

*Слабинский Д. В., канд. экон. наук, доц.
Белгородский государственный технологический университет им. В.Г. Шухова*

ЭКОНОМИЧЕСКАЯ ПРИРОДА, СОДЕРЖАНИЕ И ВИДЫ КОРПОРАТИВНОГО МОШЕННИЧЕСТВА КАК ОБЪЕКТ УЧЕТНО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ КОРПОРАТИВНОГО МЕНЕДЖМЕНТА

dslabinskiy@gmail.com

В статье рассматриваются юридические и социально-психологические аспекты мошенничества и его подвидов корпоративного мошенничества: коррупции, манипуляций в финансовой отчетности и хищения активов. Рассмотрены исследования крупных аудиторских организаций, составлен «портрет» и описание типичного мошенничества.

Ключевые слова: финансовая отчетность, аудит финансовой отчетности, внутренний контроль, мошенничество, Международные стандарты финансовой отчетности

*В Аверн спуститься нетрудно,
День и ночь распахнута дверь в обиталище
Дита.*

*Вспять шаги обратить и к небесному свету
пробиться –*

Вот что труднее всего!

- Вергилий. «Энеида», книга шестая

*Прим. Аверн – озеро в Италии, через которое,
по верованиям древних римлян, лежал путь в царство
мертвых. Дит – бог подземного мира*

Рассмотрим, как трактуется термин «мошенничество» в современном понимании. Так, согласно российскому законодательству мошенничество представляет собой «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» (ст. 159 УК РФ). Наказание за мошенничество представлено нами в табл. 1:

Таблица 1

Наказания за различные виды мошенничества в России

Мошенничество:	(а) штраф до 120 000 руб. или размер годового дохода; (б) обязательные работы до 360 часов; (в) исправительные работы до 1 года; (г) ограничение свободы до 2 лет; (д) принудительные работы до 2 лет; (е) арест до 4 месяцев; (ж) лишение свободы до 2 лет
- совершенное группой лиц по предварительному сговору либо с причинением значительного ущерба гражданину (не менее 2 500 руб.)	(а) штраф до 300 000 руб. или размер двухлетнего дохода; (б) обязательные работы до 480 часов; (в) исправительные работы до 2 лет; (г) принудительные работы до 5 лет с ограничением свободы до 1 года; (д) лишение свободы до 5 лет с ограничением свободы до 1 года;
- совершенное с использованием служебного положения либо в крупном размере (свыше 250 000 руб.)	(а) штраф от 100 000 до 500 000 руб. или размер дохода за срок от 1 до 3 лет; (б) принудительные работы до 5 лет с ограничением свободы до 2 лет; (д) лишение свободы до 6 лет со штрафом до 80 000 руб. или дохода за 6 месяцев ограничением свободы до 1,5 лет;
- совершенное организованной группой либо в особо крупном размере (1 млн. руб.), или повлекшее лишение права гражданина на жилое помещение	(а) лишение свободы до 10 лет со штрафом до 1 млн. руб. или в размере дохода до 3 лет и с ограничением свободы до 2 лет.
- отдельно выделены мошенничество: (а) в сфере кредитования; (б) при получении выплат; (в) с использованием платежных карт; (г) в сфере предпринимательской деятельности; (д) в сфере страхования; (е) в сфере компьютерной информации	Ответственность та же, что и выше, кроме (г) – мошенничества в сфере предпринимательской деятельности. В зависимости от размера, (а) штраф от 500 000 до 1 500 000 руб., (доход за 1-3 года) (б) обязательные работы в 240 часов (в случае крупного и особо крупного размера не применяется); (в) принудительные работы до 3-5 лет (крупный и особо крупный размер); (г) ограничение свободы до 1-2 лет; (д) лишение свободы до 3-5 лет.

В Великобритании, согласно Закону о мошенничестве 2006 г. (*Fraud Act 2006*), оно классифицируется на три категории – умышленный обман (*false representation*), сокрытие информации (*failing to disclose information*) и злоупотребление положением (*abuse of position*). При признании лица виновным, ответственность установлена от 12 месяцев лишения свободы (при суммарном правонарушении – *summary conviction*) до 10 лет лишения свободы и штрафа при индикционном правонарушении (*indictable offence*).

