Особенности регулирования рисков информационного обмена в системе внутреннего контроля

Features of the Regulation of Information Exchange Risks in the Internal Control System

УДК 338.51

DOI: 10.12737/1998-0701-2020-33-37

В.В. Земсков, д-р экон. наук, профессор Департамента «Экономическая безопасность и управления рисками», Финансовый университет при Правительстве Российской Федерации

e-mail: VVZemskov@fa.ru

V.V. Zemskov, Doctor of Economic Sciences, Professor, Department «Economic Security and Risk Management», Financial University under the Government of the Russian Federation

e-mail: VVZemskov@fa.ru

Аннотация. *В статье рассматриваются проблемы анализа и оценки рисков информационного обмена в системе внутреннего контроля. Сделан вывод о том, что дальнейшее совершенствование инфраструктуры внутреннего контроля способствует функции управления хозяйствующего субъекта, обеспечивает своевременный сбор, обобщение и анализ первичной и сводной информации для принятия своевременных управленческих решений.*

Ключевые слова: система внутреннего контроля, информационная инфраструктура, информационный обмен, риски информационного обмена.

Abstract. *The article deals with the problems of analysis and risk assessment of information exchange in the internal control system. It is concluded that further improvement of the internal control infrastructure contributes to the management function of an economic entity, provides timely collection, synthesis and analysis of primary and summary information for making timely management decisions.*

Keywords: internal control system, information infrastructure, information exchange, risks of information exchange.

Одним из компонентов системы внутреннего контроля является формирование информационной инфраструктуры с учетом влияния рисковых ситуаций и неопределенностей. Как известно, в практике хозяйственной деятельности формирование условий для эффективной реализации управленческих функций позволяет руководству и работникам хозяйствующего субъекта принимать своевременные и обоснованные решения, выполнять свои должностные обязанности, так как любое управленческое решение, как правило, однозначно базируется на информации, на служебном документе. Все это достигается за счет организации как внутри хозяйствующего субъекта, так и за его пределами информационного обмена. Под информационным обменом в контексте данного исследования понимается внедрение каналов коммуникации и информационных технологий в общую систему управления хозяйствующим субъектом в целях обеспечения прозрачности бизнеса, обмена информацией между структурными подразделениями и работниками, работниками и высшим руководством по вопросам ведения деятельности, отдельных бизнес-процессов, в том числе процессов подготовки финансовой отчетности, а также внедрения контрольных процедур, обеспечивающих информационную безопасность.

Процесс информационного обмена может быть организован как на бумажном носителе, так и в электронном виде. В настоящем исследовании рассмотрим лишь некоторые аспекты потенциальных рисков, которые могут возникать в процессе информационного обмена.

При этом следует отметить, что перевод информационного обмена в практическую плоскость будет предъявлять новые повышенные требования к формированию компетенций у субъектов внутреннего контроля и видоизменять существующий функционал у персонала хозяйствующего субъекта. Это связано с тем, что непрерывные информационные потоки формируют огромный массив

данных, которые необходимо собрать по определенным критериям, обработать, ранжировать для анализа и представить аналитические материалы руководству хозяйствующего субъекта для принятия управленческих решений.

В системе внутреннего контроля основными элементами информационного обмена являются:

- документооборот;
- документационное обеспечение;
- информационные технологии;
- информационная безопасность.

Документооборот. Согласно Большому толковому словарю русского языка [7], под документооборотом понимается процесс прохождения документов в установленной последовательности с момента их появления и до сдачи в архив.

В соответствии с Федеральным законом «Об обязательном экземпляре документов» [1], под документом понимается материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначенный для передачи во времени и в пространстве в целях общественного использования и хранения. Кроме того, документальным подтверждением информации являются письменные пояснения клиента.

В системе внутреннего контроля под документооборотом понимается процесс оформления и движения документов:

- при планировании;
- при формировании рабочих документов, подтверждающих полученные выводы в ходе контрольных мероприятий;
- при подготовке отчетных документов по результатам контрольных мероприятий;
- при доведении информации о результатах контрольных мероприятий до руководства хозяйствующего субъекта;
- при оформлении распорядительных документов руководства хозяйствующего субъекта о назначении ответственных лиц за корректировочные мероприятия по устранению выявленных недостатков и нарушений;
- при подготовке и проведении процесса мониторинга по результатам корректировочных мероприятий;
- при передаче исполненных документов на хранение в архив;
- при востребовании документов из архива в случае возникновения соответствующих запросов по тому или иному вопросу.

