УДК 33.025.12
DOI 10.36511/2588-0071-2020-4-61-67

Прасолов Валерий Иванович
кандидат политических наук, доцент, доцент кафедры «Анализ рисков и экономическая безопасность»
Финансовый университет при Правительстве Российской Федерации (125993, Москва, ГСП-3, Ленинградский проспект, 49)

Valeriy I. Prasolov
candidate of political science, associate professor of the department "Risk analysis and economic security"
Financial university under the Government of the Russian Federation (49 Leningradsky av., GSP-3, Moscow, Russian Federation, 125993)

E-mail: VIPrasolov@fa.ru

Земсков Владимир Васильевич
доктор экономических наук, доцент, заведующий кафедрой «Анализ рисков и экономическая безопасность»
Финансовый университет при Правительстве Российской Федерации (125993, Москва, ГСП-3, Ленинградский проспект, 49)

Vladimir. V. Zemskov
doctor of economics, associate professor, head of the department "Risk analysis and economic security"
Financial university under the Government of the Russian Federation (49 Leningradsky av., GSP-3, Moscow, Russian Federation, 125993)

E-mail: VVZemskov@fa.ru

Противодействие корпоративному мошенничеству: контрольные процедуры в сфере закупок

Countering corporate fraud: control procedures in the field of procurement

Государственные закупки – обширная сфера, в которой обращается большое количество бюджетных денежных средств. Неудивительно, что к ней проявляют интерес мошенники, использующие многообразие схем по обману государства. Цель статьи – рассмотреть контрольные процедуры по предупреждению мошеннических действий при закупках. Важным этапом работы над темой также стало определение специфики мошенничества в закупочной деятельности, проведение анализа реализуемых контрольных процедур в рассматриваемой компании. Результатом исследования стали рекомендации по совершен-

ствованию системы противодействия корпоративному мошенничеству в сфере закупок.

Ключевые слова: экономическая безопасность, корпоративное мошенничество, контрольные процедуры, закупки.

Public procurement is an extensive area in which a large amount of budget funds is used. It is not surprising that scammers who use a variety of schemes to deceive the state show interest in it. The purpose of the article is to review control procedures for preventing fraudulent actions in procurement. An important stage of work on the topic was also to determine the specifics of fraud in procurement activities, to analyze the control procedures implemented in the company under consideration. The study resulted in recommendations for improving the system for countering corporate fraud in the field of procurement.

Keywords: economic security, corporate fraud, control procedures, procurement.

Мошенничество, согласно уголовному законодательству Российской Федерации, – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Одним из подвидов корпоративного мошенничества является мошенничество в закупках. Это один из наиболее популярных видов мошенничеств. Как следует из опроса PwC, 33% выявленных случаев мошенничества приходится именно на сферу закупок. Самый уязвимый этап в процессе закупок – этап выбора поставщика. 95% респондентов PwC считают, что на этом этапе происходят мошеннические действия [1]. Один из путей противодействия мошенничеству – обращение пристального внимания на контрольные процедуры.

Однако, ознакомившись с классификацией корпоративного мошенничества Ассоциации дипломированных специалистов по расследованию мошенничества (ACFE) [2], Fraud Tree (дерево мошенничества), можно понять, что мошенничество в компании выходит за рамки, очерченные российским законодательством. Помимо традиционного мошенничества – присвоения активов – ею выделено еще два вида корпоративного мошенничества: коррупция и мошенничество с финансовой отчетностью. Дословный перевод термина-синонима корпоративного мошенничества в методологии Ассоциации означает «профессиональное мошенничество и злоупотребление». В данный термин авторы аналитических материалов вкладывают следующий смысл: это использование своей должности в целях личного обогащения путем преднамеренного злоупотребления или неправильного применения ресурсов или активов компании-работодателя.

Говард Р. Давиа [3] определяет корпоративное мошенничество как любое умышленное действие со стороны персонала, менеджмента, третьих лиц, связанное с обманом и злоупотреблением доверием, причиняющее ущерб компании и направленное на обогащение действующих лиц. Данное определение отличается от предыдущего тем, что выделяется такой вид субъекта корпоративного мошенничества, как третьи лица. Таким образом, приведен-

ное определение несколько шире, если трактовать третье лицо как изолированный субъект, который совершает мошеннические действия без сговора с сотрудниками компании.

