**УДК 33** **DOI: 10.34670/AR.2020.91.1.034**

# Риски мошенничества как угроза экономической безопасности промышленного предприятия

**Захарова Татьяна Сергеевна**

Студент
Финансовый университет при Правительстве РФ,
125993, Российская Федерация, Москва, просп. Ленинградский, 49;
e-mail: tsz1998@yandex.ru

**Аннотация**

В статье приводится перечень рисков промышленного предприятия, анализ теоретических основ рисков мошенничества как одного из важнейших их видов, приводится базовое определение экономической безопасности хозяйствующего субъекта. По итогам теоретического анализа предлагается вариант системы управления рисками и описываются особенности ее внедрения на рассматриваемом предприятии. В работе показано, что оценка рисков мошенничества должна проводиться по каждому направлению деятельности с учетом всех уровней персонала и распределения между сотрудниками ответственности за разработку, проведение и контроль этапов бизнес-процессов. Оценка помогает предприятиям выявить специфические риски мошенничества и определить, насколько существующие системы контроля действенны и применимы. В последние два года в России такую оценку проводили 61% компаний, что является достаточно высоким показателем.

**Для цитирования в научных исследованиях**

Захарова Т.С. Риски мошенничества как угроза экономической безопасности промышленного предприятия // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 1А. С. 313-318. DOI: 10.34670/AR.2020.91.1.034

**Ключевые слова**

Риски мошенничества, экономическая безопасность, промышленное предприятие.

## Введение

Обеспечение экономической безопасности предприятия - одна из обязательных частей его деятельности, учитывая не только современный этап развития рыночной экономики, но и постоянно прогрессирующие цифровые технологии, которые помогают открывать и пользоваться все более и более фантастическими способами мошенничества.

## Основное содержание

Основываясь на определении понятия «экономическая безопасность», представленном в Указе Президента РФ от 13.05.2017 №208 «О стратегии экономической безопасности Российской Федерации на период до 2030 года», можно сформулировать следующее: экономическая безопасность хозяйствующего субъекта – это состояние его защищенности от внешних и внутренних угроз, при котором сохраняется возможность беспрепятственной деятельности, достижения поставленных руководством целей согласно миссии хозяйствующего субъекта, а также обеспечиваются интересы его сотрудников.

Любое современное промышленное предприятие сталкивается с достаточно широким перечнем рисков. В частности, многообразие рисков промышленного предприятия можно объединить в несколько категорий: риски финансового, материального и морального характера [Виды рисков пищевой промышленности, www...]. На стыке всех трех категорий рисков находятся риски мошенничества. Данный риск достаточно важен и актуален. В 2018 году 66% компаний столкнулись с фактами мошенничества, из них 56% увеличили расходы на борьбу с ним. [Противодействие мошенничеству: какие меры принимают компании, www…]

«Мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». [Уголовный кодекс Российской Федерации от 13.06.1996 № 63] Соответственно риски мошенничества – это потенциальная возможность ущерба от мошеннических действий. Согласно исследованию PwC, в России, как и во всем мире самым распространенным видом мошенничества является незаконное присвоение активов. На второе место становятся взяточничество и коррупция. Далее следует мошенничество в сфере закупок товаров и услуг. [Уголовный кодекс Российской Федерации от 13.06.1996 № 63]

Методом обнаружения рисков мошенничества являются не столько прямые указания на них указания, а косвенные индикаторы:

1.Индикаторы внутреннего контроля – отсутствие и/или несоблюдение регламентов, недостаточность проведения контрольных процедур, отсутствие надлежащего распределения полномочий, недостатки в документообороте.

2. Индикаторы образа жизни – выходящий за привычные рамки образ жизни «не по средствам». Большинство мошенников не могут удержаться и активно тратят похищенные средства.

3.Поведенческие индикаторы – смена обычного поведения и привычек. Мошенник инстинктивно чувствует себя виноватым: стресс, раздражительность, увеличенное потребление табака и алкоголя, подозрительность. Мошенник не оставляет рабочее место без присмотра, редко уходит в отпуск, чтобы не допускать никого к контролю за его областью рабочего процесса.

4.Наводки и жалобы, анонимные сообщения, поведение и активность в социальных сетях.

5.Отношение к информационным ресурсам предприятия. Это может быть необоснованный интерес и получение доступа к «чужим» направлениям работы, копирование и затем передача конфиденциальной информации. [Основы противодействия фроду]

Перечисленные индикаторы обнаружения мошенничества не следует абсолютизировать, всегда нужно действовать в рамках конкретной ситуации и обстоятельств и не выходить за рамки ограничений, которые накладывает Федеральный закон "Об оперативно-розыскной деятельности" от 12.08.1995 № 144-ФЗ на подразделения безопасности в коммерческой организации.

