

Скрытое хищение активов как один из видов корпоративного мошенничества

Кочурова Ольга Сергеевна, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; факультет безопасности и таможни (Санкт-Петербург, Российская Федерация);

студентка 5-го курса специалитета;

e-mail: okochurova-19@edu.ranepa.ru.

Научный руководитель:

Алексеев Антон Александрович, Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; кафедра безопасности (Санкт-Петербург, Российская Федерация);

старший преподаватель;

e-mail: alekseev-aa@ranepa.ru.

Аннотация

Корпоративное мошенничество — это крайне опасное явление, с которым сталкивается, как правило, больше половины компаний, работающих в России и странах СНГ. Это явление сопровождается не только финансовыми потерями, но и утратой деловых связей, ухудшением репутации, снижением развития компании и потерей конкурентоспособности. Согласно исследованию, проведенному Ассоциацией сертифицированных экспертов по борьбе с мошенничеством, самым распространенным видом корпоративного мошенничества, который встречается в 86% случаев, является незаконное присвоение активов.

В рамках данной статьи рассмотрены особенности скрытого хищения активов как одного из видов корпоративного мошенничества. В работе приведены актуальные данные статистики по наиболее распространенным видам корпоративного мошенничества, способам совершения сотрудниками мошеннических действий и причинам, обуславливающим этот факт.

Одной из основных угроз развития бизнеса является человеческий фактор, поэтому в статье были не только проанализированы причины противоправных действий, но также рассмотрены уровни мошенничества, совершаемого персоналом, и категории похитителей, которые способны посягать на безопасность компании. Имея на балансе активы, использование которых обеспечивает организации успешную деятельность, ее руководитель, а также сотрудники службы безопасности обязаны решать вопросы, связанные с предупреждением мошеннических действий со стороны персонала.

Снизить потенциальные возможности совершения мошеннических действий, установить приемлемый контроль за действиями сотрудников и сформировать корпоративную культуру позволит разработка перечня мер выявления, профилактики и противодействия хищению активов. С этой целью в заключительной части работы автором приведен перечень конкретных превентивных мер, направленных на защиту имущественного комплекса. Принятие конкретных действий по предупреждению корпоративного мошенничества является принципиальной задачей, решаемой в ходе построения и ведения бизнеса. Грамотная система защиты активов организации будет способствовать поддержанию доверия клиентов, партнеров и самих работников компании, что является важным элементом ее функционирования.

Ключевые слова: корпоративное мошенничество, незаконное присвоение активов, внутренние хищения, уровни мошенничества, категории похитителей, внутренний контроль, методы предупреждения.

Concealed Embezzlement of Assets as a Type of Corporate Fraud

Olga S. Kochurova, North-Western Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation; Department of Security (Saint Petersburg, Russian Federation)

5th-year student;

e-mail: okochurova-19@edu.ranepa.ru.

Academic Supervisor:

Anton A. Alekseev, North-Western Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation; Faculty of International Relations and Politics (Saint Petersburg, Russian Federation)

Senior Lecturer of the Department;

e-mail: alekseev-aa@ranepa.ru.

Abstract

The corporate fraud is an extremely dangerous phenomenon, typically faced by more than half of the companies operating in Russia and CIS countries. This phenomenon is accompanied not only by financial losses, but also by the loss of business contacts, deterioration of reputation, decline in company development and competitive disadvantage. According to the research conducted by the Association of Certified Fraud Examiners, the most prevalent type of corporate fraud, occurring in 86% of cases, is misappropriation of assets.

Within the framework of this article, the author examines some specific features of hidden asset misappropriation as one of the types of corporate fraud. The paper provides up-to-date statistics on the most common types of corporate fraud, the ways employees commit fraud and the reasons behind this fact.

One of the main threats to business development is the human factor, and, therefore, the paper analyzes not only the causes of illegal operations, but also the levels of fraud committed by staff and the categories of embezzlers who are in the position to infringe on the security of the company. With assets on the balance sheet, the use of which ensures the organization's operational success, its CEO and Security Service employees must address the issues related to the prevention of fraudulent actions on the part of the personnel.

The development of a set of measures to detect, prevent and counteract the theft of assets will contribute to reducing the potential for fraudulent actions, establishing acceptable control over the employees' conduct, and building a corporate culture. For this purpose, the final section of the paper presents a list of specific preventive measures aimed at protecting the property complex. Taking specific measures to prevent corporate fraud is a fundamental task to be addressed in the course of building and running a business. A competent system of protection of the organization's assets will contribute to maintaining the trust of customers, partners and employees, which is an important element of its functioning.