Прим. **Суммарное правонарушение** (*summary offence*) – в системе англосаксонского обычного (прецедентного) права (*common law*) уголовное преступление, наименее тяжкое по степени ответственности. Процесс по такому преступлению может проходить без суда присяжных или обвинительного заключения (необходимого при индикции)

Индикционное правонарушение, (*indictable offence*) – уголовное правонарушение в системе обычного права, требующее обвинительного заключения

В США, согласно нормам обычного права, мошенничество состоит из девяти элементов:

- ссылка на существующий факт;
- его существенность;
- его фальсификация;
- осведомленность ответчика о фальсификации факта;
- убежденность ответчика в действиях истца;
- незнание истца о фальсификации факта;
- убежденность истца в достоверности факта;
- правомочность истца на такую убежденность;
- последующие убытки истца.

При этом, в зависимости от штата, установлены различные формы ответственности за мошенничество.

Рассмотрев мошенничество в общем смысле, перейдем к интересующему нас подвиду – корпоративному мошенничеству.

В российском законодательстве термин «корпоративное мошенничество» не используется; наиболее близко ему соответствует «мошенничество в сфере предпринимательской деятельности», которое Уголовный кодекс трактует как «мошенничество, связанное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности». Функция выявления, предупреждения, пресечения и раскрытия таких преступлений находится

в сфере юрисдикции отдела по борьбе с экономическими преступлениями МВД России.

В Великобритании расследованием преступлений, связанных с крупным мошенничеством или коррупцией, занимается подведомственное генеральному прокурору Бюро по расследованиям крупного мошенничества (*Serious Fraud Office, SFO*). При этом, данным Бюро корпоративное мошенничество (*corporate fraud*) определено как мошенничество, произошедшее в организации, включающее преднамеренный обман общественности, инвесторов или кредиторов, для получения финансовой выгоды преступным лицом или организацией. При этом, далее корпоративное мошенничество делится на:

(а) «освобождение от активов» (*asset stripping*) – передача активов одной организации в другую и ликвидация организации с долгами. Как правило, такое мошенничество применяется:

- с целью намеренного захвата активов организации и ее последующей ликвидации; либо
- «фениксизации» (*phoenixing*) – перемещения («спасения») активов из одной организации с ограниченной ответственностью в другую и ликвидации обязательств.

(б) мошеннические торговые операции (*fraudulent trading*) (подделка документов, и т.д.);

(в) наращивание цены акции (*share ramping*). Как правило, такие мошеннические действия сводятся к тому, чтобы вывести компанию на биржу и создать ложное представление о ее рентабельности, либо приобрести акции компании по низкой стоимости и создать слухи о ее покупке другой организацией либо ofercie со стороны мажоритарного акционера.

Например, 20 декабря 2012 г. на информационных лентах ведущих экономических изданий – «Ведомости» и «Коммерсант» появилась новость об обратном выкупе акций ОАО «АвтоВАЗ» по 24,17 руб. за акцию (существенно выше рынка), в результате чего за день акции этой компании выросли на 23%. Затем сообщение было опровергнуто, и рост сменился падением.

(г) публикация заведомо ложной информации (*publishing false information*).

Международный стандарт аудита 240 «Обязанность аудитора по рассмотрению рисков мошенничества при аудите финансовой отчетности» (ISA 240 – The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements) говорит, что искажения в финансовой отчетности могут возникнуть в результате мошенничества либо ошибки [1]. Определяющим фактором между двумя этими категориями является нали-

чие или отсутствия намерения. При этом, аудитор следует выделять только тот вид мошенничества, который вызывает существенные искажения в финансовой отчетности [2].

Далее стандарт 240 выделяет два вида намеренного искажения, уместные для аудита – искажения в результате мошенничества в финансовой отчетности (*fraudulent financial reporting*) и искажения, связанные с незаконным присвоением активов (*misappropriation of assets*). При этом, аудитор воздерживается от юридического определения подозреваемых им случаев мошенничества [3, 4].

Американским социологом и криминологом Д. Кресси в 1950 г. было проведено исследование

о причинах мошенничества. В течение 5 месяцев им было опрошено 250 преступников, которые злоупотребили доверием по вверенным им полномочиям. Кресси пришел к выводу, что для нарушения доверия необходимо наличие трех факторов – наличие скрываемой финансовой проблемы, возможности совершить обман и рационализации такого обмана преступником. Гипотеза Кресси получила название «треугольника мошенничества» (*fraud triangle*) и схематично изображается тремя сторонами: давлением или мотивом совершить мошенничество, возможностью такого совершения и рационализацию поступка (рис. 1):

