Риски и возможности цифровизации учетно-контрольных процессов в субъектах малого предпринимательства

Risks and Opportunities of Digitalization of Accounting and Control Processes in Small Businesses

УДК 657.1

DOI: 10.12737/1998-0701-2024-10-8-31-37

Н. Калпакчи, главный бухгалтер ООО «ЕВА Групп»

e-mail: natasha96n@mail.ru

N. Kalpakchi, Chief Accountant, EVA Group LLC

e-mail: natasha96n@mail.ru

Аннотация. *В статье представлена идентификация рисков цифровизации учетно-контрольных процессов в субъектах малого предпринимательства. Исследование последствий наступления рисков безопасности данных при использования цифровых инструментов, а также проведенный сравнительный анализ рисков цифровизации учетно-контрольных процессов в малых и крупных предприятиях позволили разработать предложения по минимизации рисков безопасности данных в субъектах малого предпринимательства при цифровизации их учетно-контрольных процессов.*

Ключевые слова: субъекты малого предпринимательства, учетно-контрольные процессы, цифровизация, риски цифровизации, цифровые инструменты.

Abstract. *The article presents the identification of risks of digitalization of accounting and control processes in small business entities. The study of the consequences of the occurrence of data security risks when using digital tools, as well as a comparative analysis of the risks of digitalization of accounting and control processes in small and large enterprises allowed us to develop proposals to minimize the risks of data security in small businesses when digitalizing their accounting and control processes.*

Keywords: small business entities, accounting and control processes, digitalization, risks of digitalization, digital tools.

Цифровая трансформация определена как одна из национальных целей развития Российской Федерации [1]. В качестве индикатора реализации этой цели выделено достижение «цифровой зрелости» ключевых отраслей экономики. В связи с этим утверждена национальная программа «Цифровая экономика», одной из целей которой является доступность новых цифровых сервисов для снижения издержек, развития бизнеса и формирования конкуренции [2]. Достижение заявленной цели предполагается до конца 2024 г.

Цифровизация предпринимательства на основе повсеместного применения цифровых технологий направлена на обеспечение конкурентоспособности российской экономики и улучшение условий ведения предпринимательской деятельности [3].

В настоящее время цифровые технологии широко применяются в предпринимательской деятельности, они используются субъектами предпринимательства для взаимодействия с государственными органами, иными внешними контрагентами и для оптимизации бизнес-процессов [4], в том числе учетно-контрольных.

В профессиональном стандарте «Бухгалтер» умение пользоваться компьютерными программами для ведения бухгалтерского учета, а также информационными и справочно-правовыми системами, оргтехникой при осуществлении указанного вида профессиональной деятельности определено в качестве одного из необходимых [5]. Что касается главного бухгалтера, то он должен уметь разрабатывать предложения по интегрированию информационной системы бухгалтерского учета в информационную систему экономического субъекта. В Стандарте указано, что бухгалтер должен знать [5]:

- порядок обмена информацией по телекоммуникационным каналам связи;
- современные технологии автоматизированной обработки информации;

- компьютерные программы для ведения бухгалтерского учета;
- правила защиты информации.

К минимальным цифровым инструментам, которые используются в настоящее время всеми организациями, относятся следующие:

- телекоммуникационные каналы связи для обмена информацией;
- автоматизированная обработка информации (например, обработка платежных документов при загрузке банковской выписки в учетную программу, автоматическое формирование товарных накладных в учетной программе на основе заказов на сайте компании, дополнительные обработки по загрузке кассовых чеков в учетную программу и формирование соответствующих записей на счетах бухгалтерского учета и т.п.);
- программы для ведения бухгалтерского учета.

Большинство организаций для автоматизации процессов и повышения эффективности работы также используют системы электронного документооборота, онлайн-банкинг и электронные платежные системы, облачные хранилища данных, а также автоматизированные системы отчетности [6]. Применение цифровых инструментов при осуществлении учетно-контрольных процессов позволяет:

- сократить время на обработку информации (автоматизация рутинных процессов учета и контроля сокращает время работы персонала и позволяет ему сконцентрироваться на более сложных бухгалтерских процедурах, таких как выбор целесообразного метода учета для обеспечения достоверности, применение профессионального суждения при формировании оценочных значений и т.д.);
- повысить достоверность данных (использование цифровых инструментов приводит к уменьшению количества ошибок и улучшению качества данных, поскольку они обрабатываются автоматически);
- обеспечить быстрый доступ к релевантной информации, тем самым быстрее реагировать на изменения в бизнес-среде;
- повысить качество принимаемых решений на основе более обширной и своевременной информации благодаря возможности в режиме реального времени отслеживать данные и получать сигналы при сильных отклонениях таких данных от норм или средних значений;
- автоматизировать составление отчетов.