Keywords: corporate fraud, misappropriation of assets, internal embezzlement, levels of fraud, categories of embezzlers, internal control, prevention methods.

ВВЕДЕНИЕ

Организация работы любого предприятия — это весьма сложный и многозадачный процесс, который связан с решением широкого круга вопросов: организационных, правовых, технических, кадровых. При этом особое значение приобретают вопросы обеспечения безопасности и сохранности активов. Наиболее распространенным и крайне негативным противоправным явлением для большинства организаций является корпоративное мошенничество. Его опасность состоит, прежде всего, в прямой потере активов, ущербе, причиненном имиджу предприятия, утрате деловых связей, снижении эффективности деятельности. При этом существует довольно широкий перечень противоправных действий, которые можно отнести к корпоративному мошенничеству. Одним из таких примеров может являться скрытое хищение активов.

Целью статьи является определение особенностей хищения активов как одного из видов корпоративного мошенничества.

Задачи:

- 1) выявить причины, обуславливающие возможность совершать внутренние хищения;
- 2) проанализировать уровни мошенничества, совершаемого персоналом;
- 3) определить основные категории похитителей в организации;
- 4) обозначить способы контроля, выявления, предупреждения и нейтрализации мошеннических действий со стороны персонала.

1. МАТЕРИАЛЫ И МЕТОДЫ

При написании статьи была использована отечественная литература, посвященная вопросам в области противодействия корпоративному мошенничеству, отчеты, опубликованные Ассоциацией сертифицированных экспертов по борьбе с мошенничеством, исследования, проведенные консалтинговой компанией KPMG.

Кроме того, использовались общенаучные методы познания, такие, как системный подход, статистические методы обработки массивов информации, методы анализа и синтеза, что позволило более полно изучить исследуемый вопрос.

2. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

В законодательстве Российской Федерации четко не закреплён термин «корпоративное мошенничество». На практике он включает в себя, как правило, махинации, совершаемые с целью либо хищения активов, либо причинения вреда без присвоения собственности. В совместной работе Д. Л. Скипина, Ю. С. Сахно, Л. А. Баденова и М. О. Кузнецова приведено следующее определение данного термина: «Корпоративное мошенничество — это умышленное, продуманное неправомерное действие сотрудников компании, связанное непосредственно с их должностным положением и обязанностями, направленное на получение личной выгоды и удовлетворения собственных интересов, вопреки интересам компании, путем воздействия на финансово-хозяйственную деятельность, хищение ее активов, несанкционированное использование преимуществ на рынке» [8].

В силу проблематичности выявления и сложности формирования доказательной базы мошеннические действия способны не только привести к негативным финансовым последствиям, но и сказаться на репутации и имидже фирмы.

Виды корпоративного мошенничества включают в себя:

- 1) скрытое хищение активов;
- 2) присвоение и растрата чужого имущества;

- 3) нанесение материального ущерба посредством обмана или халатного отношения;
- 4) иные виды, такие, как открытое хищение активов, вымогательство с применением шантажа и угроз.

Согласно отчету Occupational Fraud 2022: a Report to the Nations, опубликованному Ассоциацией сертифицированных экспертов по борьбе с мошенничеством (ACFE), наиболее распространенным видом корпоративного мошенничества, который встречается в 86% случаев, является незаконное присвоение активов¹.

Активы — это имущество организации, которым она имеет право распоряжаться в ходе своей деятельности. «Под имуществом организации понимаются основные средства, нематериальные активы, финансовые вложения, производственные запасы, готовая продукция, товары, прочие запасы, денежные средства и прочие финансовые активы»².

Обратимся к высказыванию «гуру» менеджмента Питера Ф. Друкера: «Главная задача бизнеса — это выживание, а главный принцип деловой экономики — не получение максимальной прибыли, а предотвращение потерь». Потери в отношении имущества — это введенные в оборот и утраченные по разным причинам товарно-материальные ценности. Они состоят из недостач, брака и естественной убыли.

Незаконное присвоение активов как один из видов корпоративного мошенничества и причин потерь основано на махинациях с товарно-материальными ценностями и денежными средствами. Частая причина возникновения потерь — это мошеннические действия персонала.

Для того чтобы в этом убедиться, обратимся к данным, представленным консалтинговой компанией KPMG, которая ежегодно исследует экономические преступления внутри компании, а также отделы и органы, которые наиболее подвержены мошенническим действиям (рис. 1).



