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/65FAVN123.pdf

Ссылка для цитирования этой статьи:
Алексеев, Л. В. Применение информационных технологий в области выявления и противодействия корпоративному мошенничеству / Л. В. Алексеев // Вестник евразийской науки. — 2023. — Т. 15. — № s1. — URL: https://esj.today/PDF/65FAVN123.pdf

For citation:
Alekseev L.V. Application of information technologies in the field of detection and counteraction to corporate fraud. *The Eurasian Scientific Journal*. 2023; 15(s1): 65FAVN123. Available at: https://esj.today/PDF/65FAVN123.pdf. (In Russ., abstract in Eng.)

УДК 338

Алексеев Леонид Владимирович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Информационных технологий и анализа больших данных»
E-mail: leonidalekseevv@mail.ru

Научный руководитель: **Прасолов Валерий Иванович**
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Доцент Департамента экономической безопасности и управления рисками
Кандидат политических наук
E-mail: VIPrasolov@fa.ru

Применение информационных технологий в области выявления и противодействия корпоративному мошенничеству

Аннотация. Целью данной научной статьи является определение тенденций в области выявления и противодействия корпоративному мошенничеству с применением информационных технологий. В рамках исследования были определены ключевые подходы к определению корпоративного мошенничества, которые сводятся к тому, что данное явление проявляется в противоправных действиях со стороны сотрудников организации благодаря занимаемой позиции в организации и наличии корыстных мотивов. Информационные технологии и системы обработки и хранения данных позволяют защищать конфиденциальную информацию и предотвращать несанкционированный доступ к ним. С помощью ИТ-систем можно контролировать и анализировать финансовые операции, что способствует выявлению и предотвращению экономических преступлений. В работе проведен анализ возникновения корпоративного мошенничества, в частности была рассмотрена концепция «случайных мошенников» и «хищников». Автором были изучены основные виды мошенничества, а именно коррупция, мошенничество с отчетностью и присвоение активов. Важность рассмотрения корпоративного мошенничества и противодействия ему обоснована статистикой по количеству корпоративных правонарушений и статистикой по сумме убытков от корпоративного мошенничества на один случай. По результатам анализа статистических данных автором было выдвинуто предположение о том, что эпизодические отдельные меры не способны эффективно обеспечивать экономическую безопасность хозяйствующего субъекта в части противодействия корпоративному мошенничеству. Для противодействия мошенничеству применяются различные виды мероприятий, которые разделены на превентивные и проверочные, которые могут быть стандартными и активными. Профилактические действия часто не воспринимаются как эффективные, однако они могут значительно снизить вероятность наступления фактов

корпоративного мошенничества в организациях. Одним из наиболее пагубных видов корпоративного мошенничества является искажение финансовой отчетности организации. В работе было рассмотрено многообразие причин возникновения данного вида корпоративного мошенничества, а также описаны основные схемы реализации преступных действий с финансовой отчетностью.

Ключевые слова: информационные технологии; корпоративное мошенничество; экономика организации; анализ рисков; антикризисное управление; профилактика мошенничества; внутренний контроль

Введение

Актуальность выбранной темы обоснована, с одной стороны, высоким уровнем корпоративного мошенничества в компаниях, с другой стороны, низким уровнем информационной защиты и профилактики корпоративного мошенничества. Для борьбы с мошенничеством можно использовать различные информационные технологии. Например, можно разрабатывать алгоритмы машинного обучения, которые будут анализировать данные и выявлять потенциальных мошенников. Также можно использовать блокчейн-технологии для создания безопасных баз данных и систем идентификации. Еще одним способом борьбы с мошенничеством является использование системы двухфакторной аутентификации при входе в онлайн-сервисы. Корпоративное мошенничество возникает независимо от размера организации или от области ее деятельности, ключевой причиной появления данного негативного явления выступает человеческий фактор, заключающийся в корыстном умысле.

Целью данной работы является определение тенденций в области выявления и противодействия корпоративному мошенничеству.

