

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2023, Том 15, № s1 / 2023, Vol. 15, Iss. s1 <https://esj.today/issue-s1-2023.html>

URL статьи: <https://esj.today/PDF/22FAVN123.pdf>

Ссылка для цитирования этой статьи:

Кравченко, А. К. Выявление рисков корпоративного мошенничества в технологической отрасли /

А. К. Кравченко // Вестник евразийской науки. — 2023. — Т. 15. — № s1. — URL:

<https://esj.today/PDF/22FAVN123.pdf>

For citation:

Kravchenko A.K. Identifying corporate fraud risks in the technology industry. *The Eurasian Scientific Journal*. 2023; 15(s1): 22FAVN123. Available at: <https://esj.today/PDF/22FAVN123.pdf>. (In Russ., abstract in Eng.)

УДК 338

Кравченко Александр Кириллович

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия

Факультет «Информационных технологий и анализа больших данных»

E-mail: kraoff@mail.ru

Научный руководитель: **Боташева Людмила Хасановна**

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия

Доцент Департамента экономической безопасности и управления рисками

Кандидат экономических наук, доцент

Выявление рисков корпоративного мошенничества в технологической отрасли

Аннотация. Автор данной публикации проводит анализ и структурирование данных, касающихся проявлений рисков корпоративного мошенничества в организациях технологической отрасли. Автором были изучены факторы, влияющие на потенциальное возникновение рисков технологической отрасли, что позволяет формировать детальную картину проявлений рисков, в том числе корпоративного мошенничества. Одним из самых частых проявлений корпоративного мошенничества в технологической отрасли являются незаконные «вознаграждения», которые выступают в качестве необходимого условия в процессе регулирования бизнес-процессов и базиса межличностных отношений в процессе совершения мошеннических действий. Автором была описана классификация «вознаграждений» в зависимости от их размера и формы проявления, благодаря чему повышается эффективность изучения данного явления в структуре корпоративного мошенничества. Кроме того, были изучены ключевые схемы «вознаграждений», включающие в себя этапы реализации недобросовестных мотивов и противоправных действий субъектов. Самым потенциально негативным проявлением корпоративного мошенничества в любой организации, а не только в технологической отрасли, является искажение финансовой отчетности. В качестве примера организации, в отношении которой могло произойти искажение финансовой отчетности, был выбрано ООО «Современные Технологии». Автором были применены актуальные в настоящее время и высокоточные модели М. Бениша и Роксас, которые с вероятностями 68 % и 70 % соответственно позволяют сделать вывод о наличии или отсутствии фактов фальсификации отчетности организации. В заключении были определены выводы по результатам анализа ООО «Современные Технологии», а также подведены итоги относительно проявления корпоративного мошенничества в технологической отрасли.

Ключевые слова: технологическая отрасль; экономическая безопасность; корпоративное мошенничество; анализ отчетности; риски корпоративного мошенничества; коррупция

Введение

Необходимо отметить актуальность данной работы, которая заключается в большом количестве рисков, которые могут оказывать негативное влияние на деятельность организаций в технологической отрасли. В свою очередь данные риски становятся катализатором возникновения широкого спектра проблем, тормозящих и сковывающих высокотехнологичные организации. Высокие показатели незаконных «вознаграждений» и прочих видов корпоративного мошенничества становятся причиной стагнации не только отдельных организаций, но и всей высокотехнологической отрасли.

В качестве цели научной работы выступает анализ ключевых рисков корпоративного мошенничества в технологической отрасли. В соответствии с целью был выделен ряд задач:

1. Определить факторы рисков в технологической сфере.
2. Выявить ключевые проблемы в технологической сфере.
3. Рассмотреть механизм корпоративного мошенничества на примере ООО «Современные Технологии».
4. Сформировать выводы относительно последствий корпоративного мошенничества для организации.

Объектом данного исследования выступает корпоративное мошенничество в технологической сфере. Предметом — ключевые риски корпоративного мошенничества в технологической отрасли.

1. Материалы и методы

Факторы риска фрода от английского — Fraud risk factors — события или условия, которые приводят к возникновению побуждения или давления, направленных на совершение мошеннических действий, или к возможности их совершения.

Для более полной характеристики рассматриваемого вопроса были изучены работы Е.И. Ефремовой [1], Д.Д. Нактостик [2], Ю.А. Ефименко [3] в области корпоративного мошенничества. Также стоит отметить работы Н.Ю. Извариной [4], Н.С. Филатова [5], Е.В. Шадринной [6], А.И. Пияльцева [7], А.А. Шаманиной [8], отражающие различные аспекты корпоративного мошенничества в организациях.

Среди методов, примененных в исследовании, стоит отметить наблюдение, сравнение, измерение, а также абстрагирование. Кроме того, были использованы методы синтеза и анализа.