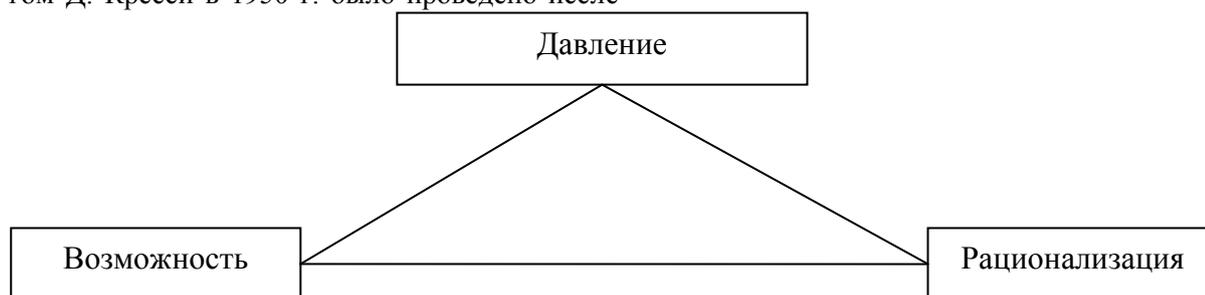


Рис. 1. Треугольник мошенничества

В 1953 г. Кресси опубликовал результаты своей работы в книге «Деньги других людей» (*Other People's Money*), при этом выделил шесть категорий скрываемых финансовых проблем:

- трудности с возвратом задолженности;
- личные неудачи;
- неконтролируемые деловые проблемы (экономический спад или инфляция);
- физическая изоляция;
- завышенные жизненные потребности, не отвечающие имеющимся средствам;
- несправедливые отношения внутри рабочего коллектива.

Гипотеза Кресси впоследствии легла в основу разработки аудиторских стандартов по проверке рисков мошенничества и систем внутрифирменного контроля. Так, Комиссия Тредвея (*Treadway Commission*), известная как Комитет организаций-спонсоров (*Committee of Sponsoring Organizations, COSO*) была сформирована в 80-х гг. XX в. в качестве ответа на мошенничества ссудо-сберегательных организаций. Комитет пришел к выводам, что лучшим способом бороться с мошенничеством является создание сильной системы внутреннего контроля, положения о котором вошли в американский стандарт по аудиту SAS 78, *Consideration of Internal Control in a Financial Statement Audit*. Принятый в начале XXI в. Закон Сарбанеса-Оксли (*Sarbanes-Oxley Act*) закрепил в практике США тре-

бование независимой оценки системы внутреннего контроля за аудиторами.

В 1998 г. COSO выпустила подробный отчет об исследовании фактов мошенничества в финансовой отчетности – *Landmark Study on Fraud in Financial Reporting*, в котором рассмотрела 200 случайно выбранных расследований по финансовому мошенничеству Комиссии по ценным бумагам и биржам США (*Securities and Exchange Commission, SEC*) – из 300 дел (то есть, выборка составила около двух третей), с 1987 по 1997 гг. COSO сравнила эти расследования по общим характеристикам и выявила следующее:

- большая часть мошеннических преступлений совершено в небольших организациях (к ним причислены компании с активами менее 100 млн. долл. США);
- советы директоров таких организаций состояли из инсайдеров и некомпетентных лиц;
- мошенниками в основном являлись лица из топ-менеджмента (высшего руководства) организации – 83% случаев;
- средний период «жизни» мошеннической операции составил 23,7 месяца;
- средняя сумма одного мошенничества составила 25 млн. долл. США;

COSO пришла к выводу о том, что небольшой размер организаций является причиной невозможности или нежелания внедрять целесообразную затратную систему внутреннего контроля,

в результате чего резко повышается риск возникновения мошенничества.

В США с 1988 г. действует Ассоциация сертифицированных специалистов по расследованию хищений (*Association of Certified Fraud Examiners, ACFE*), целью которой является подготовка профессиональных специалистов по предупреждению, обнаружению и предотвращению мошенничества. В своем ежегодном докладе *Report to the Nations (RTTN)* за 2012 г. Ассоциацией отмечены следующие факты:

- участники опросов оценили потери организации от мошенничества в размере 5% от годовой выручки ежегодно; с учетом оцениваемого мирового ВВП за 2011 г., это составляет 3,5 трлн. долл. США;

- средний убыток от одного факта мошенничества составляет 140 тыс. долл. США, при этом около 20% мошеннических действий привели к возникновению убытков в размере 1 млн. долл. США;

- средняя продолжительность «жизни» мошеннического факта составляет 18 месяцев до момента его обнаружения;

- в 43% случаев мошенничество выявлялось по доносительству, 15% - контролю со стороны руководства, 15% - службами внутреннего аудита, 7% - случайно, 5% - проверкой бухгалтерии, на прочие факты (изучение документации, внешний аудит, признание) приходились остальные 15%.