Задачи исследования:

1. Изучить основные аспекты проявления корпоративного мошенничества.
2. Определить виды корпоративного мошенничества.
3. Рассмотреть базовые методы выявления фактов корпоративного мошенничества.
4. Выявить ключевые методы противодействия корпоративному мошенничеству с применением информационных технологий.

Объектом данного исследования выступает корпоративное мошенничество.

Предметом — тенденции в области выявления и противодействия корпоративному мошенничеству.

1. Материалы и методы

Система противодействия корпоративному мошенничеству является важным объектом научных исследований, среди ученый в области оценки противодействия корпоративному мошенничеству выделяются Тамбовцева Т.А. [1], Голованова Н.А. [2], Лысенко Е.А. [3], Суин И.П. [4], Снимщикова И.В. [5]. Последствия корпоративного мошенничества рассматривали Сидельникова В.И. [6], Шумилин П.Е. [7], Санникова И.Н. [8], Лабынцев Н.Т. [9].

При написании работы использовались общенаучные методы познания, такие как системный поход, методы анализа и синтеза. Были широко использованы индуктивный и дедуктивный методы, а также сравнительный анализ.

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

2. Результаты и обсуждение

В настоящее время корпоративное мошенничество является одной из наиболее актуальных проблем в бизнес-сфере. Для борьбы с этим явлением широко используются информационные технологии.

Одним из наиболее эффективных методов выявления корпоративных мошенников является использование систем аналитики данных. Эти системы позволяют автоматически анализировать большие объемы информации, выделять аномалии и выявлять потенциально опасные операции.

Также для борьбы с корпоративным мошенничеством часто используются системы контроля доступа к информации. Они позволяют ограничить доступ к конфиденциальной информации только уполномоченным сотрудникам, что уменьшает риски утечки информации и злоупотребления ей.

Кроме того, существуют специализированные программные продукты для выявления мошеннических операций. Они используются для мониторинга операций сотрудников и выявления подозрительных действий. Применение информационных технологий в области выявления и противодействия корпоративному мошенничеству является эффективным и необходимым инструментом в современном бизнесе.

Мошеннические действия становятся все более распространенными в нашем современном обществе, и информационные технологии могут быть полезны в борьбе с этим явлением. Существует множество способов, которые могут помочь в противодействии мошенничеству, используя информационные технологии.

Один из таких способов — это использование специальных программных средств, которые позволяют отслеживать и анализировать транзакции, происходящие в системе. Банки, онлайн-магазины и другие компании используют такие средства для того, чтобы выявлять мошеннические действия и принимать меры по предотвращению их совершения.

Другой способ — это использование защищенных каналов связи и шифрования данных. Конфиденциальность данных и безопасность транзакций являются важными аспектами в борьбе с мошенничеством. Использование защищенных каналов связи и шифрования данных может помочь снизить уровень риска мошеннических действий.

Еще один способ — это использование двухэтапной аутентификации. Это процесс, при котором пользователь должен ввести не только свой пароль, но и дополнительный код, который отправляется на его мобильный телефон или другое устройство. Это может помочь убедиться в том, что только авторизованный пользователь имеет доступ к аккаунту и снизить уровень риска мошенничества.

Также важным является повышение осведомленности пользователей. Обучение пользователей тому, как распознавать мошеннические схемы, может помочь снизить уровень риска мошенничества. Это может быть достигнуто путем проведения обучающих курсов, семинаров и других мероприятий.

Следует отметить, что помимо технических решений, важным фактором в борьбе с корпоративным мошенничеством является обучение сотрудников. Регулярные тренинги и обучающие программы помогают повысить осведомленность сотрудников о возможных угрозах и методах их предотвращения.

Одним из дополнительных методов противодействия корпоративному мошенничеству является использование систем видеонаблюдения. Они могут помочь в выявлении подозрительных действий и повысить ощущение ответственности у сотрудников. Также

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

эффективным инструментом являются системы автоматического оповещения о сомнительных операциях, которые могут свидетельствовать о корпоративном мошенничестве.