2. Результаты и обсуждение

Согласно статистике, в крупных компаниях наиболее высок риск «откатов» или, иными словами, незаконных «вознаграждений» — 31 % [9]. Сама по себе культура корпоративных отношений подразумевает под собой возникновение «вознаграждений» из-за распространенности договорных отношений на разных этапах бизнес-процессов. Именно поэтому большинство бизнес-процессов в технологической отрасли можно считать критическими.

Существование «вознаграждений» в высокотехнологической сфере является большой проблемой, ведь значительная часть средств уходит в никуда, также, это пагубно влияет на качество работ. Любители «вознаграждений», желая побольше забрать к себе в карман,

экономят на материалах, заказывают некачественные услуги, в результате чего производится низко ликвидная и некачественная продукция. Такие формы коррупционных проявлений стимулируют должностное лицо, оно заинтересовано быстрее повернуть сделку. Тем не менее, это считается злоупотреблением служебным положением в личных целях и уголовно наказуемо.

Чаще всего «вознаграждение» происходит по такой системе — заказчик услуг или материалов платит завышенную цену, разницу ему потом отдаёт поставщик. В производстве довольно часто встречаются «вознаграждение» на материалах, причём они бывают как мелкими, так и крупными, в государственных масштабах. Их можно разделить на такие схемы:

1. Завышается цена на товар или услугу.
2. Указывается большее количество.
3. В счёте или смете могут находиться ненужные товары или услуги [10].

Чаще служебному лицу возвращается часть денег, но иногда «вознаграждение» может выражаться материалами или услугами. Например, чиновник способствовал тому, что технологическую компанию выбрали как поставщика программного продукта, однако основания для передачи таких прав никто не проверил. Такие факты напрямую свидетельствуют о коррупционном проявлении, подкупе, кумовстве и иным противоправным деяниям, таким как:

1. Лоббирование — содействие в продвижении определённой организации при формировании технической документации и последующем определении поставщика в рамках ключевых «тендерных» нормативно-правовых актов — 44 и 223 федерального законов.
2. Подкуп — если говорить о мошеннических действиях с мелкими суммами, то их чаще всего осуществляют частные предприниматели и посредники, которые занимаются перепродажей программного обеспечения. Они могут становиться посредниками для реализации небольших закупок до шестисот тысяч рублей.
3. Сговор — взаимодействие группы лиц, направленное на совершение ряда противоправных мошеннических действий в одной или нескольких купных организаций, действия которых приносят весомый ущерб государственной либо коммерческой структуре. Зачастую такие действия оформляются официально, деньги переводятся из государственного бюджета, либо со счета коммерческой структуры безналичным способом.
4. «Вознаграждение» за бухгалтерский документ — когда технологической организации нужно обналить часть денег, тогда нужен бухгалтерский документ, подтверждающий расходы. За предоставление таких документов он платит «вознаграждение».
5. Стороны — схема незаконного «вознаграждения», может проводиться не только между двумя сторонами, но и между несколькими. Особенно часто это происходит в высокотехнологической сфере, где есть чиновник, подрядчик и поставщик. Одной из сторон «вознаграждения» может являться банк, заведомо или нет.
6. Закупка материалов — материально техническое снабжение (умудряются даже продавать материалы прямо с объекта).

7. Страхование — юристы, например страхование объекта у определенной страховой организации с последующим получением «вознаграждения».
8. Кредит — «вознаграждение» при лизинге или закупке техники в кредит, в том числе просто для завлечения оборотных средств.

Все вышеперечисленные формы проявления противоправных коррупционных действий со схемами «вознаграждений» можно разделить на следующие типы:

1. Классический: с использованием наличных или безналичных денежных средств.
2. Альтернативный: может быть, в виде любых материальных средств.
3. Нематериальная форма: должности, звания.

По статистике 78 % сотрудников на должности специалиста по материально-техническому снабжению прибегают в своей практике к «вознаграждениям», зачастую это связано со сложившимися правилами в технологической отрасли [11]. Поэтому «вознаграждения» в производстве могут расти по цепочке в арифметической прогрессии, что в итоге скажется на качестве выполняемых работ. Любой сотрудник в организации на своей должности может получать «вознаграждения». Их величина зависит от:

1. Положения который сотрудник занимает и степени его влияния.
2. Величины бюджета, которой он распоряжается.

При расследовании нельзя делать поспешных выводов, потому что сотрудник, ставящий свою подпись в договоре, не всегда является получателем «вознаграждения». Зачастую получают вознаграждение лица, которые готовят эти документы. Также выстраиваются различные коррупционные цепочки чтобы было трудно отследить лицо, получившее «вознаграждение».

В структуре корпоративного мошенничества можно выделить три основные группы (рис. 1).



