в Украине, по которым наблюдается значительное отличие от стран Центральной и Восточной Европы и мира в 2011 году

	Взяточничество и коррупция	Практика недобросовестной конкуренции
Украина	60%	23%
Центр.-Вост. Европа	36%	12%
Мир	24%	7%

% от общего количества респондентов, столкнувшихся со случаями экономических преступлений на протяжении последних 12 месяцев

Имеет ли значение размер организации?

В этом году результаты опроса показывают, что все украинские организации (независимо от их размера) в равной степени страдают от экономических преступлений.

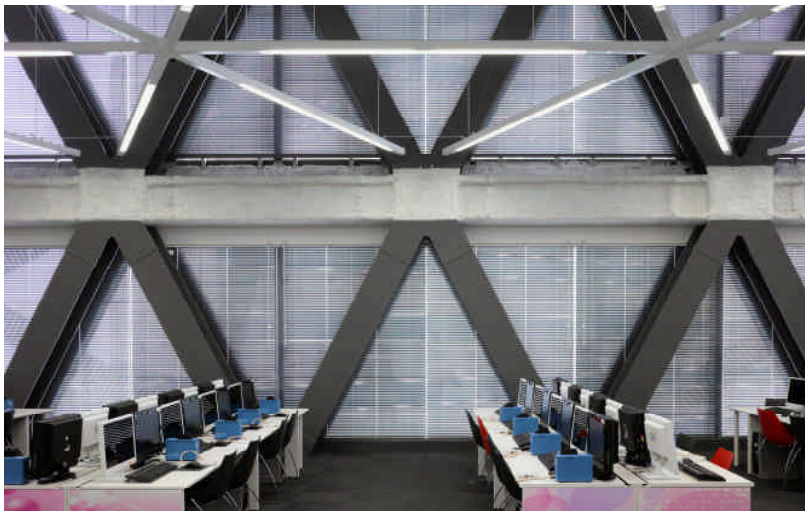
Таблица 3: Злоупотребления в Украине в 2011 году с разбивкой по размеру организаций

До 200 сотрудников	27%
201 – 1 000 сотрудников	30%
1 001 – 5 000 сотрудников	23%
Более 5 000 сотрудников	20%

% от общего количества респондентов, столкнувшихся со случаями экономических преступлений на протяжении последних 12 месяцев

* в 2009 в качестве варианта ответа не предлагался

Более 40% респондентов в Украине ожидают случаи коррупции и взяточничества в следующие 12 месяцев



Какие отрасли больше всего страдают от экономической преступности?

В этом году в опросе представлены взгляды представителей более 13 различных отраслей. Финансовые услуги, розничная торговля, производство потребительских товаров, промышленное производство и профессиональные услуги представляют более половины (63%) от общего числа участников опроса в Украине и мире.

Каждый второй респондент, работающий в секторе финансовых услуг, энергетики и горнодобывающей промышленности за последние 12 месяцев столкнулся с экономическими преступлениями.

Мы провели сравнение фактов экономической преступности по отраслям и отметили рост числа таких случаев в 2011 году в отрасли розничной торговли и производстве потребительских товаров на 6%, а в секторе финансовых услуг – на 5%.

Будущие ожидания

Несмотря на уменьшение по данным опроса уровня взяточничества и коррупции на 9%, свыше 40% респондентов из Украины ожидают такие случаи в течение следующих 12 месяцев. Кроме того, ведущие позиции в опросе среди ожидаемых видов злоупотреблений занимают нарушение прав интеллектуальной собственности (36%) и незаконное присвоение имущества (35%).

Для сравнения, организации в мире ожидают роста случаев незаконного присвоения имущества (34%), киберпреступности (26%) и взяточничества и коррупции (23%).

Таблица 4: Виды мошенничества, ожидаемые в будущем организациями в Украине

Взяточничество и коррупция	42%
Нарушение прав интеллектуальной собственности	36%
Незаконное присвоение имущества	35%
Манипуляции с финансовой отчетностью	25%
Киберпреступность	25%
Практика недобросовестной конкуренции	24%
Отмывание денег	17%
Налоговое мошенничество	14%
Торговля инсайдерской информацией	12%
Промышленный шпионаж	10%

% от общего количества респондентов

Рис. 3: Злоупотребления по отраслям экономики в Украине в 2011 году

% респондентов, столкнувшихся с экономической преступностью за последние 12 месяцев

40% преступлений в Украине совершает высшее руководство

Наиболее типичный мошенник во всем мире – это, так называемый, «белый воротничок».