В настоящее время актуальны проблемы разработки направлений по эффективному выявлению случаев мошенничества, а также анализ условий, которые способствуют противодействию мошенничества и др. Но прежде, чем приступить к механизмам выявления рисков корпоративного мошенничества и способов их минимизации, необходимо разобраться с самим определением корпоративного мошенничества.

На данный момент в России не существует общепризнанного определения корпоративного мошенничества. В первую очередь, это связанно с тем, что настоящее направление в российской науке и практике изучено достаточно мало. При этом корпоративное мошенничество может принимать большое количество форм, что также усложняет процесс определения.

В соответствии с мировой практикой противодействия мошенничеству указанные злоупотребления, согласно отечественного подхода могут включаться в расширительное понятие Fraud.

Можно выделить 2 подхода:

- отечественный (согласно определению мошенничества в Уголовном кодексе РФ);
- расширенный (ИСА 240).

В данной работе корпоративное мошенничество рассматривается в разрезе понятия «риск корпоративного мошенничества» со всеми присущими риску характеристиками (неопределенность, альтернативность и т. д.). «Риск — это потенциальная возможность возникновения управляемого события в условиях неопределенности среды осуществления экономической деятельности, которая поддается количественной и качественной оценке». Таким образом, риск корпоративного мошенничества — это потенциальная возможность возникновения корпоративного мошенничества в условиях неопределенности экономической среды. Этот риск можно оценить и просчитать. Также ему присуща альтернативность и неразрывная связь с человеческим фактором.

Для понимания природы корпоративного мошенничества необходимо рассмотреть треугольник мошенничества, который представляет собой модель развития данного явления в зависимости от психологии сотрудников. Есть два вида сотрудников, а именно «случайные мошенники» — совершающие мошенничества в первый раз и «хищники» — патологические мошенники, совершающие нарушающие раз за разом. Эволюция развития корпоративного мошенничества представлена ниже (рис. 1).

«Хищники» намного более опасны для организаций, однако их намного меньше, чем тех, кто совершает незаконные действия под воздействием внешних обстоятельств. Из-за этого возникает сложная ситуация, когда, с одной стороны, есть определенная часть опасных корпоративных преступников, которые совершают крупные мошеннические действия, однако их численность очень невелика, с другой стороны, большинство из оставшихся преступников могли стать ими под стечением обстоятельств, при этом на них возможно воздействовать при помощи профилактических и превентивных действий.

Таким образом, можно сделать вывод, что корпоративное мошенничество стало настоящей проблемой для российских предприятий. Но масштаб бедствия можно ограничить, если вовремя обращать внимание на его признаки.

