DOI 10.37882/2223–2974.2020.07.01

ФОРМИРОВАНИЕ СИСТЕМЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ДАННЫХ ПО ОБНАРУЖЕНИЮ КОРПОРАТИВНОГО МОШЕННИЧЕСТВА

FORMATION OF A CORPORATE INFORMATION SYSTEM USING DATA ON DETECTING CORPORATE FRAUD

K. Abdulkhakova

Summary. The scientific article is devoted to a review of the main elements that are used in the formation of a corporate information system using corporate fraud detection data. The relevance of scientific research on selected issues is due to such a process as the development of corporate business in the Russian Federation (RF) and the increase in the number of cases of corporate fraud that adversely affects the sustainability of the business. The article describes the theoretical aspects of the concept of corporate fraud and the factors of its formation. The tasks of creating a corporate information system using data on the detection of corporate fraud in Russian companies are highlighted. The basic elements of a corporate information system are considered. The stages of the corporate risk management system in organizations are listed. The importance of the corporate risk management system, the formation of information security and an innovative methodology for identifying corporate fraud risks is described. In conclusion of the scientific work, the author noted the following: that the main direction of combating fraud in the corporate management system is the direct impact on the TOP managers of the company, who may act as dependent parties and illegally act in the interests of third parties. It is the management activity of directors in the interests of others that leads to the fact that in Russia there are so frequent cases of corporate fraud. For this reason, it is necessary to formulate an innovative methodology for identifying the risks of corporate fraud arising in the framework of the corporate business structure management system.

Keywords: corporate information; corporate governance; corporate fraud; corporate information system; corporate governance risks; corporate business..

Абдулхакова Камила Рустамовна
Аспирант, Финансовый университет при Правительстве Российской Федерации, г. Москва
kamila181091@mail.ru

Аннотация. Научная статья посвящена обзору основных элементов, которые используются в рамках формирования системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества. Актуальность научного исследования на выбранную проблематику обусловлена таким процессом, как развитие корпоративного бизнеса на территории Российской Федерации (РФ) и увеличение числа случаев корпоративного мошенничества, негативно сказывающегося на устойчивости деятельности коммерческой организации. В рамках статьи описаны теоретические аспекты понятия корпоративное мошенничество и факторов его формирования. Выделены задачи формирования системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества в российских компаниях. Рассмотрены основные элементы системы корпоративной информации. Перечислены этапы системы управления корпоративными рисками в организациях. Описано значение системы управления корпоративными рисками, формирования информационной безопасности и инновационной методики выявления рисков корпоративного мошенничества. В заключении научной работы, автором отмечено следующее: что главное направление противодействия мошенничества в корпоративной системе управления — это прямое воздействие на ТОП-менеджеров компании, которые могут выступать зависимыми лицами и незаконно действовать в интересах третьих лиц. Именно управленческая деятельность директоров в интересах других лиц приводит к тому, что в России столь частые случаи корпоративного мошенничества. По этой причине, необходимо формирование инновационной методики по выявлению рисков корпоративного мошенничества, возникающих в рамках системы управления корпоративными структурами бизнеса.

Ключевые слова: корпоративная информация; корпоративное управление; корпоративное мошенничество; система корпоративной информации; риски корпоративного управления; корпоративный бизнес.

На сегодняшний день, корпоративное мошенничество для российских организаций крупных масштабов — острая проблема, приводящая к отрицательным последствиям. В связи с этим, актуальным является формирование системы корпоративной информации и данных, которые могут использоваться для обнаружения случаев корпоративного мошенничества. Данный процесс относится к системе корпоративного управления и оценивает вероятные ее риски и угрозы, формирующиеся со стороны аффилированных лиц

и управляющих, которые могут выступать звеном в операциях по махинациям, например, с финансовой отчетностью предприятия [6].

Корпоративное мошенничество — это различного рода мошеннические операции, которые противоречат закону и проводятся сотрудником (сотрудниками) или руководителем организации. Виды такого мошенничества достаточно разнообразны [1].

Как правило, факторами корпоративного мошенничества бывает частая смена контрагентов, сложная организационная структура корпоративного бизнеса, специфические условия заключаемых договоров с партнерами и поставщиками, низкий уровень мотивации менеджмента корпоративной структуры управления [7]. Но, по нашему мнению, наиболее важным фактором проявления корпоративного мошенничества является неэффективность действующей системы корпоративной информации по обнаружению случаев корпоративного мошенничества.

Для того, чтобы обеспечить защиту и устойчивость деятельности организации, необходимо формирование эффективной системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества [8].

Ее задачами могут выступать:

- обеспечение информационной защиты и безопасности корпорации от мошеннических действий других лиц;
- обеспечение системы раскрытия корпоративной отчетности для стейкхолдеров компании, где будут опубликованы данные по обнаружению случаев корпоративного мошенничества.

Для нас, наибольшую актуальность играет выполнение задачи по обеспечению информационной безопасности компании от мошеннических действий других лиц.