Наряду с перечисленными неоспоримыми преимуществами цифровизация учетно-контрольных процессов является причиной возникновения ряда серьезных рисков, связанных прежде всего с безопасностью данных (табл. 1).

Таким образом, для минимизации рисков цифровизации вышеизложенные риски обусловливают целесообразность принятия комплексного подхода к безопасности данных, включая регулярное обновление политик безопасности, обучение персонала, использование шифрования данных.

Также важно отметить, что описанные риски и направления их минимизации характерны как для крупного, так и для малого бизнеса. В то же время отличительные особенности малых предприятий по сравнению с крупны-

Таблица 1

Последствия наступления рисков безопасности данных при использовании цифровых инструментов и меры для их минимизации

Риски безопасности данных при использования цифровых инструментов	Последствия наступления риска	Меры для минимизации рисков использования цифровых инструментов
Утеря данных	Утеря данных вследствие сбоя систем, атак злоумышленников или естественного бедствия	Создание регулярных резервных копий данных и их хранение в защищенных местах
Законодательные требования в области защиты данных	Несоблюдение этих требований может привести к юридическим последствиям, штрафам и утрате доверия со стороны клиентов	Следование всем применимым законам и стандартам безопасности данных

Окончание табл. 1

Риски безопасности данных при использования цифровых инструментов	**Последствия наступления риска**	**Меры для минимизации рисков использования цифровых инструментов**
Внутренние угрозы	Несанкционированный доступ сотрудников к данным, нарушение коммерческой тайны	Ограничение доступа к конфиденциальной информации, регулярное обновление списка сотрудников для доступа, применение принципа «минимальных привилегий» для снижения риска компрометации информации
Кибератаки и вредоносное ПО	Кража данных, вымогательство, отказ в обслуживании и другие негативным последствиям	Шифрования данных, установка систем мониторинга для отслеживания подозрительной активности и быстрого реагирования на потенциальные угрозы
Отсутствие обновлений программного обеспечения	Недостаточные меры безопасности могут оставить систему уязвимой к атакам и утечкам данных	Регулярное обновление операционных систем, антивирусного программного обеспечения и других приложений до последних версий с тем, чтобы устранить уязвимости и обеспечить защиту от новых угроз
Социальная инженерия, фишинговые письма	Обман пользователей или сотрудников для получения доступа к защищенным данным	Требования к устанавливаемым паролям, двухфакторная аутентификация, проведение обучающих курсов и тренингов по безопасности информации для сотрудников в целях повышения осведомленности о потенциальных угрозах и действий для их предотвращения
Утечка данных в облаке	Хранение данных в облачных сервисах может привести к риску утечки данных из-за нарушения безопасности самого облачного провайдера или ошибок конфигурации со стороны пользователей	Приобретение цифровых инструментов только у проверенных и надежных поставщиков с хорошей репутацией в области безопасности информации (важно проводить дополнительные исследования и обеспечивать контроль за безопасностью продуктов перед их внедрением в компании и регулярно актуализировать информацию о поставщике после внедрения)
Неправильно настроенная система использования электронных подписей	Компрометация использования электронных подписей	Предоставление доступа к ключам подписи только ограниченному перечню сотрудников и обучение их правилам безопасности

Источник: составлено автором по материалам [7–10].

ми обусловливают появление как преимуществ при внедрении цифровых инструментов в учетно-контрольные процессы, так и предопределяют появление специфических для малых предприятий рисков (табл. 2).

Отличия в процессе цифровизации учетно-контрольных процессов между малыми и крупными компаниями проистекают из различий в масштабе операций, специализированных потребностей, доступных ресурсов и различий в организационной структуре.