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

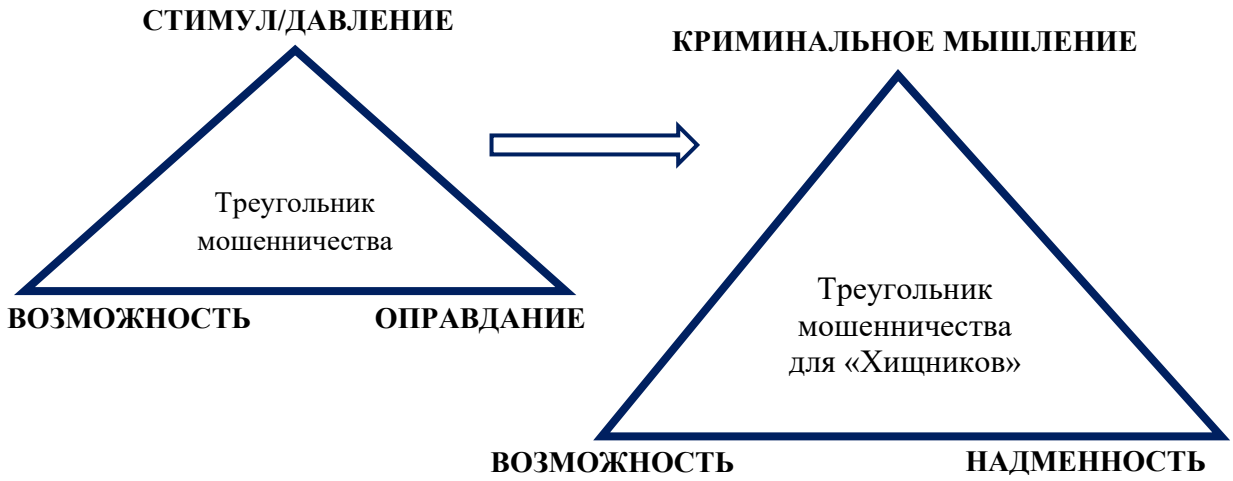

Рисунок 1. *Эволюция треугольника мошенничества [11]*

Выделяется 3 основных вида корпоративного мошенничества:

- коррупция — схемы, в которых сотрудник компании (наиболее часто — менеджер) вопреки интересам её использует свое служебное положение для влияния на финансово-хозяйственные операции с целью получения нелегальной выгоды, например «оплата» входа на рынок, «откаты»;
- мошенничество с отчетностью — схемы, которые позволяют фальсифицировать финансовую отчетность в целях ее улучшения (например, обман инвестора), так и ухудшения (например, налоговые преступления);
- присвоение (хищение) активов — схемы, приводящие к присвоению активов компании, например сокрытие доходов, выставление фиктивных счетов.

Необходимо рассмотреть статистику совершения корпоративного мошенничества по видам за предыдущий год (рис. 2).

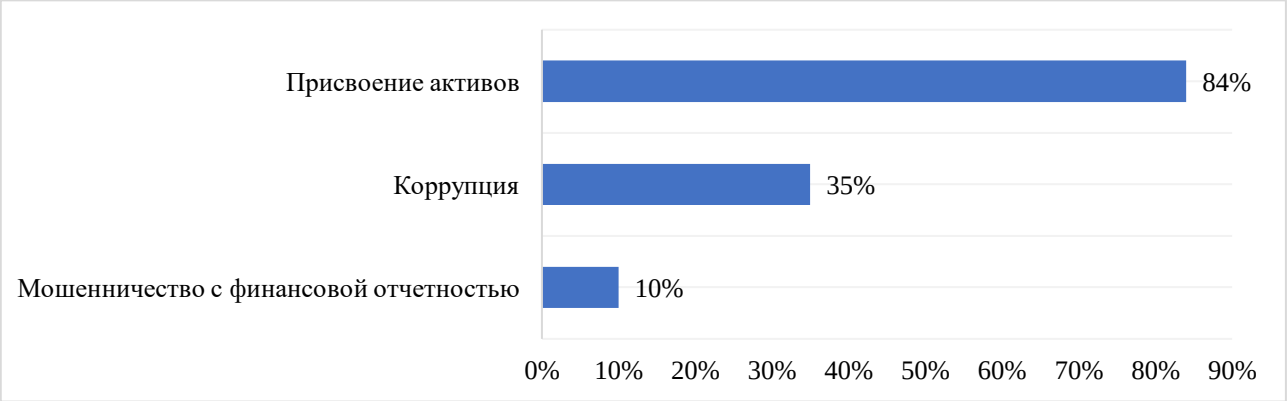

Рисунок 2. *Количество случаев злоупотреблений, 2022 г. [12]*

Исходя из указанных данных, стоит отметить, что присвоение активов является наиболее распространенным видом корпоративного мошенничества, намного опережая и коррупцию, и мошенничество с финансовой отчетностью. Однако необходимо рассмотреть ущерб от указанных видов корпоративного мошенничества.

Далее представлена статистика по сумме убытков от корпоративного мошенничества на один случай (рис. 3).