Типичный субъект экономических преступлений – это мужчина старше тридцати лет с высшим образованием, устойчивой психикой и стабильной семьей.

Портрет мошенника

В этом году организации в равной степени страдают от злоупотреблений, совершенных как своими сотрудниками, так и внешними преступниками, при этом с 2009 года число серьезных экономических преступлений, совершенных сотрудниками, выросло на 22%.

Таблица 5: Субъекты злоупотреблений

	2011	2009
Сотрудники	50%	28%
Внешние стороны	47%	72%
Неизвестно	3%	0%

% от общего количества респондентов, столкнувшихся с экономической преступностью

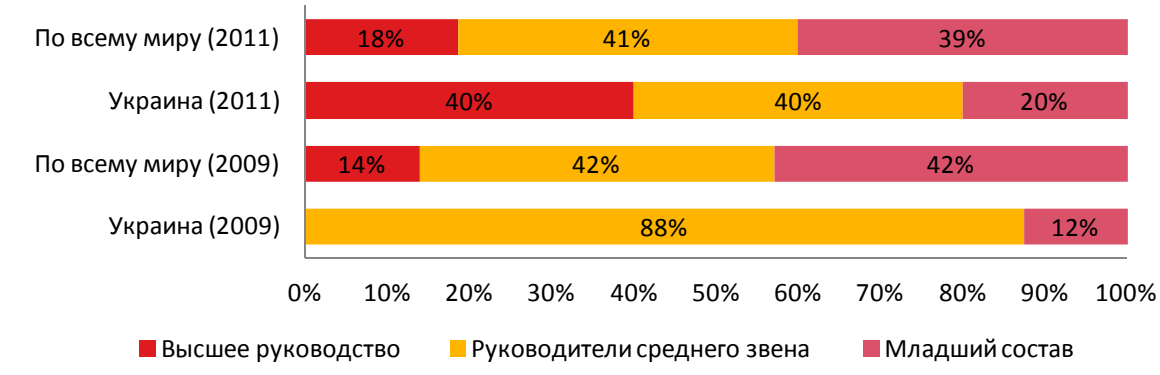
Большинство должностных преступников в Украине – представители высшего (40%) и среднего (40%) руководящего звена. В мире 60% внутренних преступлений совершает руководство среднего звена и рядовые сотрудники.

Типичный субъект экономических преступлений в Украине – это мужчина с высшим образованием в возрасте 31-50 лет, работающий в организации 3-10 лет.

И в Украине, и в мире основной внешний субъект злоупотреблений – это клиент (43% в Украине и 35% в мире). Кроме того, распространенные внешние виновники злоупотреблений – это агенты и посредники (14%), поставщики (14%).

Один из важнейших инструментов предотвращения мошенничества является подход «знать с кем вы имеете бизнес отношения». Поэтому важнейшим элементом программ по минимизации рисков становится анализ клиентов, поставщиков и агентов.

Рис. 4: Основные субъекты должностных преступлений в Украине и мире



% респондентов, столкнувшихся с экономической преступностью в 2009 и 2011 годах

Убытки большинства организаций Украины, столкнувшихся с экономической преступностью за последние 12 месяцев, составили в среднем до 5 млн. долларов США

Сколько организациям стоит мошенничество?

Большинство респондентов, столкнувшихся с экономической преступностью за последние 12 месяцев, оценивают убытки до 5 млн. долларов США. Наиболее дорогими для организаций оказались три наиболее распространенных вида злоупотреблений, а именно, незаконное присвоение имущества, взяточничество и коррупция, манипуляции с финансовой отчетностью. По сравнению с 2009 годом в 2011 году отмечено существенное увеличение частоты этих видов злоупотреблений и убытков от них.

Случаи мошенничества, совершаемого сотрудниками, обычно приводят к большим убыткам, чем при злоупотреблениях внешних сторон, например, клиентов, поставщиков или агентов.

Стоимость преступления растет с возрастом мошенника. Так, самые «дорогие» преступления (5-100 млн. долл. США) были совершены лицами старше 50 лет.

Стоимость сопутствующего ущерба

Финансовые убытки – лишь один из аспектов ущерба, который несут организации от мошеннической деятельности, и часто – далеко не самый значительный. Сопутствующий ущерб и его негативное влияние на репутацию и бренд, стоимость акций, настроения в коллективе, отношения с партнерами приводят к значительным убыткам у многих бизнесов.

