Мезенков Г.С., магистрант
Лупикова Е.В., к.э.н., доцент
Тюменский государственный университет

Оценка риска корпоративного мошенничества в рамках системы внутреннего контроля

Аннотация. Наиболее эффективным средством профилактики и выявления мошенничества в компаниях является эффективная система внутреннего контроля (СВК). Оценка рисков, как один из элементов СВК, является превентивным способом борьбы со злоупотреблением должностными полномочиями. В статье изучен международный опыт оценки рисков мошенничества и возможности его использования в отечественной практике.

Ключевые слова: внутренний контроль, корпоративное мошенничество, риски мошенничества.

Mesenkov G. C., master's degree courses
Lupikova E. V., PhD in Economic sciences, Assoc. Prof.
Tyumen state University

ASSESSING THE RISK OF CORPORATE FRAUD IN THE FRAMEWORK OF THE INTERNAL CONTROL SYSTEM

Abstract. The most effective means of prevention and detection of fraud in companies is an effective internal control system (ICS). Risk assessment as one of the elements of ICS, is a preventive way of dealing with abuse of power. In the article the international experience of assessing the fraud risk and the possibility of its use in domestic practice.
Key words: internal control, corporate fraud, risks of fraud.

Внутренний контроль – это процесс, осуществляемый экономическим субъектом, направленный на решение следующих задач [1]:

- обеспечивать достоверность и своевременность бухгалтерской (финансовой) и иной отчетности;
- обеспечивать соблюдение применимого законодательства, в том числе при совершении фактов хозяйственной жизни и ведении бухгалтерского учета;
- способствовать эффективности и результативности финансово-хозяйственной деятельности, в том числе способствовать сохранности активов [1].

Важно подчеркнуть тот факт, что сам процесс внутреннего контроля должен осуществляться непрерывно, только в этом случае задачи внутреннего контроля будут выполняться максимально эффективно.

Система внутреннего контроля (далее СВК) – совокупность организационной структуры и культуры, методов, процедур, правил, разработанных и принятых руководством хозяйствующего субъекта, позволяющих обеспечивать выполнение задач внутреннего контроля.

Одним из элементов внутреннего контроля является оценка рисков [1].

Риск – это вероятность возникновения неблагоприятного события.

Риск – вероятность, рассчитанная количественными методами, например, математическими, статистическими, а также качественными методами, например, метод экспертных оценок.

Информация Минфина России № ПЗ-11/2013 «Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности» гласит о том, что эффективность внутреннего контроля снижается, если руководство экономического субъекта либо иной персонал превышает свои должностные полномочия. Далее, согласно этой информации очень важным аспектом оценки рисков является оценка риска злоупотреблений, другими словами – мошенничества.

Тем не менее, Минфин России лишь говорит о том, что нужно оценить, но не как. Таким образом, проблемой является сам механизм оценки риска.

Сам элемент оценки рисков в СВК является превентивным способом борьбы со злоупотреблением должностными полномочиями.

Как уже было сказано выше, оценка риска может осуществляться количественным и качественными методами. Каждый из этих подходов имеет свои преимущества и недостатки. Например, количественные методы более точны в определении риска. Тем не менее, они могут быть затратными, например, с точки зрения времени, особенно при первичной разработке модели оценки риска.

Качественные методы проще в использовании, но вопрос их точности остаётся открытым.

Перед тем, как произвести оценку риска, необходимо выявить зоны риска (уязвимые места) организации [2]. Группировка таких зон может происходить, например, по отделам предприятия, направлениям видов деятельности, хозяйственным операциям. Как группировать зоны риска выбираем сама организация. В этот случае понадобятся экспертные оценки людей, которые смогут сказать, опираясь на свой профессиональный опыт, что больше подвержено риску. Отсюда следует, что вероятность возникновения злоупотреблений на таких участках должна подвергнуться более тщательной оценке уже количественными методами.

Процесс распознавания зон, подверженных риску мошенничества может проводиться с помощью следующих техник:

- семинары и интервью;
- мозговой штурм;
- анкетирование;
- пошаговый анализ бизнес процессов с их старта до финиша;
- сравнение с другими организациями [2].

Когда были определены зоны риска на основе профессионального суждения специалистах, участвующих в этом процессе, необходимо определиться к какому механизму оценки риска мошенничества организация в силах прибегнуть.

Самым простым способом оценки риска будет являться его градация. Например, разделение риска на низкий, средний, высокий. Либо с добавлением уровней выше и ниже среднего.

