DOI: 10.14451/1.210.159

АНАЛИЗ МЕЖДУНАРОДНОЙ ПРАКТИКИ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

© 2022 **Прасолов Валерий Иванович**
кандидат политических наук, доцент Департамента экономической безопасности и анализа рисков
Финансовый университет при Правительстве Российской Федерации,
Россия, Москва

В статье рассмотрена специфика мошенничества на промышленных предприятиях, анализ динамики совершенных в мире случаев мошенничества, а также способов противодействия ему в практической деятельности компаний. Актуальность исследования определяется устойчивым ростом данного вида противоправной деятельности на предприятиях. Предложенные автором способы минимизации ущерба в результате реализации основных схем мошенничества, могут использоваться в исследуемой сфере экономической деятельности.

***Ключевые слова**: мошенничество, промышленные предприятия, производственные процессы, риски, экономическая безопасность.*

Промышленное предприятие является комплексом средств производства, осуществляющим технологический процесс изготовления определённой продукции. С правовой стороны, это хозяйствующий субъект, который создан в установленном законом порядке для ведения хозяйственной деятельности, производства товаров и оказания услуг, удовлетворения общественных потребностей и получение прибыли.

Одной из основных функций производственного предприятия считаем изготовление продукции, её продажа и поставка, обслуживание потребителей после продажи, обеспечение процесса производства, организация труда персонала, управленческие процессы и обязанности, соблюдение действующего законодательства и др. При этом предприятия отличаются друг от друга наличием характерных особенностей: разных типов выпускаемой продукции; масштабами производства; местом размещения; структурой организации и прочими характеристиками.

Значительная часть вопросов, связанных с организацией, планированием и управлением имеют типовые алгоритмы, применимые к отдельным группам предприятий.

Деятельность промышленных предприятий основывается на реализации четырёх типов бизнес-процессов.

Во-первых, процесс управления — организация управления за деятельностью хозяйствующего субъекта: планирование, контроль за постановкой и реализацией целей, анализ и внедрение необходимых изменений, координация отдельных элементов.

Во-вторых, производственные процессы, которые отвечают за создание продукта, его стоимость и качество. Эти процессы можно определить, как главные в рамках производственной деятельности организации. Таких основных процессов на предприятии не более 20. (снабжение, производство, контроль качества, складское хранение, реализация).

В-третьих, стратегические процессы, определяющие направления и тенденции развития основных процессов в зависимости от целей развития предприятия, (маркетинг, разработка стратегии развития, совершенствование деятельности предприятия).

В-четвёртых, вспомогательные процессы — они создают инфраструктуру предприятия (управление экологической безопасностью, охрана труда, юридические услуги).

Согласно отчету ACFE за 2020 год наибольшее количество случаев совершения мошенничества происходит в сфере банковских и финансовых услуг, промышленности, а также государственном и социально- административном секторе. При этом наибольший средний ущерб от совершенного мошенничества приходится на энергетические компании, промышленное производство и строительство.

Таким образом, мошенничество, совершаемое в рамках промышленных предприятий, является одним из наиболее распространенных[36]

и несет за собой значительный материальный ущерб. Типичное промышленное предприятие ежегодно теряет около 5% выручки в связи с реализацией мошеннических схем.

При этом Ассоциация сертифицированных специалистов по расследованию хищений выделяет следующие виды мошенничества, присущие данной сфере (среди 212 компаний, столкнувшихся с ним):

- Мошенничество при выставлении счетов — 27%;
- Кража наличных денег — 8%;
- Мошенничество с деньгами в кассе — 15%;
- Проверка и оплата подделанных/бракованных товаров — 12%;
- Коррупция — 51%;
- Возмещение расходов — 18%;
- Мошенничество с финансовой отчетностью — 10%;
- Мошенничество с активами компании — 28%;
- Мошенничество с заработной платой — 5%;
- Мошенничество при регистрации выплат — 3%;
- Скимминг (мошенничество с банковским картами) — 7%.