Рисунок 1. Основные группы корпоративного мошенничества [12]

Самым комплексным видом корпоративного мошенничества, как правило, является искажение финансовой отчетности. Сложнее всего раскрыть именно этот вид корпоративного мошенничества, потому что доказательная база носит субъективный характер.

Искажение финансовой отчетности стоит на последнем месте по распространенности, но имеет наибольший ущерб.

В производстве 17,4 % организаций прибегает к мошенничеству с финансовой отчетностью. Этот показатель является самым большим в отраслевой структуре [13].

Для выявления фальсификации отчетности необходимо обратиться к моделям М. Бениша и Роксас. Эти модели с вероятностями 68 % и 70 % позволяют сделать вывод о наличии или отсутствии фактов фальсификации отчетности. М. Бениш в своей работе определил граничные значения, которые могут свидетельствовать о фальсификации финансовой отчетности в организации. Его модель для американских компаний выглядит данным образом [14]:

$$M\text{-score} = -4,84 + 0,920DSRI + 0,528GMI + 0,404AQI + 0,892SGI + 0,115DEPI - 0,172SGAI + 4,679TATA - 0,327LVGI.$$

Впоследствии его исследование было усовершенствовано Роксас. Из модели были убраны несущественные индексы, после чего модель стала выглядеть следующим образом:

$$M\text{-score} = -6,065 + 0,823DSRI + 0,906GMI + 0,593AQI + 0,717SGI + 0,107DEPI.$$

Если значения M-score в модели М. Бениша для американских компаний превышают -2,22, а в модели Роксас -2,76, то исследуемая организация с большой вероятностью фальсифицирует отчетность.

После адаптации, произведенной для Российских компаний модели приобрели следующий вид:

Модель Бениша:

$$M\text{-score} = -4,84 + 0,920DSRI + 0,528GMI + 0,404AQI + 0,892SGI - 0,172SGAI - 0,327LVGI.$$

Модель Роксас:

$$M\text{-score} = -6,065 + 0,823DSRI + 0,906GMI + 0,593AQI + 0,717SGI.$$

Из модели убрали два фактора индекс амортизации (DEPI) и показателя, характеризующего начисление к активам (TATA) [15].

Данное изменение не сказывается на качестве модели, потому что в российской практике нет случаев, связанных с искажением суммы начисленной амортизации.

Таблица 1

Расчет пороговых значений сводных индексов M-score [16]

M-score		Пороговые значения сводных индексов M-score
M-score Бениша	-2,314774802	< -1,802
M-score Роксас	-2,807309078	< -2,146

После исключения из базовых моделей двух показателей пороговые значения M-score в моделях Бениша и Роксас для американских компаний составили -2,424 и -2,965 соответственно.

Для российских компаний тот же самый индекс составил -1,802 для модели Бениша и -2,146 для модели Роксас.

После адаптации был произведен расчет для технологической организации ООО «Современные Технологии». Итоговые значения M-score приведены ниже (табл. 1).

Проанализировав данные отчетности ООО «Современные Технологии» по системе Бениша и Роксаса, можно увидеть, что большинство показателей организации не соответствует

нормативным значениям. Значение M-Score указывает на то, что вероятность манипуляций с отчетностью велика из-за превышения порогового значения.

Заключение

В результате изучения вопроса был получен материал, анализ которого позволил заключить, что риски корпоративного мошенничества обусловлены определенными факторами, которые, в свою очередь, также требуют внимания. Большое количество рисков, связанных с деятельностью технологических организаций, является элементом, стимулирующим появление негативных явлений, в числе которых особое место занимает корпоративное мошенничество. Корпоративное мошенничество может принимать большое количество формаций, самой популярной из которых являются «откаты» или иными словами «вознаграждения». Трудность выявления таких способов мошеннических действий в технологической сфере обусловлена тем, что они сильно варьируются в зависимости от размера и схемы применения. При этом наиболее пагубное воздействие на деятельность организаций высокотехнологической отрасли оказывает искажение финансовой отчетности. На примере ООО «Современные Технологии» были использованы модели М. Бениша и Роксас. В результате применения указанных моделей было выявлено, что большое количество нестыковок в отчетности организации позволяет с высокой вероятностью утверждать о наличии фактов корпоративного мошенничества. Данные модели могут быть использованы для анализа других организаций в отрасли и последующего формирования представлений об общем положении экономической безопасности в технологической сфере.