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

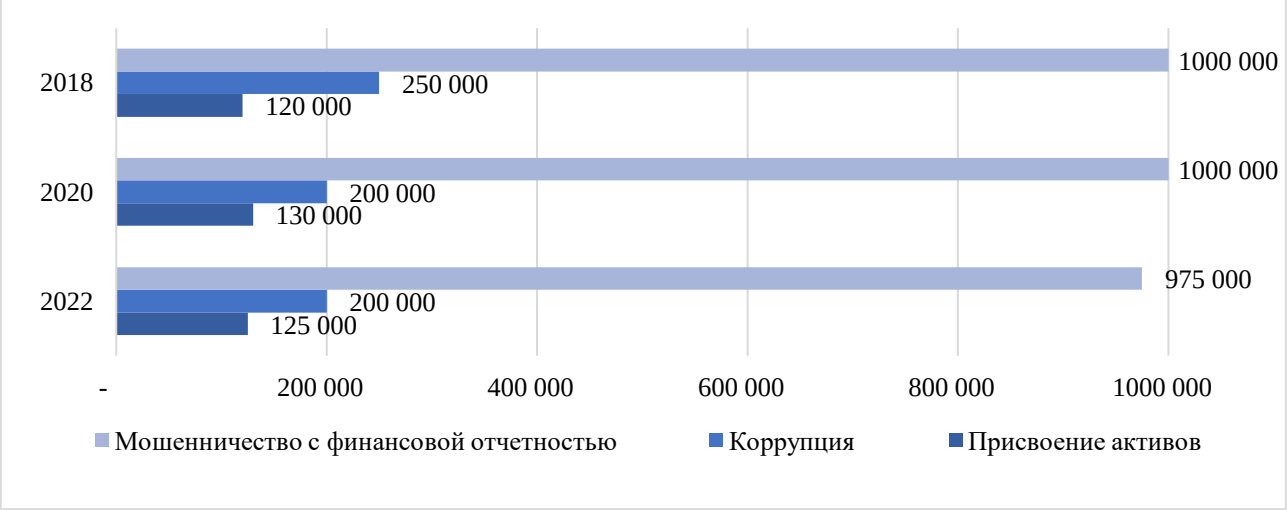

Рисунок 3. *Сумма убытков от злоупотреблений, 2018–2022 гг. [13]*

Из выше представленных данных очевиден тот факт, что сумма убытков от злоупотреблений обратно пропорциональна количеству злоупотреблений. Таким образом, мошенничество с финансовой отчетностью при небольшом количестве случаев наносит компаниям наибольший ущерб. Это также связано с тем, что присвоение активов является самым простым методом злоупотребления полномочиями, так как для него не всегда требуются специальные навыки.

Однако будут рассматриваться и другие виды корпоративного мошенничества, так как, во-первых, все они имеют схожие признаки и способы минимизации/предотвращения, во-вторых, зачастую факты мошенничества оставляют «следы», которые имеют непосредственное влияние на финансовую отчётность.

Определив понятие корпоративного мошенничества и его основные виды, важно рассмотреть механизмы противодействия данному противоправному деянию.

Согласно исследованию KPMG по России и странам СНГ более 90 % случаев мошеннических действий со стороны работников компании в 2022 году связаны либо с полным отсутствием системы внутреннего контроля, либо с её неразвитостью, наличием недостатков, то есть наличием возможности («треугольник мошенничества»).

Данная статистика подтверждает тот факт, что эпизодические отдельные меры, не способны эффективно обеспечивать экономическую безопасность хозяйствующего субъекта в части противодействия корпоративному мошенничеству.

Многие российские компании становятся легкими мишенями для «внутренних» мошенников из-за слабости своего внутреннего контроля в сочетании с географически распределенной структурой и периодических реорганизаций. Непрозрачность и неэффективность также являются причинами корпоративного мошенничества, которое будет уменьшаться по мере роста прозрачности и эффективности. Кроме того, система противодействия мошенничеству должна исходить от высшего уровня руководства.