В субъектах малого предпринимательства также важно применять комплексный подход к безопасности данных. В табл. 3 представлены шаги, необходимые для минимизации рисков в сфере безопасности данных.

Таким образом, для оптимизации учетно-контрольных процессов в субъектах малого предпринимательства путем их цифровизации необходимо оценивать существующие риски, регулярно осуществлять действия для предупреждения или минимизации неблагоприятных событий, мониторить изменения внешней и внутренней среды и актуализировать мероприятия по минимизации рисков.

Отдельное внимание стоит уделить рискам, возникающим из-за недобросовестных дей-

Таблица 2

Особенности цифровизации учетно-контрольных процессов в организациях малого бизнеса

Критерий	Значение в крупных организациях	Значение в организациях малого бизнеса	Возможности для цифровизации учетно-контрольных процессов в организациях малого бизнеса	Препятствия для цифровизации учетно-контрольных процессов в организациях малого бизнеса
Масштаб операций и объем данных	Сложные и объемные учетные операции с большим количеством транзакций и данных	Простые и менее объемные учетные операции и массивы данных	Доступны более простые и экономичные решения, такие как программы для учета и отчетности в облаке или интегрированные онлайн-сервисы	Операции с низкими объемами данных или редко встречающиеся продолжают осуществляться без автоматизации процесса ввиду низкой отдачи от затрат на цифровизацию таких процессов
Специализированные потребности	Имеют более специализированные потребности в учете, связанные с налогообложением, международной деятельностью, сложными финансовыми инструментами и т.п.	Более общие и менее специализированные потребности	Использование более простых и универсальных инструментов цифровизации, которые стоят недорого и внедряются быстро, нет затрат на обеспечение поддержки программ и обучение персонала, нет потребностей в более специализированных программных и аппаратных решениях	Компания становится заложником универсальных цифровых решений, приходится подстраивать процессы под существующие цифровые решения
Бюджет и ресурсы	Большие бюджеты и ресурсы	Ограниченный бюджет и ресурсы	Внедрение и поддержка цифровых инструментов входит в стоимость низкобюджетных цифровых решений	Небольшая вариативность инструментов цифровизации, которые могут быть доступны при ограниченном бюджете
Сложность организационной структуры	Более сложная организационная структура с множеством подразделений, филиалов и дочерних компаний	Имеют более простую организационную структуру	Упрощается процесс цифровизации и внедрения учетных систем, чаще нет потребности в более сложных решениях для интеграции и совместной работы между различными подразделениями организации	Некоторые процессы взаимодействия внутри компании невозможно привести в цифровизированный вариант

Источник: составлено автором.

ствий сотрудников. В условиях цифровизации ввиду наличия больших объемов данных и средств для быстрой передачи информации могут встречаться такие действия со стороны сотрудников организации, как использование рабочего времени не для исполнения трудовых функций, корректировка учетных данных, иные мошеннические действия.

Для минимизации данного рода рисков предлагается использовать «журнал аудита», то есть специальный файл или базу данных, где записываются события и действия, происходящие в информационной системе или сети: изменения конфигурации, попытки входа в систему, обращения к ресурсам и другие события, которые могут быть важными для безопасности и целостности системы.

Журнал аудита предоставляет возможность анализировать и отслеживать активность в системе, выявлять аномалии, обнаруживать потенциальные угрозы безопасности и проводить расследования инцидентов. Эти записи могут

быть использованы для соблюдения нормативных требований, аудита системы, расследования инцидентов безопасности и обеспечения юридической ответственности.

Обычно журнал аудита включает в себя информацию о времени события, типе события, идентификаторе пользователя или системы и других сведениях, необходимых для полного описания произошедшего события. Эти записи могут храниться в течение определенного периода времени в соответствии с политиками безопасности и стандартами организации.