Алгоритм информационного обмена в системе внутреннего контроля, основанный на модели COSO, представлен на рис. 1 [6].

Отчетность системы внутреннего контроля состоит:

- из документов планирования;
- отчетных документов о проверке, включая отчетность руководителей структурных подразделений;
- рабочих документов.

Отчетные документы о проверке подписываются всеми проверяющими и утверждаются руководителем проверки. Оригинал отчетных документов хранится в структурном подразделении, которое инициировало контрольное мероприятие (внутренний контроль, внутренний аудит).

Сущность отчетности руководителей структурных подразделений хозяйствующего субъекта заключается в том, что в этой отчетности они дают свою оценку об эффективности системы внутреннего контроля.

Как правило, рабочие документы включают необходимую документацию, относящуюся к проверочному процессу:

- документы, относящиеся к планированию;
- списки контрольных вопросов;
- копии существенных контрактов;
- учетная политика для целей бухгалтерского и налогового учета;
- письменные подтверждения от третьих лиц;
- анализ необычных операций;
- результаты аналитических процедур;
- заключительная отчетность о проверке и другие документы.

Таким образом, рабочие документы играют важную роль в качестве инструментов контроля, проверки выполнения и информационного обмена по итогам контрольных мероприятий.

Организация документооборота во внутреннем контроле подразумевает разработку форм документов планирования, отчетных и рабочих документов, утверждение графика документооборота между субъектами внутреннего контроля, определение механизма принятия документов к учету, выбор системы