- корпоративное мошенничество (или мошенничество со стороны сотрудников, *occupational fraud*) представляет наиболее серьезную угрозу для малого бизнеса. По данным ACFE, чем меньше организация, тем больше размер ее среднего убытка, что объясняется тем, что такие организации внедряют меньше систем предупреждения мошенничества, что повышает ее восприимчивость к ним.

- наиболее часто мошенничество происходит в банковской и финансовой отраслях, правительственных и общественных учреждениях, производственном секторе;

- примерно в половине (49%) случаев убытки от мошенничества не возвращаются;

- средняя величина убытка от мошенничества варьируется от занимаемой должности: так, средний убыток, причиненный собственником/директорами составил в 2012 г. 573 000 \$, менеджерами различных уровней – 180 000\$, работниками – 60 000 \$;

- подавляющее большинство мошенничеств (77%) совершено работниками одного из шести следующих отделов: бухгалтерия, оперативный отдел, отдел продаж, администрация, отдел работы с клиентами и отдел закупок;

- в большинстве (87%) все мошенники совершали преступление впервые и за ними ранее не числились правонарушения;

- в 81% случаев мошенник проявлял себя посредством одного или нескольких индикаторов мошенничества: в 36% случаев – проживание сверх собственных средств; 27% - финансовые трудности; 19% - необычно тесная связь с покупателями и поставщиками; 18% - существенные проблемы системы внутреннего контроля.

В качестве выводов ACFE советовала:

- создавать «горячие линии» и подобные механизмы оповещения о мошенничестве для сотрудников с целью получения информации о фактах мошенничества внутри организации, поощрять работников за предоставление такой информации;

- внешний аудит не может быть надежным источником обнаружения мошенничества (посредством него было обнаружено лишь 3% мошеннических действий в 2012 г.), поэтому полагаться на него в первую очередь не следует. Вместе с тем, он исполняет важную функцию независимой проверки достоверности финансовой отчетности;

- необходимо проводить периодические тренинги работников по предотвращению мошенничества и др.

При этом, ACFE разработала модель классификации известных способов мошенничества (*дерево мошенничества, fraud tree*), выделив основные 49 мошеннических схем, сгруппированных в категории и подкатегории. Три основные категории – мошенничество в финансовой отчетности, хищение активов и коррупция.

Мошенничество в финансовой отчетности, как правило, совершается топ-менеджментом организации, происходит редко, но приносит наиболее крупные убытки. Как правило, мотивацией такого мошенничества является производные от цены акции организации на рынке ценных бумаг (премирование акциями, опционы и др.)

Хищение активов чаще всего осуществляется работниками организации по разнообразным схемам, происходит достаточно часто, однако наименее затратное по убыткам в расчете на единицу. Следовательно, такие виды мошенничества не существенны с точки зрения внешнего и внутреннего аудита, что повышает сложность их обнаружения.

Коррупция включает несколько схем, в т.ч. взятки и вымогательство, в которых работник организации связан с лицом, находящимся вне данной организации. Риск коррупции, таким об-

разом, повышается на фоне операций со связанными сторонами.

Характеристики каждой категории АСФЕ можно представить в виде следующей таблицы (табл. 2):

Таблица 2

Характеристики категорий мошенничества согласно классификации АСФЕ

Показатели	Мошенничество в финансовой отчетности	Хищение активов	Коррупция
Мошенник	Высшее руководство	Работники	Две стороны
Размер мошенничества	Крупное	Низкое	Среднее
Частота	Редкое	Частое	Среднее
Мотивация	Цена акции, поощрения	Личные проблемы	Конкуренция
Существенность	Высокая	Низкая	Зависит от обстоятельств
Выгодоприобретатели	Организация и мошенник	Мошенник	Мошенник
Размер организации	Крупная	Малая	Зависит от обстоятельств

При этом, АСФЕ советует нивелировать хищения активов (которые, как правило, несущественные и не являются полем для внимания со стороны внешнего аудита) путем внедрения функции внутреннего аудита и поддержания эффективной системы внутреннего контроля.