Из тех организаций, которые столкнулись с экономическими преступлениями в 2011 году, 23% сообщают об ухудшении настроений в коллективе, 17% – об ущербе бренду организации и 13% – об ущербе деловым отношениям и отношениям с регуляторами.

Хотя эти цифры соответствуют результатам в мире, в 2011 году сопутствующий ущерб значительно ниже в сравнении с 2009 годом. В 2009 г. об ухудшении настроения в коллективе сообщило 34% респондентов, об ухудшении отношений с регуляторами – 34%, с бизнес-партнерами – 28%, и об ущербе бренду – 14%.

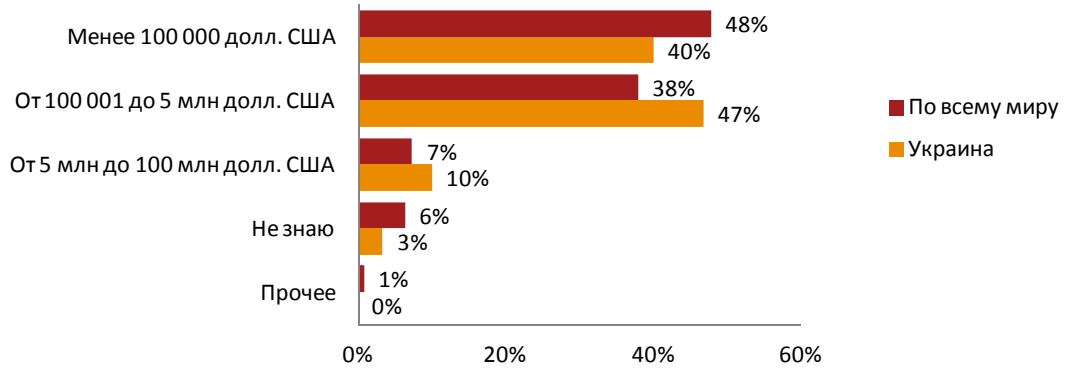
Таблица 6: Сравнение сопутствующего ущерба в Украине в 2009 и 2011 годах

	2011	2009
Отношения с регуляторами	13%	34%
Настроения в коллективе	23%	34%
Отношения с бизнес-партнерами	13%	28%
Репутация/бренд	17%	14%
Цена акций	7%	1%

% от общего количества респондентов, столкнувшихся с экономической преступностью

Низкие показатели сопутствующего ущерба в 2011 году оказались неожиданными. Злоупотребления рассматриваются, как неотъемлемая черта бизнеса в Украине, что приводит к формированию порочного круга: организации оправдывают потенциальные злоупотребления и тем самым повышают их вероятность.

Рис. 5: Финансовые убытки от экономических преступлений в Украине и в мире в 2011 году



% респондентов, столкнувшихся с экономической преступностью за последние 12 месяцев

Как организации обнаруживают мошенничество?

Обнаружение мошенничества предполагает все методы, используемые организацией для установления факта экономического преступления. В 2011 году украинские респонденты сообщили о следующих наиболее эффективных способах обнаружения мошенничества.

В Украине большинство преступлений обнаруживает Служба корпоративной безопасности организации, и только 6% злоупотреблений выявляет Служба внутреннего аудита. Результаты всемирного обзора свидетельствуют о совершенно иной ситуации.

Также следует отметить, что 27% респондентов не знали о методах обнаружения мошенничества по сравнению с 10% респондентов в мире. Это означает, что организации в других странах поддерживают высокий уровень осведомленности о программах противодействия мошенничеству.

Более половины участников опроса в Украине (54%) не используют систему анонимного оповещения. Однако, 82% респондентов, которые используют такую систему, считают ее эффективной.

Какие меры применяются организациями против мошенников?

73% сотрудников, совершивших мошенничество, были уволены или против них были поданы гражданские иски, включая требование о возмещении нанесенного ущерба. Примечательно, что организации не приняли никаких мер против мошенников в 20% случаев. В 2009 году этот показатель составил только 3%, и эта статистика вызывает беспокойство.