Ещё одним простым примером расчёта риска будет следующий вариант. Организация, разрабатывает некую форму, в которой указано, в какой степени (в %-м выражении либо в долях) анкетируемый оценивает риск мошенничества, например, в каждом отделе организации. Чем выше процент оценки, тем выше вероятность мошенничества, соответственно, чем процент ниже – тем риск противоправных действий меньше. Далее рассчитывается среднее значение риска по каждому из отделов по формуле среднего значения (1):

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

Где $\bar{x}$ - среднее значение риска;

x_i – оцененный экспертом риск в %-м выражении либо в долях;

n – количество экспертов, участвующих в оценке.

Следующий вариант оценки риска мошенничества в целом по формуле 2 предложил директор центра исследования аудита и передовых технологий EY профессор R. P. Srivastava. Данный подход основан на треугольнике мошенничества, который включает в себя три элемента, это стимул совершения мошенничества, возможность превышения должностных полномочий и самооправдание противоправных действий.

$$FR = RI * RA * RO * RSP \quad (2)$$

Где FR – риск мошенничества (Fraud Risk);

RI – риск стимулов (Risk of Incentives);

RA – риск самооправдания (Risk of Attitude or Rationalisation);

RO – риск возможностей (Risk of Opportunities);

RSP – риск того, что специальные процедуры не в состоянии обнаружить мошенничество (Risk that Special Procedures fail to detect fraud).

Автор рекомендует добавить в модель четвертый компонент – риск того, что что специальные процедуры, проводимые аудиторами, не в состоянии обнаружить мошенничество.

Следует подчеркнуть, что согласно исследованию PwC, проведенного в 2008 году, главным факторов (86% респондентов) является наличие возможности совершения мошенничества. Следовательно, рекомендуется уделять элементу RO тщательное внимание.

Также существует исследование, посвящённое применению Байесовской формулы риска мошенничества при проведении аудита бухгалтерской (финансовой) отчетности [3].

В основе исследования лежит подход рассуждений на базе свидетельств (Evidential reasoning approach – ER), объединяющий вероятности в сети переменных для получения аналитических моделей в рамках Байесовской структуры [3].

ER – это подход, основанный на многокритериальном анализе решений проблем, имеющих как количественные, так и качественные критерии при различных неопределенностях [4].

ER подход в этом случае используется для вывода формулы риска мошенничества, основанный на факторах треугольника мошенничества: стимулы, оправдание и возможность.

Таким образом, можно сделать вывод о том, что организация сама должна решить какие методы оценки рисков ей использовать. Это будет зависеть от её денежных ресурсов, трудовых ресурсов. От размера компании, так как если компания маленькая, то просто нет смысла применять, например, Байесовскую формулу риска. Также следует подчеркнуть, что если масштабы деятельности компании очень велики, то ограничиться лишь качественными методами либо градаций риска на низкий, средний и высокий будет ошибочным вариантов решения проблемы оценки риска в СВК. Как показывает практика, превентивные методы борьбы в мошенничеством оправдывают себя. Так, согласно исследованию KPMG «Profile of a Fraudster Survey 2007» лишь 16% компаний смогли восстановить свои потери от мошенничества [5]. Более того, при подсчете потерь от злоупотреблений следует учитывать не только влияние на финансовую составляющую, но также учитывать репутацию компании.

СПИСОК ЛИТЕРАТУРЫ

1. «Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности» <Информация> Минфина России № ПЗ-11/2013 // Консультант Плюс. [Электронный ресурс]. Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=156407&fld=134&rnd=208987.3040206121887008&#0

2. Алибеков Ш.И. Мошенничество и фальсификация в бухгалтерском учете. Аудит и финансовый анализ. 2008. № 5. С. 1-11.

3. Chartered Institute of Management Accountants. Fraud risk management: A guide to good practice. [Электронный ресурс]. Режим доступа: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

3. Srivastava R.P., Theodore J.M., Jerry L.T. Bayesian Fraud Risk Formula for Financial Statement Audits // A Journal of Accounting, Finance and Business Studies, Vol. 45, No. 1, 2009, pp. 66-87. [Электронный ресурс]. Режим доступа: https://pdfs.semanticscholar.org/6d39/9e203b623b5865db21a67e9405080b08ff59.pdf

4. Jian-Bo Yang. Rule and utility based evidential reasoning approach for multiattribute decision analysis under uncertainties // European Journal of Operational Research. [Электронный ресурс]. Режим доступа: http://www.sciencedirect.com/science/article/pii/S0377221799004415

5. KPMG. Profile of a Fraudster Survey 2007. // Forensic. [Электронный ресурс]. Режим доступа: http://www.itas.sk/sites/default/files/docs/analyzy/kpmg_fraudster_survey_full_en.pdf