Стоимость реализации может варьировать в зависимости от нескольких факторов: размеров организации, ее инфраструктуры, требований к безопасности, выбранных техно-

Таблица 3

Последовательность действий по минимизации рисков безопасности данных в субъектах малого предпринимательства

№	Наименование этапа	Содержание	Необходимые меры контроля
1	Оценка рисков	Проведение анализа рисков поможет выявить уязвимости и определить наиболее вероятные угрозы для организации. На основе этой оценки можно разработать план действий по обеспечению безопасности.	Фиксация возможных рисков и планов действий по минимизации
2	Обучение персонала	Обучение сотрудников основам кибербезопасности поможет им распознавать потенциальные угрозы и правильно реагировать на них, что является ключевым элементом защиты от социальной инженерии и других видов атак.	Определение круга лиц, нуждающихся в повышении квалификации, с указанием периодичности ее проведения
3	Использование антивирусного ПО и брандмауэров	Установка и регулярное обновление антивирусного программного обеспечения и брандмауэров на все устройства, используемые для работы с учетными данными, регулярное обновление ПО для защиты от вредоносных программ	Определение круга лиц, отвечающих за установку ПО, и периодичности обновлений для каждого ПО
4	Регулярное резервное копирование данных	Регулярное создание резервных копий данных и их хранение в безопасном месте поможет минимизировать потерю данных в случае кибератаки, аппаратных сбоев или других чрезвычайных ситуаций	Определение круга лиц, отвечающих за создание резервных копий, периодичности их создания, мест хранения копий
5	Шифрование данных	Шифрование конфиденциальных данных в покое и в передаче помогает защитить информацию от несанкционированного доступа даже в случае ее утечки или кражи. Все данные, передаваемые между клиентскими приложениями и сервером, должны быть зашифрованы с использованием надежных протоколов шифрования (например, SSL/TLS)	Определение круга лиц, отвечающих за шифрование и кодирование данных, мест их хранения, разработка регламента получения доступа к ним
6	Мониторинг и регистрация событий	Внедрение систем мониторинга и регистрации событий позволяет отслеживать и анализировать активность в сети и на компьютерах, выявлять аномалии и потенциальные угрозы безопасности	Определение круга лиц, отвечающих за мониторинг и регистрацию событий, фиксация показателей, действий и норм отклонений для отнесения их к угрозам безопасности
7	Регулярное аудирование систем безопасности	Проведение регулярных проверок и аудитов систем безопасности для выявления возможных уязвимых мест и составления мероприятий реагирования на них	Определение круга лиц, отвечающих за аудирование, периодичности его проведения
8	Актуализация программного обеспечения	Регулярное обновление программного обеспечения и операционных систем помогает устранить уязвимости, которые могут быть использованы злоумышленниками для атак	Определение круга лиц, отвечающих за актуализацию ПО

Источник: составлено автором.

логий и решений. Для малых предприятий с ограниченным бюджетом можно предложить следующие более доступные варианты реализации журнала аудита.

1. Использование бесплатных или открытых инструментов (например, Logstash, Graylog, ELK Stack (Elasticsearch, Logstash, Kibana).

2. Использование облачных сервисов для сбора данных в журнале аудита (Splunk Cloud, Sumo Logic, Loggly) может быть более экономически выгодным вариантом, поскольку не требует приобретения и поддержки собственной инфраструктуры.

3. Применение простых и недорогих решений для мониторинга и регистрации событий (например, Windows Event Viewer для операционной системы Windows).

4. Выбор тех решений, которые легко интегрируются с уже существующей инфраструктурой предприятия, с тем, чтобы минимизировать затраты на внедрение и поддержку.

Эти подходы позволят малым предприятиям реализовать журнал аудита с ограниченными бюджетными ресурсами, обеспечивая при этом необходимый уровень безопасности и соответствие нормативным требованиям.

Для 1С, наиболее часто используемой бухгалтерской программы, можно использовать следующие способы реализации журнала аудита с ограниченным бюджетом:

- встроенные средства (платформа 1С имеет встроенные средства, позволяющие регистрировать время и пользователя, изменившего данные, доступ к объектам и выполнение операций);
- дополнительные модули (некоторые модули и конфигурации для 1С предоставляют расширенные возможности аудита и мониторинга. Например, 1С. Управление активами предприятия. включает в себя функциональность аудита изменений;
- настройка интеграции с системами мониторинга, такими как Zabbix, Nagios или Prometheus, для сбора данных о работе программы, доступах пользователей и других событиях;
- создание пользовательских скриптов и обработок для регистрации необходимых событий и записи их в журнал аудита (более гибкий и специализированный способ);
- использование возможностей журналирования операционной системы (можно отслеживать с помощью журналов операционной системы доступ к файлам и папкам на компьютере, а также к сетевым ресурсам; успешные и неуспешные попытки входа в программы; сетевые запросы; информацию о запущенных процессах, их завершении и других системных операциях; о системных ошибках, предупреждениях и критических событиях, которые могут указывать на проблемы с работой системы или наличие вредоносного программного обеспечения).