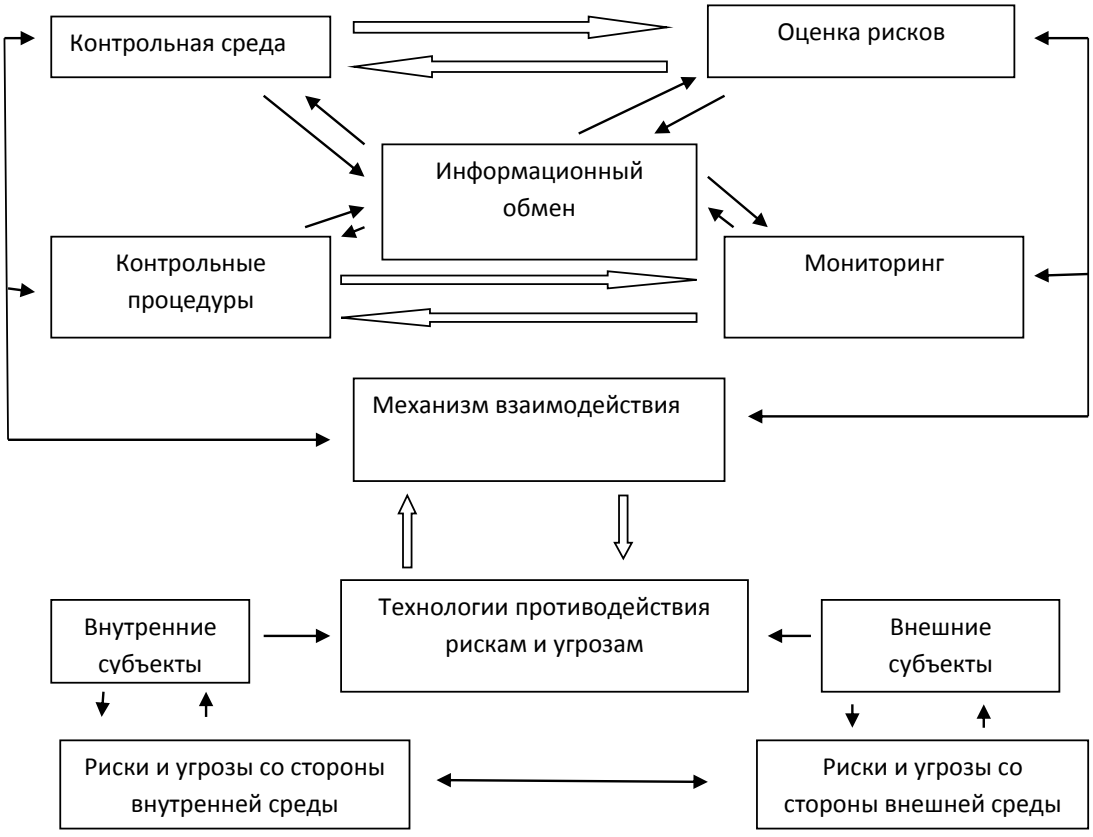

Рис. 1. Алгоритм информационного обмена в системе внутреннего контроля

обработки документов и порядок их хранения. Основное назначение графика документооборота — установление рационального документооборота между субъектами внутреннего контроля, подразделениями и исполнителями, определение минимального срока его нахождения в подразделении.

Рисками отчетных документов являются:

- отсутствие или неполный перечень объектов проверки;
- неотражение контрольных процедур;
- неполный перечень выявленных замечаний и недостатков;
- неопределение сроков устранения замечаний и недостатков;
- неуказание ответственных за исправление замечаний и недостатков;
- отсутствие контроля за исполнением документов;
- несвоевременная передача в архив исполненных документов.

Рисками рабочих документов являются:

- несвоевременное составление рабочих документов;
- неотражение контрольных процедур и порядок ее выполнения;
- неотражение существенных замечаний;
- невозможность подтверждения объема выполненной работы;
- отсутствие или пропуски в фиксации доказательств и т.д.

В целях регулирования рисков документооборота рекомендуется заполнять журнал внутреннего контроля, где отражаются данные о движении документов внутреннего контроля. Форму журнала внутреннего контроля каждый хозяйствующий субъект утверждает в составе документационного обеспечения.

Документационное обеспечение. ГОСТ Р 7.0.8-2013 под документационным обеспечением трактует управленческую деятельность, которая направлена на обеспечение документами общей системы управления, включая планирование, управление, анализ и оценку, прогнозирование [3].

В целях эффективного функционирования системы внутреннего контроля все бизнес-процессы должны иметь документационное

обеспечение. Как известно, к основным бизнес-процессам системы внутреннего контроля относятся:

- планирование контрольных мероприятий;
- выполнение и проверка контрольных мероприятий;
- информирование о результатах проверки.

Эффективное управление контрольной деятельностью начинается с процесса планирования. Процесс планирования имеет следующее документационное обеспечение [5]:

- риск-ориентированный план проведения проверок;
- карта оценки существующих рисков;
- величина риск-аппетита (риск, на который организация готова пойти для достижения целей бизнеса) для различных структурных подразделений;
- политики и процедуры;
- должностные инструкции;
- методы подготовки рабочих документов (набор стандартных форм для используемых документов, каждая страница должна иметь соответствующую «шапку», которая помогала бы правильно идентифицровать информацию, подписи и инициалы работников, порядковый номер страницы).

Рисками документационного обеспечения являются:

- планы контрольной деятельности не соответствуют целям хозяйствующего субъекта;
- планы контрольной деятельности не согласованы с руководителями структурных подразделений и советом директоров;
- не утвержден механизм ресурсного обеспечения объектов проверки;
- риск-аппетит не пересматривается в зависимости от изменения масштабов хозяйственной деятельности.

Информационные технологии. Федеральный закон «Об информации, информационных технологиях и о защите информации» [2] определяет термин информационные технологии как процесс, использующий совокупность средств и методов сбора, обработки и передачи данных для получения агрегированной информации о состоянии объекта, процесса или явления.

Широкое применение информационных технологий в деятельности хозяйствующих субъектов приводит к усилению незащищенности этих хозяйствующих субъектов от совершения ошибок и фактов мошенничества. Автоматизированная обработка данных, значительные объемы обрабатываемых данных и сложный характер операций способствуют появлению существенных рисков и вероятности материального ущерба. Поэтому общие средства контроля имеют отношение к внутренней среде хозяйствующего субъекта. При этом во внутренних локальных документах должны быть определены и закреплены типы средств контроля. Лучшая мировая практика выработала следующие типы средств контроля:

- проверка разноски;
- проверка перекрестным суммированием;
- проверка нулевого сальдо;
- проверка наличия бумажного следа и др.