Ниже представлены основные мероприятия для минимизации рисков корпоративного мошенничества, сформулированные Хмыровым С.В., членом Совета и экспертом Российского отделения ACFE, которые он разделил на 2 типа:

1. Превентивные (профилактика).
2. Проверочные:

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

2.1 стандартные проверочные мероприятия;

2.2 активные проверочные мероприятия.

Подобные меры применимы для борьбы со всеми видами корпоративного мошенничества.

Исходя из принципа поступательного проведения проверочных мероприятий «от простых к сложным», стандартные проверочные мероприятия проводятся в первую очередь, а мероприятия из арсенала активных проверочных мероприятий применяются в последующем, по мере необходимости в наращивании усилий.

Под стандартными проверочными мероприятиями подразумеваются простые проверочные мероприятия, не требующие сверх усилий, финансовых затрат, привлечения сторонних специалистов и ресурсов. В основном стандартные мероприятия связаны с проверкой и анализом документов и сотрудников.

Активные проверочные мероприятия, во-первых, подразумевают некие более сложные действия, требующие больших усилий, большей изобретательности и приложения интеллекта. Во-вторых, активные проверочные мероприятия проводятся тогда, когда не удалось достичь нужного результата меньшими усилиями, т. е. проведением стандартных проверочных мероприятий. В-третьих, на исполнение большинства из активных проверочных мероприятий требуется либо привлечение сторонних специалистов, либо использование технических средств, программного обеспечения, что обусловлено финансовыми расходами. В-четвертых, активные проверочные мероприятия, как правило, требуют предварительного согласования с вышестоящим руководством. Примером может выступать проверка на полиграфе.

Выше были указаны общие методы противодействия корпоративному мошенничеству. Рассматривая специфику мошенничества с финансовой отчетностью, необходимо учитывать более высокие интеллектуальные способности мошенников (в основном они занимают высокое положение в компании), побудившие к действиям причины и преследуемые цели, типы и методы фальсификаций, и особые методы выявления.

Необходимо рассмотреть ключевые типы фальсификации отчетности, которые применяются в большинстве случаев корпоративного мошенничества (рис. 4).

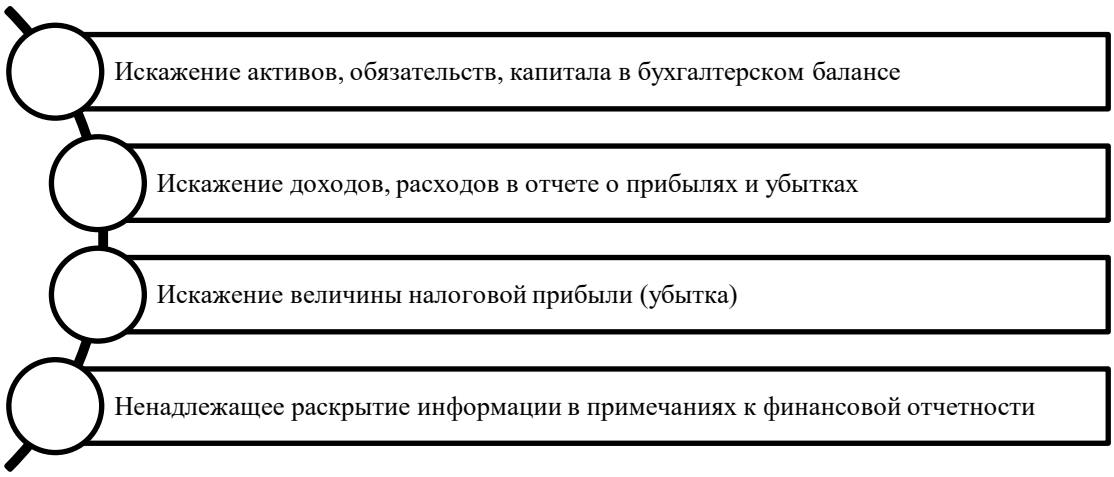

Рисунок 4. *Основные типы фальсификации отчетности [13]*

Причинами/целями фальсификации финансовой отчетности могут быть следующие:

1. Соответствие показателям, необходимым для осуществления деятельности (например, для получения кредита).