Мошенничество в финансовой отчетности, напротив, носит более существенный характер и потому находится в сфере проверки внешнего, независимого аудита. При этом основным мотивом будет являться завышение цены акции организации, на основе которой происходят поощрительные выплаты высшему руководству.

Коррупционные схемы могут быть обнаружены при аффилированных (связанных) отношениях и заключаются в откатах, манипуляциях с тендерами, подкупе.

Исследования крупнейших аудиторских корпораций *KPMG* и *PricewaterhouseCoppers* (*PwC*) по вопросам корпоративного мошенничества показали следующие результаты. *PwC* в ежегодном отчете «Опрос о глобальных экономических преступлениях» (*Global Economic Crime Survey*) за 2011 г. показала, что к трем крупным формам мошенничества – хищению активов (72% случаев за 2011 г.), мошенничеству в финансовой отчетности (24%) и коррупции (24%) – добавился четвертый – преступления в сфере информационных технологий или кибер-преступления (*cyber crime*) – 24% в 2011 г. *PwC* также сделала следующие выводы:

- проблема кибер-преступлений характерна как для развитых (выявлено 45% в США, 51% в Великобритании), так и для развивающихся стран;

- в основном такие преступления происходят в сфере связи (48%), страхования (48%), государственном секторе (46%), финансовых услугах (44%) и строительстве (31%);

- кибер-преступления характерны для крупных организаций с численностью сотрудников свыше 1 000 чел. (54%) и для средних организаций – 200-1000 чел. (29%);

- по сравнению с 2009 г., в 2011 г. доля мошенничества в финансовой отчетности упала с 38% до 24%, что может быть объяснено как внедрением системы внутреннего контроля, ужесточением наказания за такие преступления, экономическим ростом после кризисного 2009 г., и переклассификации части таких преступлений в кибер-мошенничество

PwC рекомендовала организациям учесть такие угрозы и создать защиту электронных устройств сотрудников, обладающих конфиденциальной коммерческой информацией [5].

KPMG в 2009 г. провела исследование по мошенничеству, *Fraud Survey*, в ходе которого было опрошено 204 лиц высшего руководства организаций с выручкой не менее 250 млн. долл. США. По результатам данного анализа было выявлено:

- 32% опрошенных предположили, что, как минимум, один вид мошенничества (хищение, мошенничество в отчетности или коррупция) увеличатся в течение года в организаций, в которой они работают;

- большинство интервьюируемых также выразили сомнение, что риски мошенничества упадут: 85% ответили, что количество случаев, скорее всего, останется на уровне прошлого года либо увеличатся (74%);

- наиболее серьезным ущербом от мошенничества считается репутационный (65%);

- основная причина мошенничества – неадекватная система внутреннего контроля и несоблюдение внутренних положений (66%);

KPMG предложила улучшить работу с персоналом, повысить эффективность системы внутреннего аудита, проводить мониторинг оценки риска мошенничества [6].

Рассмотрев основные виды классификации мошенничества в нормативных актах, теоретической литературе и практических опросах крупных организаций, мы выявили принципы, на которых строится мошенничество, его мотивы, виды, характеристики субъекта и объекта мошенничества с целью создания в дальнейшем

системы предупреждения, выявления и разработки методики внутреннего контроля и бухгалтерской диагностики корпоративного мошенничества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Слабинская И.А., Ровенских В.А. Бухгалтерская (финансовая) отчетность. М.: Изд. Дашков и К^о, 2013. 364 с.
2. Слабинский Д.В. Основные группы манипуляций в финансовой отчетности. // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2011. № 1. С. 109-111.
3. Ткаченко Ю.А. Внутренний контроль в обеспечении экономической безопасности предприятия / Актуальные проблемы экономического развития: сб. докл. Конф. Междунар. науч.-практ. конф. // Белгород: Изд-во БГТУ, 2012. – Ч. 2. – С. 204-208.
4. Слабинская И.А., Ткаченко Ю.А., Внутренний контроль как необходимый элемент системы экономической безопасности / Проблемы и перспективы развития предприятий в условиях международной экономической интеграции: сб. материалов конф. IV Междунар. науч.-практ. конф. – Харьков, 22-23 ноября 2012 г. // Харьковский национальный университет строительства и архитектуры. – Харьков: Изд-во ХНУБА, 2012. – Ч. 1. – С. 71-73.
5. Global Economic Crime Survey, PricewaterhouseCoopers, 2011.
6. Fraud Survey, KPMG, 2009.