Чаще всего мошенничество в промышленной сфере длится 6 месяцев и меньше, на втором месте по продолжительности схемы, реализация которых занимает 7–12 месяцев, на третьем — 19–24 месяца. При этом согласно проведенному исследованию, 40% мошенничества было выявлено по наводке, 15% удалось выявить внутреннему аудиту, 13% схем были замечены по результатам проведенного расследования менеджментом компании, 9% — при анализе документации и отчетности, 7% — случайно, 4%-внешним аудитом, 3% в рамках регулярно проводимого мониторинга, а остальные случаи прочими методами.

Ключевыми потенциальными красными флагами при совершении мошенничества в секторе промышленности являются:

- Сокращение количества товаров на складе и в обороте;
- Связь между поставщиками и персоналом компании, ответственным за закупки (возникновение конфликта интересов);
- Завышение стоимости через счета-фактуры или многочисленные перечисления подрядчикам за невыполненные объемы работ или непредставленные услуги;
- Пролонгация договоров с поставщиками, несмотря на их низкую производительность или необеспеченность основными средствами, отсутствием конкурентных преимуществ;
- Внезапный и необъяснимый рост числа жалоб клиентов, означающий появление контрагента, предоставляющего некачественную продукцию.

Причины, руководящие мошенниками, укладываются в так называемый «треугольник мошенничества», которым руководствуются специалисты, ответственные за экономическую безопасность, а также правоохранительные органы. Совершая нарушения, согласно треугольнику мошенничества, человек ориентируется на три фактора:

- возможность относиться к ситуации, способствующей возникновению мошенничества;
- мотивация объясняется потребностью, ведущей к мошенничеству;
- обоснование отражает причины совершения нечестного поступка.

При реализации фактора «возможность» в производственной организации чаще всего возникают мошеннические схемы в цикле инвентаризации. Запасы являются уязвимой частью транзакций, поскольку зачастую существует большой объем товара, требующий значительного контроля, большое количество сотрудников, имеющих физический доступ к продукции, а также производственный процесс сам по себе усложнен наличием различных этапов.

Эти факторы риска усугубляются, когда запасы невелики, имеют высокую стоимость или пользуются большим спросом. Для управления и выявления возможного мошенничества с запасами могут применяться следующие элементы управления:

- проведение инвентаризации имущества;
- проведение регулярного мониторинга и внеплановых проверок обоснованности затрат на производство и запасы;
- анализ списаний запасов;
- сверка трудовых и накладных расходов, отнесенных к запасам.

Согласно отчету Leading Edge Alliance Manufacturing Outlook 2017 года, большинство производителей считают сокращение операционных расходов главным приоритетом для достижения успешности бизнеса. При среднем мошенничестве в промышленности, длящемся 12 месяцев и приносящим ущерб $240000, край-

не важно, чтобы организации как можно скорее внедрили внутренний контроль и/или ввели процедуры технического обслуживания.

Хотя единого подхода к созданию системы внутреннего контроля в компании не существует, ниже представлены некоторые меры внутреннего контроля, которые производители применяют для предотвращения мошенничества, связанного с запасами:

- ограничение физического доступа к запасам и материалам только для определенного ряда уполномоченных сотрудников;
- ограничение должностных полномочий сотрудников в рамках производственного цикла: ответственному за хранение запасов не рекомендуется выставление счетов, осуществление закупки, доставки или ведения учета;
- установление официальной политики для выявления и обозначения дефектных изделий;
- ограничение должностных полномочий сотрудников в целях идентификации дефектных изделий и их утилизации;
- обеспечение контроля над работой сотрудников, замещающих своих коллег во время отпуска: ими могут быть отмечены странные моменты в процессе реализации должностных обязанностей;
- установление видеокамер на складах, где хранится инвентарь;
- автоматизация производственного процесса.