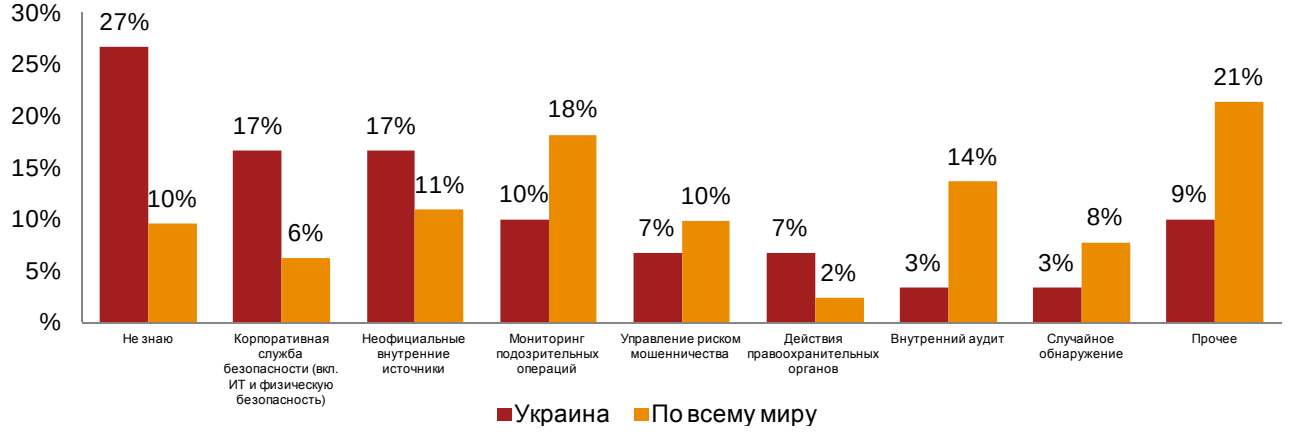
Так, в некоторых организациях наблюдается отсутствие обеспокоенности или желания активно противодействовать мошенничеству. Возникает вопрос, стоит ли удерживать мошенника в организации и подвергаться риску повторных злоупотреблений? Мы считаем, что организации должны непримиримо относиться к случаям злоупотреблений и принимать жесткие меры против мошенников с привлечением официальных органов.

Украинские организации приняли следующие меры против внешних мошенников:

- информирование правоохранительных органов (71%);
- подача гражданских исков, включая требования о возмещении ущерба (64%);
- прекращение деловых отношений (57%);
- уведомление соответствующих органов надзора (43%).

Эти показатели совпадают с мировой статистикой, а также с результатами обзора за 2009 г. Также настораживает тот факт, что 43% респондентов заявили о том, что их организации продолжают поддерживать деловые отношения с контрагентами, совершившими мошенничество. Этот факт поднимает фундаментальные вопросы касательно корпоративной культуры таких организаций.

Рис. 6: Методы обнаружения мошенничества, использованные в Украине и в мире в 2011 году



% респондентов, столкнувшихся с экономической преступностью за последние 12 месяцев

Терминология

Ввиду многообразия видов экономических преступлений, предусмотренных законодательством разных стран, в рамках данного обзора мы определили их следующие категории, для того чтобы помочь респондентам в заполнении вопросника.

Коррупция и взяточничество (включая рэкетирство и вымогательство)

Незаконное использование служебного положения с целью получения личных выгод в нарушение должностных обязанностей, включая обещание экономических льгот или оказание иной поддержки, использование угроз и шантажа. Также относится к принятию таких поощрений.

Манипуляции с финансовой отчетностью

Финансовая отчетность и другая документация искаженная или представлена таким образом, что не отражает действительную стоимость или фактические финансовые результаты организации, включая манипуляции с учетными записями, злоупотребления с заемными средствами/привлечением финансирования, незаконное проведение кредитных и несанкционированных операций, нестандартных торговых операций.

Механизм реагирования на преступления с использованием компьютерных технологий

Обычно, сюда относятся разработанные организацией средства предотвращения, выявления и расследования преступлений с использованием компьютерных технологий, сотрудничество с экспертами по финансовым расследованиям, медийные и PR планы.

Мошенничество, связанное с устойчивым развитием

Мошенничество, связанное с устойчивым развитием (см. обеспечение устойчивого развития), включая рынки торговли квотами на выброс углерода, экологические иски или официальные заявления.

Нарушение прав интеллектуальной собственности (включая торговые марки, патенты, контрафактные товары и услуги)

Сюда относится подделка и распространение поддельных товаров с нарушениями в области патентов и/или авторского права, а также создание фальшивых денежных купюр и монет с намерением их использования в качестве настоящих.