Джеральд Л. Ковасич [4, с. 52] понимает корпоративное мошенничество как преступление, участники которого неправомерно получают доступ или обманным путем завладевают корпоративными активами. Данное определение ближе всех к формулировке российского законодательства.

В настоящем исследовании под корпоративным мошенничеством будут пониматься (трактовка И.П. Бурдиковой) [5, с. 1039] любые противоправные действия, которые:

1) связаны с обманом и злоупотреблением доверием/полномочиями в целях личного или для других лиц приобретения преимуществ неправомерного характера (имеющих любую форму);

2) приводят к тому, что компания теряет активы (денежные средства, имущественные права, имущество), упускает выгоду и (или) несет дополнительные убытки;

3) совершаются сотрудниками компании.

Можно сказать, что корпоративное мошенничество – далеко не новое явление. Однако борьба с ним продолжает быть актуальной, поскольку оно представляет собой угрозу экономической безопасности компании. Обеспечение экономической безопасности хозяйствующего субъекта – одно из основных условий его успешного функционирования.

Проанализировав различные определения понятия «экономическая безопасность», автор пришел к выводу, что эта категория описывается следующими ключевыми пунктами:

1) экономическая безопасность – это состояние;

2) обеспечение экономической безопасности неразрывно связано с действиями в отношении опасностей, угроз и рисков (осознание, нейтрализация, управление);

3) экономическая безопасность является фундаментом развития организации и одновременно результатом грамотной реализации процесса развития.

Переходя к вопросам о сущности понятий «опасность», «угроза» и «риск», необходимо заметить, что они связаны между собой как формы воплощения влияния неопределенности на хозяйствующий субъект. Опасность – гипотетическая возможность явления, предмета, процесса при определенных условиях нанести ущерб объекту обеспечения безопасности. Угроза – высший уровень опасности, ее практическое воплощение, проявление. Риск – субъективная категория, поскольку его оценка и управление находятся в непосредственной зависимости от субъекта анализа рисков.

Комбинируя различные подходы в обозначенной сфере, автор приходит к следующему содержанию системы противодействия корпоративному мошенничеству:

1. Оценка рисков мошенничества (идентификация, оценка вероятности и возможного ущерба).

2. Предотвращение мошенничества (наличие общекорпоративных процедур, цель которых – минимизация мошенничества: установление ролей и обязанностей в сфере противодействия мошенничеству, наличие кодексов,

политик, информирование сотрудников о наказаниях, проведение тренингов; внедрение контрольных процедур для отдельных бизнес-процессов).

3. Выявление и расследование мошенничества (использование специальных способов мониторинга и контроля деятельности, а также поддержание эффективно функционирующей системы оповещения – «горячей линии»).

4. Осуществление корректирующих действий (направленных на недопущение случаев мошенничества в будущем и на привлечение к ответственности виновных лиц: привлечение к ответственности, устранение недостатков контрольной среды).

Результатом, полезным эффектом успешной борьбы с мошенничеством являются предотвращенный экономический ущерб (стоимость присвоенных активов и штрафы за нарушение антикоррупционного законодательства), сохранение деловой репутации как предпосылки развития компании, а также позитивный психологический климат в компании.

Осознав данные ценности, разработав их качественное и количественное описание, необходимо внедрить контрольные процедуры, которые и будут способствовать реализации на практике установок руководства.

Контрольные процедуры – это мероприятия и действия, направленные на минимизацию рисков. Риск [6] в данном контексте – потенциально возможное действие или событие, способное воспрепятствовать достижению целей компании или отдельных процессов (направлений деятельности) и влекущее за собой негативные последствия. Риск характеризуется вероятностью и существенностью последствий.

В закупочной деятельности существуют различные виды мошеннических схем. Возвращаясь к «дереву мошенничества», можно сказать, что манипуляции с финансовой отчетностью в данной сфере не являются самоцелью, а служат в большей степени прикрытием для коррупции и присвоения активов.

Коррупция помимо конфликта интересов с непрямой материальной выгодой может принимать форму «откатов» на различных основаниях: за выбор конкретного поставщика, за расширение объема и ассортимента поставок, за предоставление льготных условий (предоплата, товарное кредитование).