ЛИТЕРАТУРА

1. Ефремова Е.И., Зацаринная Е.И. Контроль корпоративного мошенничества // Управленческий учет. — 2021. — № 9–1. — С. 152–157.
2. Накостик Д.Д. Влияние корпоративного мошенничества на финансовое состояние российских компаний: проблемы и пути решения // Вектор экономики. — 2020. — № 2. — С. 34–34.
3. Ефименко Ю.А. Форензик как метод противодействия корпоративному мошенничеству // От синергии знаний к синергии бизнеса. — 2021. — С. 51–54.
4. Изварина Н.Ю., Климина К.В., Рябова Я.А. Корпоративные мошенничества как угроза экономической безопасности хозяйствующих субъектов // Экономика и бизнес: теория и практика. — 2020. — № 10–1. — С. 145–147.
5. Филатов Н.С. Корпоративное мошенничество. К вопросу о возрастающих угрозах и их корнях // Экономика и управление: проблемы, решения. — 2020. — Т. 2. — № 3. — С. 126–139.
6. Шадрин Е.В. Корпоративное мошенничество: схемы и способы их предотвращения // Цифровая экономика: перспективы аудита и безопасности бизнеса. — 2020. — С. 310–315.
7. Пияльцев А.И. Корпоративное мошенничество как угроза экономической безопасности организации // Молодежь и системная модернизация страны. — 2020. — С. 16–19.

8. Шаманина А.А. Методы выявления признаков корпоративного мошенничества // Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения. — 2021. — С. 538–542.
9. Смирнова, Е.Е. Методы выявления корпоративного мошенничества на ранних этапах / Е.Е. Смирнова // Вестник евразийской науки. — 2022. — Т. 14. — № 6. — URL: <https://esj.today/PDF/80ECVN622.pdf>.
10. Гладков Д.О., Бадма-Халгаев Р.К., Сеницын Е.С. Современные тенденции в области противодействия корпоративному мошенничеству // Вестник Евразийской науки. — 2023 № s1. — URL: <https://esj.today/PDF/15FAVN123.pdf> DOI: 10.15862/15FAVN123.
11. Сеницын Е.С. Анализ реализации механизмов противодействия корпоративному мошенничеству на примере «X5 Retail Group» // Вестник Евразийской науки. — 2022 № 5. — URL: <https://esj.today/PDF/46ECVN522.pdf>.
12. Чернякова М.М. Инновационные риски в цифровой экономике // Вестник Евразийской науки. — 2018 № 6. — URL: <https://esj.today/PDF/16ECVN618.pdf>.
13. Страхов И.А. Осуществление контроля за соблюдением правил внутреннего контроля противодействия легализации доходов, полученных преступным путем, и финансированию терроризма // Вестник Евразийской науки. — 2021 № 6. — URL: <https://esj.today/PDF/74ECVN621.pdf>.
14. Kong D. et al. Politically connected independent directors and corporate fraud in China // Accounting & Finance. — 2019. — Т. 58. — № 5. — P. 1347–1383.
15. Yin C. et al. Do corporate frauds distort suppliers' investment decisions? // Journal of Business Ethics. — 2021. — Т. 172. — № 1. — P. 115–132.
16. Lai T., Lei A.C.H., Song F.M. The impact of corporate fraud on director-interlocked firms: Evidence from bank loans // Journal of Business Finance & Accounting. — 2019. — Т. 46. — № 1-2. — P. 32–67.

Kravchenko Alexander Kirillovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: kraoff@mail.ru

Academic adviser: **Botasheva Lyudmila Khasanovna**

Financial University under the Government of the Russian Federation, Moscow, Russia

Identifying corporate fraud risks in the technology industry

Abstract. The author of this publication conducts analysis and structuring of data regarding the manifestations of corporate fraud risks in organizations in the technology industry. The author studied the factors influencing the potential occurrence of risks in the technology industry, which makes it possible to form a detailed picture of the manifestations of risks, including corporate fraud. One of the most frequent manifestations of corporate fraud in the technology industry are illegal "rewards" that act as a necessary condition in the process of regulating business processes and the basis of interpersonal relationships in the process of committing fraudulent activities. The author described the classification of "rewards" depending on their size and form of manifestation, which increases the efficiency of studying this phenomenon in the structure of corporate fraud. In addition, key schemes of "rewards" were studied, including the stages of implementation of unscrupulous motives and illegal actions of subjects. The most potentially negative manifestation of corporate fraud in any organization, not just in the technology industry, is the misrepresentation of financial statements. LLC "Modern Technologies" was chosen as an example of an organization in respect of which a financial statement could be misrepresented. The author applied the currently relevant and high-precision models of M. Benish and Roxas, which, with a probability of 68 % and 70 %, respectively, allow us to conclude that there are or are no facts of falsification of the organization's reporting. In conclusion, conclusions were drawn from the results of the analysis of Modern Technologies LLC, as well as summed up regarding the manifestation of corporate fraud in the technology industry.

Keywords: technology industry; economic security; corporate fraud; reporting analysis; risks of corporate fraud; corruption