Недобросовестная конкуренция

Это – методы, которые препятствуют или подрывают конкуренцию на рынке, включая картельные соглашения со сговором с конкурентами (например, ценообразование, мошенничество в ходе торгов и разделение рынка) и злоупотребление монопольным положением.

Незаконное присвоение имущества (включая растраты/хищения со стороны сотрудников)

Кража имущества (включая денежные средства или ТМЦ и оборудование) руководством, другими доверенными лицами или сотрудниками в личных корыстных целях.

Обеспечение устойчивого развития

Деятельность по торговле квотами на выброс углерода (покупка или продажа квот), участие в проектах, в рамках которых осуществляется взаимозачет квотами на выброс углерода.

Отмывание денег

Действия, нацеленные на узаконивание доходов от преступной деятельности с сокрытием действительного источника их происхождения.

Оценка риска мошенничества

Оценка риска мошенничества используется для проверки того, что организация проанализировала следующие аспекты:

(i) Риски мошенничества, с которыми она сталкивается;

(ii) Оценка наиболее существенных рисков (т.е. оценка рисков на предмет существенности и вероятности возникновения);

(iii) Идентификация и оценка функционирующих механизмов контроля (при их наличии), которые используются для минимизации ключевых рисков;

(iv) Оценка общих программ и механизмов контроля для предотвращения мошенничества в организации;

(v) Меры по устранению пробелов в системе контроля.

Топ-менеджер

Топ-менеджер (например, Генеральный директор, Управляющий директор или Исполнительный директор) – это лицо, ответственное за принятие решений в организации.

Торговля инсайдерской информацией

Инсайдерская торговля обычно относится к покупке или продаже ценных бумаг с нарушениями в области фидуциарных обязанностей и других доверительных отношений вследствие обладания существенной непубличной информацией о ценных бумагах. Такие нарушения могут также включать умышленное раскрытие такой информации, торговлю ценными бумагами лицом, которое обладает секретной информацией, и торговлю ценными бумагами лицами, которые незаконно завладели такой информацией.

Шпионаж

Шпионаж – это действие или практика использования шпионов для получения секретной информации или использования технологий для того, чтобы действовать от имени организации.

Экономическое преступление или мошенничество

Преднамеренный обман с целью хищения денежных средств, имущества или законных прав.

Контакты

PwC помогает организациям и частным лицам достигать поставленных целей. Международная сеть фирм PwC работает в 158 странах, где 169 000 специалистов предоставляют аудиторские, налоговые и консалтинговые услуги наивысшего качества. Вы можете высказать свои пожелания и получить более детальную информацию о деятельности фирм сети PwC на сайте www.pwc.com.

Форензик – финансовые расследования

Крупнейшая в мире практика по предоставлению услуг в области финансовых расследований (форензик), насчитывающая 1 400 профессиональных консультантов в 63 странах, позволяет PwC использовать их экспертные знания и огромный практический опыт для решения сложных ситуаций, в которых оказались компании, работающие в различных отраслях в многочисленных юрисдикциях.

Наша динамично развивающаяся практика по предоставлению услуг в области финансовых расследований в Центральной и Восточной Европе насчитывает более 70 профессиональных консультантов, включая бухгалтеров, экономистов и специалистов в области информационных технологий.

Мы предоставляем следующие услуги:

- Корпоративные расследования
- Управление рисками мошенничества
- Поддержка в ходе хозяйственных споров
- Международный арбитраж
- Споры с акционерами и в связи со сделками по слиянию и поглощению, а также связанные с этим расследования
- Технологические решения для проведения финансовых расследований
- Услуги по выявлению мошенничества в области интеллектуальной собственности
- Консультационные услуги в области управления лицензированием
- Консультационные услуги в связи со страховыми исками
- Противодействие легализации доходов, полученных незаконным путем
- Консультации в рамках инвестиционных проектов
- Поддержка в расследованиях, проводимых регулирующими органами США, и в судебных разбирательствах по ценным бумагам

Эксперты PwC в области форензик-услуг

Рафаль Краснодебски

Партнер

Услуги в области бизнес консультирования

rafal.krasnodebski@ua.pwc.com

Ирина Новикова

Партнер

Форензик-услуги в России

irina.n.novikova@ru.pwc.com

Геннадий Чуприков

Старший менеджер

Руководитель группы форензик-услуг в Украине

gennadiy.chuprykov@ua.pwc.com

Виктория Цыцак

Менеджер

Форензик-услуги в Украине

victoriya.tsytsak@ua.pwc.com