Интересным является портрет типичного мошенника, который обязательно следует учитывать при обнаружении фактов реализовавшихся рисков. В России около 90% офисных мошенников составляют мужчины, причем 75% из них имеет высшее образование. Подозрительными являются:

1. Обладатели негативных черт характера (азартность, безответственность, алчность, неуравновешенность).

2. Обладатели мягкого и податливого характера («подкаблучники»).

3. Работники, которые мечтают о крупной покупке.

4. Работники, которые часто меняет место работы.

5. Работники, столкнувшиеся с неприятностью, связанной с большими расходами (ограбление, автомобильная авария, дорогостоящее лечение родственников и прочее). [Основы противодействия фроду]

Мошенничество легче предотвратить, чем выявить, поэтому программа по борьбе с ним должна преимущественно ориентироваться именно на превентивные меры с дополнениями в виде мер по устранению ущерба от реализовавшихся рисков. Система управления рисками мошенничества предполагает собой целый комплекс мер, который может включать:

1. Внедрение Кодекса корпоративной этики (ККЭ).

2. Утверждение Политики противодействия мошенничеству (ППМ).

3. Работа горячей линии.

4. Помощь услуги Форензик.

5. Организация бизнес-процессов в виде agile-системы.

6. Оценка рисков мошенничества и др.

Рассмотрим более подробно приведенные выше способы предотвращения мошенничества.

Внедрение Кодекса корпоративной этики предполагает разработку документа, который представляет собой свод корпоративных ценностей и правил поведения: нормы деловых отношений между сотрудниками, нормы их поведения на территории предприятия и по отношению к имуществу предприятия, правила реагирования на мошенничество, регламент таких ситуаций как: конфликт интересов, совместная работа родственников, получение и дарение подарков, отношения с контрагентами. ККЭ покрывает принцип обучения сотрудников в компании (anti-fraud awareness program).

Политика противодействия мошенничеству (ППМ) представляет собой документ, который по силе следует за ККЭ и разрабатывается преимущественно генеральным директором. В рамках ППМ Совет Директоров, генеральный директор, руководители структурных подразделений, системный администратор в отделе информационных технологий, все остальные работники компании, а также директор Департамента безопасности должны осуществлять функции по противодействию мошенничеству.

Горячая линия, дает возможным раскрыть информацию о мошенничестве анонимно, если

информатор не хочет раскрывать свою личность.

Помощь Форензик - вида услуг, который включает расследования хищений и мошенничества, выявление причин убытков, их последствий для компании, выявление лиц, причастных к таким нечестным действиям и процессам, оценку ущерба, поиск и возврат активов. [Наш бизнес - Ваше финансовое благополучие, www…]

Организация бизнес-процессов в виде agile-системы. Прозрачные этапы бизнес-процессов, точно определенные обязанности каждого сотрудника, фокус на задание и его цель. Работа ведется небольшими фиксированными отрезками времени, за которые должно реализоваться определённое количество задач. Дробление задач на мелкие подзадачи должно избавить компанию от упущения фактов реализации рисков мошенничества и помочь обнаружить таковые на самых ранних этапах реализации бизнес-процесса. [Что такое Agile-подход и зачем он нужен бизнесу?, www…]

Оценка рисков мошенничества должна проводиться по каждому направлению деятельности с учетом всех уровней персонала и распределения между сотрудниками ответственности за разработку, проведение и контроль этапов бизнес-процессов. Оценка помогает предприятиям выявить специфические риски мошенничества и определить, насколько существующие системы контроля действенны и применимы. В последние два года в России такую оценку проводили 61% компаний, что является достаточно высоким показателем.

## Заключение

Таким образом, можно сказать, что проведенное в рамках работы исследование не позволяет в полной мере оценить эффективность мер системы управления рисками мошенничества на практике, так как необходимо учитывать специфику деятельности промышленного предприятия. При этом целесообразно полагать, что приведенные выше мероприятия окажут положительный эффект на состояние экономической безопасности анализируемого предприятия.

