

# Внутренний аудит цифровой учетной среды

## Internal Audit of the Digital Accounting Environment

УДК 657.6

DOI: 10.12737/1998-0701-2022-8-1-37-41

**С.А. Варданын**, преподаватель кафедры «Бухгалтерский учет и аудит», ФГБОУ ВО «Волгоградский государственный аграрный университет»

**e-mail:** sv@volgau.com

**Е.С. Шемет**, канд. экон. наук, доцент кафедры «Бухгалтерский учет и аудит», ФГБОУ ВО «Волгоградский государственный аграрный университет»

**e-mail:** shemet\_es@volgau.com

**Е.В. Ягупова**, канд. экон. наук, доцент кафедры «Бухгалтерский учет и аудит», ФГБОУ ВО «Волгоградский государственный аграрный университет»

**e-mail:** yev26@volgau.com

**S.A. Vardanyan**, Lecturer, Department of the Accounting and Audit, Volgograd State Agricultural University

**e-mail:** sv@volgau.com

**E.S. Shemet**, Associate Professor, Department of the Accounting and Audit, Volgograd State Agricultural University

**e-mail:** shemet\_es@volgau.com

**E.V. Yagupova**, Associate Professor, Department of the Accounting and audit, Volgograd State Agricultural University

**e-mail:** yev26@volgau.com

**Аннотация.** В данной статье раскрывается содержание нового объекта внутреннего аудита — цифровой учетной среды, а также вопросы методики организации и проведения внутреннего аудита. Детально представлены элементы внутреннего аудита цифровой учетной среды.

**Ключевые слова:** внутренний аудит, внутренний контроль, компьютерная обработка учетных данных, контрольная среда, цифровая учетная среда.

**Abstract.** This paper presents the content of a new object of internal audit — a digital accounting environment, discloses the issues about methods of organizing and conducting of internal audit. The elements of internal audit of the digital accounting environment are presented in detail.

**Keywords:** internal audit, internal control, computer processing of credentials, control environment, digital accounting environment.

В современных экономических условиях эффективное функционирование хозяйствующих субъектов невозможно без обеспечения контроля над сохранностью имеющихся активов и рациональным использованием ресурсов. Одной из наиболее эффективных, на наш взгляд, форм организации внутреннего контроля в любой компании является внедрение внутреннего аудита. Внутренний аудит обладает широким инструментарием, позволяющим оперативно выявлять ошибки и нарушения в ведении бухгалтерского учета имущества, капиталов и обязательств, своевременно проводить мероприятия для недопущения возникновения краж и хищений имущества, следить за эффективным использованием имеющихся средств и т.д. В отличие от внутренне-

го контроля, результаты работы внутреннего аудита предназначены не столько для руководства компании (хотя и это тоже), сколько для собственников, желающих получать надежную и достоверную информацию о финансовом состоянии компании.

Кроме обеспечения контроля над сохранностью имеющихся активов, компании заинтересованы в расширении возможностей привлечения финансовых средств. Бесспорно, что для привлечения дополнительных инвестиций большую роль может сыграть достоверная финансовая отчетность, подтверждающая стабильное финансовое состояние компании, ее способность обеспечивать сохранность своего имущества и рациональность использования имеющихся средств. В решении

этих задач существенную помощь может оказать внутренний аудит.

При организации внутреннего аудита необходимо учитывать явления и процессы, связанные с ростом масштабов применения во многих сферах цифровых технологий. Не является исключением и бизнес-сфера. По мнению М.В. Беляевой, мир продолжает меняться, и скорость изменений увеличивается. Бесполезно бороться с концепцией всеобщей цифровизации — ее нужно принять и понять, как в нее можно встроиться [2, с. 85].