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

2. Соответствие рыночным прогнозным и/или целевым показателям.
3. Демонстрация инвестиционной привлекательности.
4. Влияние на принятия решений инвесторами/акционерами.
5. Получение конкурентных преимуществ.
6. Сокрытие фактов коррупции руководством организации для реализации поставленных собственниками целей (например, получение лицензий).
7. Сокрытие факта хищения активов организации.
8. Противодействие «недружественному» поглощению.
9. Создание «запаса эффективности» в период смены руководства.
10. Обоснование поддержания и увеличения тарифов на товары (работы, услуги).
11. Снижение налогового бремени на организацию и т. д.

В современном мире корпоративное мошенничество является одной из самых распространенных проблем, которая может серьезно повлиять на финансовую устойчивость организации. Для предотвращения этой проблемы внедрение систем противодействия корпоративному мошенничеству является необходимым шагом.

Системы противодействия корпоративному мошенничеству позволяют своевременно обнаруживать и предотвращать несанкционированные действия внутри организации. Они также помогают улучшить финансовую устойчивость, защитить бренд и репутацию компании, а также повысить доверие со стороны клиентов и инвесторов.

Системы противодействия корпоративному мошенничеству включают в себя несколько ключевых элементов, таких как мониторинг финансовых операций, проведение аудитов, обучение персонала и установление этических стандартов. Каждый из этих элементов имеет свою роль в обеспечении эффективной работы системы.

Внедрение систем противодействия корпоративному мошенничеству является необходимым шагом для защиты финансовой устойчивости организации и ее репутации. Эти системы помогают предотвратить несанкционированные действия внутри компании и улучшить доверие со стороны клиентов и инвесторов. Поэтому, каждая организация должна обеспечить соответствующую защиту от корпоративного мошенничества для своей жизнеспособности и процветания.

Заключение

В заключение использование информационных технологий может быть полезно в противодействии мошенническим действиям. Программные средства, защищенные каналы связи, шифрование данных и повышение осведомленности пользователей — это лишь некоторые из способов, которые могут помочь снизить риск мошенничества.

Подводя итог, следует отметить, что корпоративное мошенничество представляет собой комплексное явление, которое заключается в злоупотреблении положением сотрудника в организации. Оно может быть выражено в виде хищения активов, коррупции или искажения финансовой отчетности. Каждый из указанных видов корпоративного мошенничества несет опасность для организации. Хищение является наиболее распространенным видом, однако самый негативный эффект проявляется от искажения финансовой отчетности организации. В работе были выявлены тенденции в области выявления и способов минимизации основных рисков корпоративного мошенничества: представлены признаки мошенничества, составлен

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

перечень профилактических и проверочных мероприятий. Профилактические мероприятия способны оказать воздействие на «случайных» мошенников, которые в основном действуют из-за стечения обстоятельств. Проверочные мероприятия помогают выявить «хищников», то есть немногочисленную группу лиц, целенаправленно совершающих незаконные действия в организации.