## Библиография

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63 // Российская газета. - Ст. 159 "Мошенничество" с изм. и допол. в ред. от 08.01.2019
2. Основы противодействия фроду. Политика противодействия фроду и проблемы, связанные с её реализацией // Доклад Трофимова А.Ю., генерального директора ООО «Группа компаний «ИнСис», к.э.н. (дата обращения: 19.03.2019).
3. Смородинова Н.И. Финансовые риски промышленного предприятия // Решетневские чтения. 2017.
4. Виды рисков пищевой промышленности // AgroFoodInfo URL: https://agrofoodinfo.com/articles/2547/ (дата обращения: 02.05.2019).
5. Наш бизнес - Ваше финансовое благополучие // FORENSIC & BUSINESS SOLUTIONS URL: http://forensic.su/ (дата обращения: 10.04.2019).
6. Противодействие мошенничеству: какие меры принимают компании? Исследование PwC. // PricewaterhouseCoopers.ru URL: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf (дата обращения: 04.04.2019).
7. Что такое Agile-подход и зачем он нужен бизнесу? // ScrumTrek URL: https://scrumtrek.ru/blog/chto-takoe-agile-podhod-i-zachem-on-nuzhen-biznesu/ (дата обращения: 10.04.2019).
8. Волкова Н.М., Надточий Ю.Б. Новые направления исследований в неоэкономике // Экономические системы. 2019. Том 12. № 1. С. 23 – 32.
9. Туркина Д.Е. Три ключевые проблемы внедрения искусственного интеллекта в российских банках на современном этапе развития экономики // Инновации и инвестиции. 2018. № 12. С. 335 – 336.
10. Диких В.А. Управление инвестиционными вложениями в строительство удаленной энергоэффективной недвижимости // Вестник университета. 2014. № 3. С. 29 – 32.

# The risks of fraud as a threat to the economic security of an industrial enterprise

**Tat'yana S. Zakharova**

Student
Financial University under the Government of the Russian Federation,
125993, 49, Leningradsky, ave., Moscow, Russian Federation;
e-mail: tsz1998@yandex.ru

**Abstract**

The article provides a list of risks of an industrial enterprise, analysis of the theoretical foundations of fraud risks as one of their most important types, provides a basic definition of economic security of an economic entity. Based on the results of the theoretical analysis, a variant of the risk management system is proposed and the features of its implementation at the enterprise in question are described. The work shows that fraud risk assessment should be carried out for each area of activity, taking into account all levels of personnel and the distribution of responsibility among employees for the development, conduct and control of the stages of business processes. The assessment helps enterprises identify the specific risks of fraud and determine how effective control systems are. In the past two years, 61% of companies conducted such an assessment in Russia, which is a high indicator.

**For citation**

Zakharova T.S. (2020) Riski moshennichestva kak ugroza jekonomicheskoj bezopasnosti promyshlennogo predprijatija [The risks of fraud as a threat to the economic security of an industrial enterprise]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 10 (1A), pp. 313-318. DOI: 10.34670/AR.2020.91.1.034

**Keywords**

Fraud risks, economic security, industrial enterprise.

## References

1. The Criminal Code of the Russian Federation of June 13, 1996 No. 63 // Russian newspaper. - Art. 159 Fraud rev. and extra. as amended from 01/08/2019
2. The basics of countering fraud. Anti-fraud policy and problems associated with its implementation // Report by A. Trofimov, Director General of InSis Group of Companies, Ph.D. (Date of treatment: 03/19/2019).
3. Smorodinova N.I. Financial risks of an industrial enterprise // Reshetnev readings. 2017.
4. Types of risks of the food industry // AgroFoodInfo URL: https://agrofoodinfo.com/articles/2547/ (accessed: 05/02/2019).
5. Our business is your financial well-being // FORENSIC & BUSINESS SOLUTIONS URL: http://forensic.su/ (accessed: 04/10/2019).
6. Fraud Prevention: What measures are companies taking? PwC study. // PricewaterhouseCoopers.ru URL: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf (accessed 04.04.2019).
7. What is an Agile approach and why is a business needed? // ScrumTrek URL: https://scrumtrek.ru/blog/chto-takoe-agile-podhod-i-zachem-on-nuzhen-biznesu/ (accessed: 04/10/2019).
8. Volkova N.M., Nadtochy Yu.B. New directions of research in neo-economics // Economic systems. 2019.Vol. 12. No. 1. P. 23 - 32.
9. Turkina D.E. Three key problems of introducing artificial intelligence in Russian banks at the present stage of economic

development // Innovations and Investments. 2018.No 12. S. 335 - 336.
10. Wild V.A. Management of investment in the construction of remote energy-efficient real estate // University Herald. 2014. No. 3. P. 29 - 32.