В современной российской и зарубежной научной литературе выделяют большое количество видов внутреннего аудита, например, внутренний аудит бизнес-процессов, внутренний аудит достоверности финансовой отчетности, внутренний аудит инвестиционных проектов, внутренний экологический, социальный, правовой аудит и др. Однако, анализ различных подходов к определению видов внутреннего аудита показывает, что не уделяется должного внимания состоянию бухгалтерского учета и, соответственно, внутреннего аудита, осуществляемых в условиях цифровой экономики [1, с. 40].

Развитие технологий приводит к внедрению инноваций во всех отраслях экономики [4, с. 39]. При этом, к сожалению, не учитывается тот факт, что за последние 15 лет масштабы использования компьютерной техники в процессе бухгалтерского учета возросли не в разы, а на порядок. Начиная с небольших организаций и заканчивая крупнейшими корпорациями и холдингами — везде бухгалтерский учет основан на использовании различных компьютерных программ для бухгалтерского учета, включая получение, регистрацию, обработку, хранение информации на всех уровнях, начиная со складов, производственных подразделений и заканчивая высшим менеджментом и руководством компаний.

Следует отметить, что современное развитие различных информационных, компьютерных, сетевых технологий, применяемых в бухгалтерском учете, дает широкое поле для деятельности тех сотрудников компаний, у которых есть к ним доступ и корыстные побуждения. Этот фактор должны учитывать собственники компаний, стремящиеся обеспечивать сохранность и рациональное использование ресурсов компании. В целях оперативного получения надежной и по-

лезной информации, предотвращения и недопущения злонамеренных нарушений со стороны лиц, имеющих доступ к различным информационным и компьютерным системам и ресурсам компании, собственникам следует обратить внимание на возможности внутреннего аудита.

В этой связи мы предлагаем внедрять в деятельность компаний новый вид внутреннего аудита — внутренний аудит цифровой учетной среды.

Актуальность предлагаемого вида внутреннего аудита обусловлена тем фактом, что с развитием информационных систем все больше возрастают масштабы применения в бухгалтерском учете систем компьютерной обработки учетных данных (систем КОУД) практически на всех этапах движения информации. Это, в свою очередь, ведет к росту рисков появления случайных ошибок или умышленных искажений при представлении учетной информации. Также не может быть полностью исключена вероятность утечки из организации учетной информации, содержащей элементы коммерческой тайны, например, о размере НИОКР на создание новых видов продукции, или о величине финансовых вложений в высокорисковые инвестиционные портфели, или о планах продаж и т.п. В этой связи на внутренний аудит ложится новая ответственность по контролю за состоянием цифровой экономической безопасности организации.

Цель предлагаемого нового вида внутреннего аудита — поиск и своевременное выявление уязвимых мест в цифровой среде получения, регистрации, обработки, использования и хранения учетной информации.

Основным объектом, на который направлены действия внутреннего аудитора, является цифровая учетная среда (ЦУС). Под ЦУС мы понимаем совокупность различных систем электронного документооборота, через которые осуществляется движение учетных документов.

ЦУС включает пять уровней, при движении «снизу — вверх» эти уровни следующие:

- 1) поступление извне или создание внутри организации первичных документов;
- 2) электронный документооборот с внешними контрагентами;
- 3) обработка учетной документации в системах КОУД;



- 4) составление и предоставление заинтересованным пользователям финансовой отчетности;  
5) хранение и архивирование информации.

На каждом из выделенных нами уровней существуют свои риски появления ошибок или умышленных искажений, на которые должен обращать внимание внутренний аудитор. В первую очередь, внутренний аудитор должен изучить состояние организации ЦУС в целом на предприятии. Далее он проводит проверку надежности и защищенности функционирующих систем КОУД [3, с. 116]. В целях осуществления такой проверки внутренний аудитор должен:

- 1) разработать план проверки;

- 2) осуществить профессиональную оценку состояния системы КОУД;

- 3) провести необходимые процедуры аудита;

- 4) сформулировать рекомендации и предложения, позволяющие устранить обнаруженные недостатки и нарушения.