Рис. 1

¹ Association of Certified Fraud Examiners Occupational fraud 2022: a Report to the Nations / Association of Certified Fraud Examiners [Электронный ресурс]. — URL: <https://legacy.acfe.com/report-to-the-nations/2022/> (дата обращения: 13.11.2023).

² Приказ Минфина РФ от 13.06.1995 № 49 (ред. от 08.11.2010) «Об утверждении Методических указаний по инвентаризации имущества и финансовых обязательств».

Согласно статистике, наибольшее число мошеннических действий, связанных с хищением активов, совершают работники низового звена, например, кассиры, продавцы, грузчики, работники склада. На их деятельность приходится около 50% выявленных противоправных действий. Этим лицам зачастую важно одновременно украсть и использовать похищенное в личных целях.

Примерно на одном уровне находятся сотрудники отдела закупок, бухгалтерии и финансового отдела — 22% и 20% соответственно. Предметом их посягательства, как правило, являются денежные средства. Они совершают мошеннические действия вследствие возложенных на них широких полномочий.

Также обратимся к исследованию, проведенному аналитиками «РТК-Солар» (рис. 2).



Рис. 2. Какое мошенничество допускали сотрудники

Самыми популярными способами мошенничества являются мошенничество с продажами (17%) и хищение денег, товарно-материальных ценностей и других активов (15%). В первую очередь это может быть связано с простотой реализации в силу наличия доступа к материальным ценностям и денежным средствам в процессе трудовой деятельности. На мошенничество при осуществлении закупок приходится 14%.

«Парадокс заключается в том, что одним из главных ресурсов развития бизнеса, так и основной угрозой для него, является человеческий фактор» [6, с. 3608].

Среди причин, обуславливающих совершение преступных действий внутри организации, выделяют три основных мотива, которые также условно называют углами «треугольника мошенничества». «Каждый человек способен совершить мошенничество, нужно только, чтобы он оказался в соответствующей ситуации» [4, с. 388].

Обозначим основные причины согласно теории «треугольника мошенничества»:

- 1) давление внешних обстоятельств, которые человек не может преодолеть. Чаще всего такие обстоятельства связаны с финансовым неблагополучием;
- 2) возможность на протяжении какого-то времени скрывать факты мошенничества или последствий мошеннических действий;
- 3) оправдание совершаемых преступных действий трудной жизненной ситуацией.

Согласно исследованию Deloitte Forensic «Корпоративное мошенничество», более 60% мошеннических действий в компании стали возможными из-за отсутствия, недостаточности или неэффективности мер контроля, которые не позволяют своевременно выявить недобросовестные действия сотрудников.

Другие причины, обуславливающие возможность совершать внутренние хищения, как правило, представлены:

- 1) слабой производственной дисциплиной или ее отсутствием;
- 2) максимально предоставленными полномочиями;
- 3) равнодушием со стороны отдельных руководителей;
- 4) иными причинами, например, некомпетентностью должностных лиц, возможностью предоставления искаженной информации.

При этом существует несколько уровней мошенничества, совершаемого персоналом.

Первый уровень — это мелкие разовые хищения. Может, они и не наносят существенного вреда экономической безопасности, но тем не менее способствуют возникновению подозрений в коллективе. Особенность подобного рода хищений заключается в том, что происходят они без особой предварительной подготовки. При этом чаще всего сотрудник будет полностью убежден в своей безнаказанности за содеянное, а значит, существует опасность, что подобные хищения в скором времени приобретут систематический характер.

Второй уровень — это систематические хищения, или, по-другому, «надбавка к зарплате». Если говорить о денежных средствах как материально-вещественном элементе имущества компании, расхищаются чаще всего незначительные на фоне общего денежного потока суммы. Отличие от первого уровня — в наличии экономических мотивов и определенной подготовки. Именно такие хищения создают угрозу для организации, поскольку носят систематический характер.

Третий уровень можно условно назвать «внутреннее предпринимательство». Как правило, «внутренних предпринимателей» не бывает много, однако их отличительная особенность в том, что «это наиболее опасный уровень злоупотреблений, возникающий там, где работникам предоставляется возможность распоряжаться крупными суммами и самостоятельно принимать крупные финансовые решения» [1, с. 101].

Выделяется несколько категорий похитителей.

Первая категория — самая опасная — это «профессионалы». Такие сотрудники устраиваются на работу с целью совершения хищений. Мошеннические действия являются их источником дохода.