Кроме того, необходимо принятие более глобальных мер, включающих в себя:

1. Организацию программы управления рисками мошенничества: для производственного сектора. Необходимо учитывать специфичные ключевые уязвимые места, такие как: постоянное взаимодействие с третьими лицами и контрагентами, наличие конфликта интересов и безналичного мошенничества с активами предприятия и тд.
2. Создание системы внутреннего контроля: проактивный подход к идентификации и минимизации рисков мошенничества на этапе их возникновения способствует избеганию значительных затрат.
3. Корректное ведение соответствующей документации и отчетности, которое позволяет сохранять и поддерживать бумажный след для мониторинга производственного процесса.
4. Обеспечение контроля за решением вопросов, связанных с выплатой наличных средств, и поощрение электронных способов оплаты.

На макроуровне в компании необходимо создать политику о неэтичном поведении, положение о конфликте интересов, мотивационную политику сотрудников, контролировать соблюдение необходимых региональных и применимых глобальных законов (комплаенс контроль), принять необходимые требования в сфере противодействия отмыванию денег и финансированию терроризма.

Для обеспечения эффективности функционирования внутреннего контроля решающее значение имеет проведение периодических проверок и обеспечение регулярного мониторинга.

Технологическое обеспечение: технологии в настоящее время все чаще становится первой линией обороны для предприятий, чтобы обнаружить и предотвратить мошенничество. Использование сложного программного обеспечения и ИТ-систем, анализ и мониторинг данных для выявления потенциальных несоответствий позволяют значительно снизить потери из-за мошенничества.

Сфера промышленного производства продолжает подвергаться риску мошенничества. Это существенно замедляет рост и подрывает прогресс в секторе, препятствуя потенциальным новым инвестициям и ограничивая возможности для существующих производителей и новых участников рынка.

Однако управление рисками мошенничества, основанное на выявлении существующих и возникающих угроз, могут смягчить ущерб и частоту мошенничества. При этом особое внимание следует уделять аудиту и контролю над деятельностью третьих сторон. Своевременно принятые меры по борьбе с мошенничеством, адаптированные к данному сектору, могут значительно снизить и устранить возникающие угрозы мошенничества.

Библиографический список

1. *Княжев О. А.* Корпоративное мошенничество. Охота на крыс. — Издательские решения, 2016. — 90 с.;
2. *Гундега Т.* Мошенничество: Определения, портрет типичного мошенника, как бороться с последствиями // KPMG — М., 2013

3. *Ордынская И.* Как противодействовать мошенничеству в компании // Финансовый директор — М., 2016
4. http://www.pwc.ru/en/forensic-services // Российский обзор экономических преступлений за 2016 год (дата обращения: 19.12.2019)
5. http://www.pwc.ru/en/forensic-services // Российский обзор экономических преступлений за 2018 год (дата обращения: 19.12.2019)
6. Отчет о мошенничестве ACFE 2016 // https://s3-us-west-.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf (дата обращения:20.12.2019)
7. Отчет о мошенничестве ACFE 2018 // www.acfe.com URL: http://www.acfe.com/rttn2016.aspx (дата обращения: 20.12.2019)
8. Портрет современного корпоративного мошенника 2016 — URL: https://assets.kpmg.com/content/dam/kpmg/ru/pdf/2016/12/ru-ru-profiles-of-the-fraudster-russia-and-the-cis.pdf (дата обращения: 19.12.2019)
9. Global profiles of the fraudster: Technology enables and weak controls fuel the fraud URL: https://home.kpmg.com/xx/en/home/insights/2016/05/global-profiles-of-the-fraudster.html (дата обращения: 20.12.2019)
10. LEA Manufacturing Outlook Survey Shows Despite Industry Headwinds, U. S. Manufacturers Are Optimistic and Expecting Revenue Growth in 2017 URL: http://anderscpa.com/lea-manufacturing-outlook-survey-results/ (дата обращения:20.12.2019)
11. How Manufacturers Can Detect and Prevent Fraud Using Inventory Internal Controls URL: http://anderscpa.com/manufacturers-internal-controls/ (дата обращения: 20.12.2019)1