ЛИТЕРАТУРА

1. Тамбовцева Т.А. Корпоративное мошенничество: способы осуществления и меры предотвращения // Учетно-аналитическое и правовое обеспечение экономической безопасности организации. — 2022. — С. 162–166.
2. Голованова Н.А. Корпоративная ответственность: трансформация уголовно-правового регулирования // Журнал зарубежного законодательства и сравнительного правоведения. — 2022. — Т. 18. — № 2. — С. 82–96.
3. Лысенко Е.А. Механизмы противодействия корпоративному мошенничеству // Международные стандарты учета и аудита: практика применения в условиях цифровой экономики. — 2022. — С. 267–270.
4. Суин И.П., Кашурников С.Н. Совершенствование системы противодействия корпоративному мошенничеству в компаниях аудиторского сектора // Финансовый бизнес. — 2022. — № 5(227). — С. 67–76.
5. Снимщикова И.В., Мельников А.Б., Чугаева Ю.А. Антикоррупционная политика как фактор противодействия корпоративному мошенничеству в нефтяных компаниях // Вестник Северо-Кавказского федерального университета. — 2020. — № 1. — С. 151–157.
6. Сидельникова В.И. Экономические преступления и оффшорный бизнес // Молодежь и научно-технический прогресс. — 2022. — С. 180–183.
7. Шумилин П.Е., Нежижимова П.С. Влияние корпоративного мошенничества на бизнес и экономическую безопасность страны в целом // Современные проблемы экономической безопасности, учета и права в Российской Федерации. — 2019. — Т. 2. — С. 5–13.
8. Санникова И.Н., Степанова А.Н. Ключевые аспекты корпоративного мошенничества // Проблемы устойчивого развития в отраслевом и региональном аспекте. — 2020. — С. 297–301.
9. Лабынцев Н.Т., Горбатко Н.А. Методы обнаружения мошенничества в процессе аудита // Актуальные направления развития учета, анализа, аудита и статистики в отечественной и зарубежной практике. — 2021. — С. 190–196.
10. Чернобаева О.В., Коваленко А.А., Алексеев Р.В. Противодействие внутреннему мошенничеству // Управление и экономическая безопасность: страна, регион, предприятие. — 2019. — С. 46–50.
11. Тё О.Ю. Форензик-влияние корпоративного мошенничества // Международные стандарты учета и аудита: практика применения в условиях цифровой экономики. — 2022. — С. 426–428.
12. Rostami V., Rezaei L. Corporate governance and fraudulent financial reporting // Journal of Financial Crime. — 2022. — Т. 29. — № 3. — С. 1009–1026.
13. Caplan D.H., Dutta S.K., Marcinko D.J. Unmasking the fraud at Toshiba // Issues in Accounting Education. — 2019. — Т. 34. — № 3. — С. 41–57.

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Alekseev Leonid Vladimirovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: leonidalekseevv@mail.ru

Academic adviser: **Prasolov Valeriy Ivanovich**
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: VIPrasolov@fa.ru

Application of information technologies in the field of detection and counteraction to corporate fraud

Abstract. The purpose of this scientific article is to identify trends in the field of detection and counteraction to corporate fraud using information technology. As part of the study, key approaches to the definition of corporate fraud were identified, which boil down to the fact that this phenomenon manifests itself in illegal actions on the part of employees of the organization due to their position in the organization and the presence of selfish motives. Information technology and data processing and storage systems allow you to protect confidential information and prevent unauthorized access to it. With the help of IT systems, financial transactions can be monitored and analyzed, which contributes to the detection and prevention of economic crimes. The paper analyzes the emergence of corporate fraud, in particular, the concept of "random scammers" and "predators" was considered. The author studied the main types of fraud, namely corruption, reporting fraud and misappropriation of assets. The importance of considering corporate fraud and counteracting it is justified by statistics on the number of corporate offenses and statistics on the amount of losses from corporate fraud per case. Based on the results of the analysis of statistical data, the author suggested that episodic individual measures are not able to effectively ensure the economic security of an economic entity in terms of combating corporate fraud. To combat fraud, various types of measures are used, which are divided into preventive and verification, which can be standard and active. Preventive actions are often not perceived as effective, but they can significantly reduce the likelihood of corporate fraud occurring in organizations. One of the most pernicious types of corporate fraud is the misrepresentation of an organization's financial statements. The paper examined the variety of causes of this type of corporate fraud, and also described the main schemes for the implementation of criminal acts with financial reporting.

Keywords: information technology; corporate fraud; organizational economics; risk analysis; crisis management; fraud prevention; internal control

65FAVN123
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com