На основе плана проверки разрабатывается детализированная программа, включающая в себя мероприятия по выявлению и исправлению слабых мест системы КОУД (табл. 1).

При этом информационное обеспечение внутреннего аудита должно позволять проводить проверку различных сфер финансово-хозяйственной деятельности компании на каждом из рассматриваемых уровней ЦУС (рис. 1).

Таблица 1

### Программа проверки систем компьютерной обработки учетных данных

Процедуры проверки	Потенциальные нарушения в системе КОУД
Проверка наличия документов, дающих право использовать программный продукт	Отсутствие документов, дающих право использовать программный продукт
Проверка факта наличия и утверждения в установленном порядке распоряжения руководства о вводе в эксплуатацию какой-либо системы КОУД	Отсутствует распоряжение руководства о вводе в эксплуатацию системы КОУД или оно утверждено не в установленном порядке
Проверка факта наличия и утверждения в установленном порядке распоряжения руководства об определении перечня сотрудников, которым разрешается работать в системе КОУД	Отсутствует распоряжение руководства об определении перечня сотрудников, которым разрешено работать с системой КОУД, или оно утверждено не в установленном порядке
Проверка факта наличия и утверждения в установленном порядке руководством локальных актов, в которых прописаны права, обязанности, уровни допуска сотрудников, допущенных к работе в системе компьютерной обработки данных	Отсутствуют локальные акты, в которых прописаны права, обязанности, уровни допуска сотрудников, допущенных к работе в системе компьютерной обработки данных, или они утверждены не в установленном порядке
Проверка того, является ли эксплуатируемый программный продукт лицензионным	Эксплуатируемый программный продукт является не лицензионным
Проверка наличия возможности регистрации в системе операций «задним числом»	Имеется возможность регистрации операций «задним числом»
Проверка наличия и степени конфиденциальности паролей для работы в системах КОУД	Низкая конфиденциальность либо полное отсутствие применения паролей
Проверка существования плана действий по поддержке программного продукта, его обновлению и восстановлению.	Отсутствует план действий по поддержке программного продукта, его обновлению и восстановлению.
Проверка наличия возможности регистрировать в системе КОУД не получившие разрешения или утверждения руководством операции	Имеется возможность регистрировать в системе КОУД не получившие разрешения или утверждения руководством операции
Анализ уровня квалификации работников, пользующихся программными продуктами системы КОУД при помощи проведения тестирования	Недостаточно высокий уровень квалификации работников

Источник: составлено автором



Рис. 1. Элементы внутреннего аудита  
Источник: разработано автором

Основные риски, вероятные ошибки и нарушения на каждом из уровней ЦУС, действия внутреннего аудитора при проверке параметров ЦУС представлены в табл. 2.

Конечно, говорить сегодня о «полной роботизации» аудита финансовой отчетности, по меньшей мере, недальновидно [5, с. 276].

### Заключение

Организация эффективного контроля над движением учетной информацией является сегодня одной из важнейших задач управления. Недостаточное внимание к данной проблеме может привести к серьезным экономическим потерям для хозяйствующих субъектов. Для того, чтобы уменьшить риск возникнове-