Вторая категория — так называемые «жертвы соблазна». Кражи такими сотрудниками совершаются в тот момент, когда они видят, что можно взять или присвоить что-то без особого риска обнаружения в результате недостаточного контроля над их деятельностью. Это могут быть продавцы или кладовщики, тайно присваивающие понравившийся им товар, сотрудники отдела продаж, пользующиеся периодически деньгами клиента, полученными за поставленный товар.

Третья категория — «зависимые», это лица, страдающие kleptomанией, наркозависимые, а также любители острых ощущений.

Перед каждым руководителем стоит задача определить и проанализировать причины, способствующие совершению преступных деяний в организации, разработать ряд

эффективных мер выявления, профилактики и противодействия хищениям активов. Для устранения возможности совершения внутрикорпоративного мошенничества необходимо создание эффективной системы внутреннего контроля.

«Внутренний контроль — это процесс, который направлен на достижение основных целей сохранности имущества организации. Он является результатом работы руководства по планированию, организации и мониторингу всей деятельности компании» [7, с. 1]. «Эффективная система внутреннего контроля помогает снизить потенциальные возможности к совершению мошеннических действий, устанавливает приемлемый контроль за действиями сотрудников организации, сформировать приемлемую корпоративную культуру» [3, с. 507].

Определим перечень методов, направленных на предупреждение мошеннических действий.

Информационные методы предполагают создание баз данных по имуществу, ведение учета и инвентаризации, использование электронных систем мониторинга и сопоставления данных.

Самой распространенной процедурой является ревизия. Она позволит проверить соответствие реального наличия товаров документальному, выявить недостачу или излишки, привести в порядок учетные данные.

Одна из возможных составляющих ревизии — инвентаризация — проверка субъектом контроля материальных активов фактического наличия и сохранности имущества и сверка полученных данных с документами учета материальных ценностей.

Порядок проведения включает в себя следующие обязательные этапы:

- 1) созыв комиссии и утверждение ответственных лиц;
- 2) издание приказа о проведении инвентаризации;
- 3) определение остатков продукции по учетной информации;
- 4) проведение инвентаризации и отражение полученных данных в специальных описях и актах;
- 5) фиксация итогов проверки в ведомости учета результатов.

По методу проведения различают сплошную и выборочную инвентаризацию. Разница состоит в том, что сплошная инвентаризация предполагает полную проверку имущества по всем местам хранения, а выборочная — конкретную категорию товара или определенное место хранения. Правильно проведенная инвентаризация — это один из основных «способов фактического контроля по сохранению имущественных ценностей и средств» [5].

На практике многие торговые организации используют контрольное вложение или закладку позиции в заказе. Контрольно-ревизионный отдел совместно со службой безопасности намеренно вкладывает в заказ 2–3 единицы товара, не учтенного в документации. Цель данной процедуры — проверить клиентов организации и своих же сотрудников на добросовестность.

Осмотр и обследование имущества также являются процедурами метода контроля сохранности имущества. Их цель — непосредственное изучение специалистом определенных объектов.

Технические методы позволяют обнаруживать и предотвращать незаконные действия, совершаемые как сотрудниками, так и внешними силами. Сегодня системы видеонаблюдения можно встретить практически везде: в банках, на складах, в супермаркетах. С одной стороны, применение камер видеонаблюдения носит профилактический характер, с другой — камеры видеонаблюдения могут помочь установить факты противоправных действий. Система видеонаблюдения способна значительно повысить эффективность обеспечения сохранности имущества.

К техническим методам относится использование DLP-систем. Этот программный продукт позволяет выявить случаи корпоративного мошенничества, утечки конфиденциальной информации, а также дает возможность вести постоянный мониторинг качества работы сотрудников. «DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения блокируется» [2, с. 93].

При комплексном обеспечении безопасности особое значение имеет организация пропускного режима. Основная задача — пресечение несанкционированного проникновения посторонних лиц на территорию и контроль выноса материальных ценностей. Также установка охранной сигнализации отвечает аналогичным задачам и позволяет отслеживать движение внутри охраняемого помещения.

Важным «кирпичиком», влияющим на сохранность имущества в системе комплексной безопасности, является взаимодействие с людьми. Оно включает в себя «выстраивание системы ценностей, корпоративной культуры, создание объективной системы мотивации руководства и работников, в рамках которой оценивается вклад сотрудника и определяется вознаграждение за него, но при этом подразумевается наказание за действия, наносящие урон компании» [9].