К присвоению денежных активов относятся: оплата вне соответствия качеству и количеству, выставление фиктивных счетов («обналичивание»), оплата компании-дублеру. Согласно методологии компании KPMG [7] завышение цены можно расценивать не только как коррупцию, но и как присвоение денежных средств. Ущерб рассчитывается как размер денежных средств, выведенных на оплату, за минусом самого высокого рыночного предложения товара.

Кроме того, в части присвоения денежных активов существуют схемы без участия поставщика. Например, могут осуществляться в сговоре с бухгалтером выдача денежных средств на закупки под отчет и их возврат как неиспользованных. Таким образом, появляется возможность получить во временное пользование деньги организации. Также возможны закупки оборудования и услуг для личного пользования за счет организации.

В части дизайна и реализации контрольных процедур большое значение имеет степень их автоматизации. Компания «ВымпелКом» не первый год за-

нимается вопросами автоматизации закупок. В 2015 году появилась статья о том, что она автоматизировала закупки товаров, работ и услуг, переведя их на электронную торговую площадку B2B-Center. Была автоматизирована вся закупочная деятельность – все этапы процедур и взаимодействий с поставщиками. Это позволило, помимо сокращения затрат, повысить управляемость закупочной деятельности филиалов. Автоматизация способствует отслеживанию эффективности и результативности закупок, оцениванию их в режиме реального времени.

В начале марта этого года пресс-служба оператора «ВымпелКом» сообщила о комплексной оптимизации логистических процессов [8]. Оптимизация выражалась во внедрении программы 3PL (компания предоставила поставщикам логистические услуги), в трансформации бизнес-процесса планирования закупок, а также реинжиниринге P2P-процесса (Purchase to Pay – от заявки до оплаты) – была произведена автоматизация в части запросов, закупок, приемки, платежа и учета.

Необходимо сказать, что компания «ВымпелКом» открыта для обратной связи – есть конфликтная комиссия, принимающая жалобы от контрагентов. Ее цель – повысить прозрачность процедур и обеспечить внутренний контроль. В случае подозрения в нарушении процедур отбора для снижения конкуренции контрагент может апеллировать к итогам предварительной квалификации, дисквалификации, выбора контрагента. Очевидно, что компания значительное внимание уделила построению контрольной среды, это относится в большей степени к предупредительным мерам контроля мошеннических действий сотрудников:

– этические стандарты и нормы поведения;

– основополагающие политики и процедуры (например, антикоррупционная политика, кадровая политика, политика по распределению обязанностей и т. п.);

– положение о совете директоров и его комитетах;

– организационная структура;

– правила коммуникации и распространения информации.

К рыночным тенденциям на данный момент относятся усиление роли внутреннего аудита и усовершенствование систем выявления противоправных действий. Это говорит о том, что происходит усиление этапа выявления мошенничества [1].

И даже четкое прописывание бизнес-процессов, разделения полномочий не позволит спасти компанию от фрода. Результат может быть прямо противоположным – автоматизированные системы могут создать иллюзию алгоритмизированной правильности всех процессов. Однако мошенничество – дело творческое и специалисты в данной области рано или поздно смогут придумать, как обойти ограничения системы.

Иными словами, превентивных и текущих контрольных процедур, которые обеспечивает работа автоматизированных информационных систем в сфере закупок, недостаточно.

Необходимо заниматься отдельно выявлением мошеннических схем – аномалий в бизнес-процессах. Это не означает кардинальную перестройку бизнес-процессов компании, подобные программы представляют собой всего лишь

дополнение к уже существующему программному обеспечению. На основе данных, полученных из базовых систем, проводится Data Mining [9].

Переходя к следующей рекомендации, следует сказать, что важно в свете автоматизации не забыть про проблему кибербезопасности [10]. Киберпреступления – вид экономического преступления, который на настоящий момент недооценен, это следует из отчета PwC. Особое внимание должно уделяться управлением доступа и обеспечению непрерывности работы системы [1].

Итак, к уязвимым местам системы отнесено было недостаточное внимание мерам последующего контроля, направленного на выявление мошенничества, что означает необходимость привлечения представителей внутреннего аудита. Кроме того, была подчеркнута значимость обеспечения информационной безопасности автоматизированных систем, обеспечивающих реализацию контрольных процедур. Привлечение специалистов в области анализа данных и кибербезопасности позволит минимизировать риски мошеннических действий сотрудников и партнеров компании и, следовательно, избежать дополнительных рисков, с ними связанных.