Таблица 2

### Элементы внутреннего аудита цифровой учетной среды

Уровень ЦУС	Вероятные ошибки	Вероятные нарушения	Действия аудитора по контролю	Источники информации
1	2	3	4	5
Уровень поступления извне или создания внутри организации первичных документов	Ошибочное / неполное заполнение реквизитов в первичных документах; арифметические ошибки	Несвоевременное оформление первичных документов; несвоевременная передача документов в бухгалтерию; документ подписан лицом, не обладающим правом подписи; отправка документов с личной электронной почты сотрудника, а не с корпоративной	Провести сверку первичного документа с учетным регистром, отправить запрос о сверке контрагенту	Первичные документы, учетные регистры, внутренние регламенты, запросы контрагентам и третьим лицам
Уровень электронного документооборота с внешними контрагентами	Отправка документов по ошибочным адресам	отправка документов с личной электронной почты сотрудника, а не корпоративной; отсутствия системы подтверждения взаимного документооборота с контрагентами	Провести сверку электронных реквизитов контрагента с данными документов, отправить запрос о сверке контрагенту	Первичные документы, учетные регистры, внутренние регламенты, запросы контрагентам и третьим лицам
Уровень движения электронной учетной документации в системах КОУД бухгалтерии	Передача информации, содержащей коммерческую тайну, по открытым каналам (общие папки, «облако», сетевой диск и т.п.)	Отсутствие внутренних регламентов, определяющих права доступа к системам КОУД бухгалтерии; отсутствие персональных учетных данных с паролями для каждого работника; возможность переноса информации, содержащей коммерческую тайну, на внешние носители	Провести сверку регламентных прав сотрудников с фактическими правами	Первичные документы, учетные регистры, внутренние регламенты, запросы контрагентам и третьим лицам



Окончани табл. 2

1	2	3	4	5
Уровень составления и представления заинтересованным пользователям финансовой отчетности	Неправильные переносы остатков с одного отчетного периода на другой; неправильное закрытие счетов в системе; неправильное применение даты отражения операции и др.	Доступ к редактированию финансовой отчетности лиц, не обладающих таким правом; передача финансовой отчетности, содержащей коммерческую тайну, третьим лицам	Проверить защищенность мест хранения электронной документации и финансовой отчетности, убедиться в отсутствии свободного доступа к этим местам	Первичные документы, учетные регистры, внутренние регламенты, запросы контрагентам и третьим лицам
Уровень хранения и архивирования информации	Хранение документов вне систематизированной структуры	Отсутствие внутреннего регламента, определяющего порядок передачи документов в архив, перечень ответственных лиц	Проверить порядок хранения электронных документов и их передачи в архив / уничтожения	Первичные документы, учетные регистры, внутренние регламенты

ния ошибок, нарушений, утечки информации в цифровой учетной среде компании, включающей системы компьютерной обработки

учетных данных, представляется целесообразным организовать и проводить в организации внутренний аудит цифровой учетной среды.

### Литература

1. Азарская М.А. Развитие методического обеспечения аудита в условиях цифровой экономики // В сборнике: Цифровая экономика и современное общество. Сборник материалов I Международной научно-практической конференции. — 2018. — С. 39–43.
2. Беляева М.В. Организационно-экономические алгоритмы цифрового аудита и цифрового контроллинга в системе управления крупными промышленными предприятиями / М.В. Беляева, Ю.В. Ляскова // Вестник МИРБИС. — 2019. — № 1 (17). — С. 85–89.
3. Варданян С.А. Организационное обеспечение внедрения информационных систем во внутренний аудит // Развитие АПК на основе принципов рационального природопользования и применения конвергентных технологий: Материалы международного научно-практического форума, посвященного 75-летию образования Волгоградского государственного аграрного университета, 30 января — 01 февраля 2019 г., г. Волгоград. Том 4. — Волгоград: Волгоградский ГАУ, 2019. — С. 115–121.
4. Залевская М.А. Цифровая трансформация внутреннего аудита / М.А. Залевская, О.Н. Галюта // Управление экономическими системами: электронный научный журнал. — 2018. — № 11 (117). — С. 39.
5. Кочинев Ю.Ю. Развитие аудита в условиях цифровой экономики // В сборнике: Развитие финансовых отношений в период становления цифровой экономики: Материалы II Международной научно-практической конференции / Под научной редакцией А.Ю. Румянцевой. — 2019. — С. 274–278.
6. Лазаренко Т.А. Задачи внутреннего аудита в условиях цифровой экономики // В сборнике: Проблемы эффективности и безопасности функционирования сложных технических и информационных систем. сборник статей Международной научно-практической конференции. — 2017. — С. 70–73.