За счет методов, направленных на предупреждение мошеннических действий, организация предотвращает потери, связанные с утратой, кражей активов. Система обеспечения сохранности имущества организует непрерывность бизнес-процессов. Утечки данных, инциденты безопасности и другие происшествия способны нанести урон репутации организации. Защита имущества способствует поддержанию доверия клиентов, партнеров, самих работников компании.

Таким образом, широкий перечень методов позволит предупредить несанкционированный доступ персонала к материальным ценностям, организовать контроль и учет движения активов, выявить и нейтрализовать лиц, нарушающих режим доступа и посягающих на сохранность имущественного комплекса.

ЗАКЛЮЧЕНИЕ

В заключение хотелось бы отметить, что одним из самых распространенных видов корпоративного мошенничества является незаконное присвоение имущества.

В статье были рассмотрены причины совершения хищений в организации, уровни мошеннических действий и категории субъектов, совершающих противоправные действия.

Также были описаны меры для защиты имущества. Важно исключить возможность возникновения факторов, способствующих хищению активов, свести к минимуму потери от действий внутренних и внешних субъектов, создать такую систему безопасности, которая обеспечит сохранность имущественного комплекса. При этом стоит отметить, что полученная экономия окупит затраты на создание такой системы.

Благодаря контролю доступа к помещениям, установке камер видеонаблюдения и контрольно-пропускного режима, организации правильной системы хранения имущества появляется возможность защитить бизнес от прямых финансовых потерь, сохранить доверие клиентов и партнеров, предотвратить нанесение ущерба репутации фирмы.

Также необходимо отметить, что предупредить незаконное присвоение имущества — это важная и актуальная задача для каждого предприятия, вызванная необходимостью снижения финансово-экономических потерь, обеспечения стабильности и роста бизнеса.

Литература

1. Аусилова Н. М. Применение DLP-систем как инструмента обеспечения информационной безопасности // Наука и реальность. — 2023. — № 1(13). — С. 93–96.
2. Галеева З. Корпоративная крепость: как выстроить систему противодействия мошенничеству в компании [Электронный ресурс] // Forbes. — URL: <https://blogs.forbes.ru/2023/07/20/korporativnaja-krepost-kak-vystroit-sistemu-protivodejstvija-moshennichestvu-v-kompanii/?ysclid=lqkxt716ti179647395> (дата обращения: 25.12.2023).
3. Маслова В. А., Филимонцева Е. М. Роль инвентаризации в сохранности собственности экономического субъекта // Научный лидер. — 2021. — № 31(33). — URL: <https://scilead.ru/article/774-rol-inventarizatsii-v-sokhrannosti-sobstvennos>.
4. Панкратьев В. В. Методическое пособие по корпоративной безопасности. — URL: metodicheskoe_posobie_po_korporativnoj_bezopasnosti_pankratev_29122023.doc (live.com) (дата обращения: 07.03.2024).
5. Раджабов Р. Ш. Роль внутреннего контроля в профилактике и выявлении корпоративного мошенничества // Экономика: вчера, сегодня, завтра. — 2022. — Т. 12. — № 3. — С. 502–509.
6. Скипин Д. Л., Быстрова А. Н., Кутырева Е. В., Труфанова К. Н. Корпоративное мошенничество: сущность, риски и влияние на экономическую безопасность бизнеса // Российское предпринимательство. — 2017. — № 22. — URL: <https://cyberleninka.ru/article/n/korporativnoe-moshennichestvo-suschnost-riski-i-vliyanie-na-ekonomicheskuyu-bezopasnost-biznesa> (дата обращения: 03.02.2024).
7. Скипин Д. Л., Сахно Ю. С., Баденова Л. А., Кузнецов М. О. Корпоративное мошенничество: понятие, сущность, риски, влияние на экономическую безопасность // Экономические отношения. — 2019. — Т. 9. — № 3. — С. 2299–2310.
8. Трушина Т. С., Нестеренко А. В. Экономическая важность создания и функционирования системы внутреннего контроля в целях обеспечения сохранности имущества организации и законности совершаемых операций // Концепт. — 2015. — Т. 13. — С. 1611–1615.
9. Швецов Д. Р. Финансовые мошенники и как с ними бороться? // Экономика и социум. — 2019. — № 2(57). — URL: <https://cyberleninka.ru/article/n/finansovye-moshenniki-i-kak-s-nimi-borotsya> (дата обращения: 15.02.2024).

Для цитирования:

Кочурова О. С. Скрытое хищение активов как один из видов корпоративного мошенничества // Новизна. Эксперимент. Традиции (Н.Экс.Т). — 2024. — Т. 10. — № 1 (25). — С. 58–66.