Примечания

1. Российский обзор экономических преступлений за 2016 год // PwC Россия. URL: https://www.pwc.ru/ru/recs2016.pdf (дата обращения: 25.03.2020).

2. Report to the nations on occupational fraud and abuse. URL: https://s3-uswest2.amazonnaws.com/acfepublic/2016-report-to-the-nations.pdf (дата обращения: 25.03.2020).

3. Говард Р. Давиа. Мошенничество: методики обнаружения / пер. с англ. Санкт-Петербург: ДНК, 2005.

4. Джеральд Л. Ковасевич. Противодействие мошенничеству. Как разработать и реализовать программу мероприятий. М.: Маросейка, 2010.

5. Бурдикова И.П. Понятие системы противодействия мошенничеству и ее роль в корпоративном управлении // Сборник трудов конференции IV Международного студенческого конгресса. 2013. М.: Финансовый университет при Правительстве Российской Федерации, 2013.

6. Политика по противодействию мошенничеству и коррупции открытого акционерного общества «Интер РАО ЕЭС» // Интер РАО ЕЭС. Энергия без границ. URL: https://www.interrao.ru/upload/docs/Politika.pdf (дата обращения: 25.03.2020).

7. Практические аспекты мошенничества в закупочной деятельности. KPMG // Внутренний контроль и аудит в России: материалы Национальной практической конференции. URL: http://conf-audit.ru/wp-content/uploads/2014/10/Isaeva.pdf (дата обращения: 25.03.2020).

8. Алексей Када, «ВымпелКом»: Убрать лишние звенья // Entelligent enterprise. URL: https://www.iemag.ru/interview/detail.php?ID=32197 (дата обращения: 25.03.2020).

9. Машинное обучение против фрода // Издательство «Открытые системы». URL: https://www.osp.ru/os/2017/02/13052223/ (дата обращения: 25.03.2020).

10. Почему алгоритмы машинного обучения нужно защищать от хакеров // Социальные технологии. URL: https://te-st.ru/2017/03/21/why-machine-learning-algorithms-need-to-be-protected-from-hackers/ (дата обращения: 25.03.2020).

References

1. Russian review of economic crimes for 2016. *PwC Russia*. URL: https://www.pwc.ru/ru/recs2016.pdf (accessed 25.03.2020). (In Russ.)

2. Report to the nations on occupational fraud and abuse. URL: https://s3-uswest2.amazonпaws.com/acfepublic/2016-report-to-the-nations.pdf (accessed 25.03.2020).

3. Goward R. Davia. Fraud: methods of detection / transl. from Engl. St. Petersburg: DNK Publ., 2005. (In Russ.)

4. Gerald L. Kovasevich. Countering fraud. How to develop and implement a program of events. Moscow: Maroseyka Publ., 2010. (In Russ.)

5. Burdikova I.P. The concept of anti-fraud system and its role in corporate governance. *Proceedings of the conference of the IV International student congress. 2013*. Moscow: Financial University under the Government of the Russian Federation Publ., 2013. (In Russ.)

6. Policy on combating fraud and corruption of the open joint stock company «Inter RAO UES». *Inter RAO UES. Energy without borders.* URL: https://www.interrao.ru/upload/docs/Politika.pdf (accessed 25.03.2020). (In Russ.)

7. Practical aspects of fraud in procurement. KPMG. *Internal control and audit in Russia: materials of the National practical conference*. URL: http://conf-audit.ru/wp-content/uploads/2014/10/Isaeva.pdf (accessed 25.03.2020). (In Russ.)

8. Alexey Kada, VimpelCom: Remove unnecessary links. *Entelligent enterprise*. URL: https://www.iemag.ru/interview/detail.php?ID=32197 (accessed 25.03.2020). (In Russ.)

10. Machine learning against fraud. *Open systems publishing house*. URL: https://www.osp.ru/os/2017/02/13052223/ (accessed 25.03.2020). (In Russ.)

11. Why machine learning algorithms need to be protected from hackers. *Social technologies*. URL: https://te-st.ru/2017/03/21/why-machine-learning-algorithms-need-to-be-protected-from-hackers/ (accessed 25.03.2020). (In Russ.)