Рисками информационных технологий являются:

- отсутствие списка всех ошибок, возникших при прогоне данных через информационную систему;
- отсутствие кодов самодиагностики информационной системы;
- отсутствие контрольных цифр, используемых для верификации данных.

Информационная безопасность. В современном мире обеспечение информационной безопасности является важнейшей задачей любого хозяйствующего субъекта, так как от того, как эффективно работает ИТ-подразделение, во многом зависит успех или проигрыш хозяйствующего субъекта. Таким образом, под информационной безопасностью понимается система мероприятий, направленных на обеспечение сохранения, передачи и защиты любой информации.

Согласно COBIT основными бизнес-процессами в информационной безопасности являются:

- планирование и организация;
- приобретение и внедрение;
- эксплуатация и сопровождение;
- мониторинг и оценка [6].

Сущность самих бизнес-процессов информационной безопасности в рамках данного исследования не рассматривается. Следовательно, рисками процесса обеспечения информационной безопасности являются:

- некорректные планирование и организация информационной безопасности, которые

могут привести к большим затратам и неэффективности информационной безопасности;

- приобретение компьютерной техники с заниженными качественными характеристиками;
- завышенные затраты на эксплуатацию и сопровождение информационной безопасности, что, в конечном счете, пагубно отражается на самой безопасности.

Важно отметить, что лишь применение системного и комплексного подхода в защите информации может обеспечить информационную безопасность.

Таким образом, результатом информационного обмена является процесс получения документов (информации), которые должны обрабатываться, на их основе должны приниматься определенные управленческие решения, последние должны доводиться до ответственных лиц, а действия этих лиц должны контролироваться. При этом такой информационный обмен должен обеспечивать возможность противодействовать любым угрозам и рискам.

Литература

1. Федеральный закон РФ от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов». — URL: https://www.rsl.ru/photo/!_ORS/1-O-BIBLIOTEKE/7-documenty/fz/FZ-77_03072016.pdf (дата обращения: 01.09.2020).

2. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». — URL: https://normativ.kontur.ru/document?moduleId=1&documentId=346863 (дата обращения: 01.09.2020).

3. ГОСТ Р 7.0.8-2013 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения». — URL: http://www.consultant.ru/document/cons_doc_LAW_163800/ (дата обращения: 01.09.2020).

4. Внутренний контроль — Интегрированная модель, Концепция и Приложения», Комитет спонсорских организаций Комиссии Тредуэя (Джерси-Сити, Нью-Джерси: Американский институт дипломированных общественных бухгалтеров, май 2013 г.). — URL: http://www.coso.org (дата обращения: 01.09.2020).

5. Международные профессиональные стандарты внутреннего аудита (Стандарты). — URL: https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20Russian.pdf (дата обращения: 01.09.2020).

6. COBIT (Control Objectives for Information and Related Technologies) version 4.1, 2008. 195 p. ISBN 978-1-60420-290-8.

7. *Кузнецов С.А.* Большой толковый словарь русского языка. — 1-е изд. — СПб.: Норинт, 1998.

FORBES ОПУБЛИКОВАЛ РЕЙТИНГ КРУПНЕЙШИХ ЧАСТНЫХ КОМПАНИЙ РОССИИ

Российское издание журнала Forbes опубликовало обновленный рейтинг 200 крупнейших частных компаний России. Как и годом ранее, его возглавил «Лукойл» — выручка компании за 2019 г. составила 7,841 трлн руб.

На втором месте расположился «Сургутнефтегаз» с выручкой 1,814 трлн руб. Третье место занял ритейлер X5 Retail Group (1,734 трлн руб.), четвертое — «Магнит» (1,369 трлн руб.). Пятерку лидеров замкнула нефтяная компания «Татнефть» с показателем в 932,3 млрд рублей.

В первую десятку также вошли «Новатэк», «Норильский никель», Evraz, ГК «Мегаполис» и НЛМК. Суммарная выручка 200 крупнейших частных компаний в 2019 г. составила 45,3 трлн руб.

Крупнейшим работодателем среди частных компаний России стал ритейлер «Магнит» — в его штате числятся 308,4 тыс. сотрудников. Второе место заняла X5 Retail Group (307 тыс. человек), третье — «Сургутнефтегаз» (почти 113 тыс. сотрудников).

Источник: Rambler News Service
Дата публикации: 18 сентября 2020 г.