В современных условиях экономики России, информационная система обмена данными и ее аккумуляции — частый инструмент, используемый в рамках корпоративного управления. По этой причине, среди всех рисков корпоративной системы управления, именно риски раскрытия коммерческой информации (раскрытие коммерческой тайны, продажа патентов и лицензий не в интересах компании, слив инсайдерской информации, манипуляции на фондовом рынке) выступают наиболее весомыми при определении урона негативного воздействия на экономическую устойчивость деятельности организации [2].

Поэтому, первым элементом формирования системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества будет система управления корпоративными рисками компании. Она, в свою очередь, состоит из следующих этапов [3]:

- определение целей и задач;
- выявление корпоративных рисков;
- оценка корпоративных рисков;
- воздействие на корпоративные риски;
- мониторинг системы управления корпоративными рисками;
- корректировка стратегии управления корпоративными рисками.

Следующий элемент формирования системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества — это система информационной безопасности организации. Ключевой причиной важности информационной безопасности, как основы корпоративной системы обнаружения мошенничества является экономическая конкурентная разведка, приводящая к промышленному шпионажу и краже конфиденциальной информации и интеллектуальной собственности компании [9; 10].

Среди действий по защите информационных ресурсов, необходимо внедрение системы повышения конфиденциальности информации внутри компании, что можно провести при помощи следующих рекомендаций [4]:

- создать качественную документацию в сфере защиты;
- увеличить разграничение доступа к информации по отдельным группам сотрудников компании;

- создать функционирование грифов «коммерческая тайна» и кодов идентификации документации;

- ввести особые режимы пользования сетью Интернет;
- использовать программное обеспечение DLP-системы и SIEM-системы.

Кроме того, с целью совершенствования процесса обеспечения информационной безопасности компании, необходимо использовать методы, отвечающих за надежность облачных технологий, которые активно применяются российскими корпоративными структурами бизнеса при обмене своею коммерческою и финансовой информацией [5]:

- шифрование — наиболее эффективный и простой способ, в рамках которого провайдер облачного хранилища обязан шифровать информацию клиентов, и безвозвратно удалять, в случае прекращения предоставления ему услуг;
- защита данных при передаче информации — способ предполагает запрет доступа к информационным данным в облачном хранилище, пока

те не будут аутентифицированы после своей передачи;

- аутентификация — способ предполагает установление одноразовых паролей, генерация ключей которых происходит при помощи таких технологий, как SAML и LDAP;
- изоляция пользователей — наиболее сложный способ обеспечения информационной безопасности в облачных хранилищах, поскольку провайдер формирует изоляцию данных клиентов друг от друга видоизменяя код внутри системы. В связи с этим, могут быть произведены ошибки, из-за которых клиенты могут случайным образом получить доступ к данным других клиентов.

Следующим элементом формирования системы корпоративной информации с использованием данных по обнаружению корпоративного мошенничества является формирование инновационной методики выявления рисков корпоративного мошенничества, осуществляемого советом директоров компании.

В 2017 году аналитическое агентство Spencer Stuart опубликовало свои научные и практические исследования по вопросу эффективности совета директоров в России. Они проанализировали 41 крупнейшую корпорацию страны, в которых действуют 447 директоров, и лишь 36,7% из них можно считать независимыми.

Это позволяет в заключении научного исследования, прийти к следующему выводу: главное направление противодействия мошенничеству в корпоративной системе управления — это прямое воздействие на ТОП-менеджеров компании, которые могут выступать зависимыми лицами и незаконно действовать в интересах третьих лиц. Для обеспечения устойчивости и экономической безопасности организации важно формирование инновационной методики, особенностями которой будет цифровизация и привлечение внешних агентов.

ЛИТЕРАТУРА

1. 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.
2. Сергеева И.Г., Грачева Е. А. Управление корпоративными рисками в предпринимательской деятельности // Экономика и экологический менеджмент.— 2014.— № 4.— С. 280–287.
3. Шихвердиев А.П., Кириенко Е. С. Управление рисками в системе корпоративного управления. URL: http://koet.syktsu.ru/vestnik/2012/2012–4/21/21.html (дата обращения: 01.06.2020).
4. Хлестова Д.Р., Попов К. Г. Особенности защиты конфиденциальной информации на предприятиях // Символ науки. 2016. № 5–2.
5. Исаев Е.А., Думский Д. В., Самодуров В. А., Корнилов В. В. Обеспечение информационной безопасности облачных вычислений. URL: http://www.matbio.org/2015/Isaev_10_567.pdf (дата обращения: 01.06.2020).
6. Ульянова О. В. Корпоративное мошенничество в финансовой отчетности // Научный журнал. 2016. № 9 (10).
7. Леонова Л. А. Проблемы бухгалтерского мошенничества в финансово-промышленных группах // Вестник Института экономических исследований. 2018. № 3 (11).
8. Когденко В. Г. Корпоративное мошенничество: анализ схем присвоения активов и способов манипулирования отчетностью // Экономический анализ: теория и практика. 2015. № 4 (403).
9. Скачкова Р. В. Проблемы оценки мошенничества с финансовой отчетностью // ИБР. 2018. № 2 (31).
10. Кагиров Д. Х. Проблема противодействия корпоративному мошенничеству // Молодой ученый. 2018. № 30 (216). С. 35–36.

Журнал «Современная наука: актуальные проблемы теории и практики»