Что касается объемов данных, которые могут генерироваться таким журналом, то они могут сильно варьировать в зависимости от интенсивности использования программы 1С, числа пользователей, типов событий и настроек регистрации. Обычно журнал событий операционной системы и программы 1С может генерировать относительно небольшие объемы данных, но при интенсивном использовании и большом числе пользователей объемы могут быть значительными. В любом случае резервирование достаточного места для хранения данных и оптимизация их анализа могут помочь управлять объемами данных.

Заключение

Таким образом, специфические особенности малых субъектов предпринимательства обусловливают необходимость имплементации мер по минимизации рисков цифровизации в учетно-контрольные процессы. Реализацию мероприятий по минимизации рисков цифровизации, осуществляемых в целом по организации, должны отслеживать работники учетной сферы, в том числе для получения достаточной уверенности в том, что компания будет продолжать деятельность в обозримом будущем.

Литература

1. Указ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» / СПС КонсультантПлюс — URL: https://www.consultant.ru/document/cons_doc_LAW_357927/ (дата обр. 24.04.2024).

2. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации — URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обр. 24.04.2024).

3. Постановление Правительства РФ от 07.09.2018 № 1065 (ред. от 18.12.2023) «О Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности» (вместе с «Положением о Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности») (ред. от 06.06.2024)/ СПС КонсультантПлюс — URL:https://www.consultant.ru/document/cons_doc_LAW_306391/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обр. 24.06.2024).

4. *Гришкина С.Н., Калпакчи Н.* Цифровизация учетно-контрольных процессов в организациях малого бизнеса как фактор повышения их информационной прозрачности // Аудитор. — 2023. — Т. 9, № 9. — С. 41–47. — DOI 10.12737/1998-0701-2023-9-9-41-47.

5. Приказ Минтруда России от 21.02.2019 № 103н «Об утверждении профессионального стандарта «Бухгалтер» (Зарегистрировано в Минюсте России 25.03.2019 № 54154).

6. *Гришкина С. Н., Калпакчи Н.* Влияние пандемии на цифровизацию учетных процедур в субъектах малого предпринимательства // Аудитор. — 2022. — Т. 8, № 3. — С. 38–43. — DOI 10.12737/1998-0701-2022-8-3-38-43.

7. *Щербакова Е. П., Азалиева М.А.* Организация бухгалтерского учета с применением облачных технологий в программе «1С: бухгалтерия» в малом бизнесе // Вестник ИПБ (Вестник профессиональных бухгалтеров). — 2023. — № 1. — С. 18–23. — DOI 10.51760/2308-9407_2023_1_18.

8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» / СПС КонсультантПлюс — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обр. 24.04.2024).

9. *Калпакчи Н.* Документооборот в субъектах малого предпринимательства: трансформация в условиях цифровизации // Экономика и управление: проблемы, решения. — 2023. — Т. 1, № 9 (139). — С. 195–200. — DOI 10.36871/ek.up.p.r.2023.09.01.022.

10. Цифровые технологии в российских компаниях, КПМГ, 2019. — URL: https://assets. kpmg/content/dam/kpmg/ru/pdf/2019/01/ru-ru-digital-technologies-in-russian-companies. Pdf (дата обр. 24.04.2024).

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕНЕЖНО-КРЕДИТНОЙ ПОЛИТИКИ: ЦБ РФ ПРЕДСТАВИЛ ПРОЕКТ НА 2025–2027 ГОДЫ

Банк России сформулировал цель и принципы денежно-кредитной политики, а также представил базовый и 3 альтернативных сценария развития экономики на ближайшие 3 года. Во всех них предполагается возвращение инфляции к 4%.

Базовый сценарий предполагает, что уже в 2025 году инфляция снизится до 4–4,5%, затем она стабилизируется вблизи 4%. Для этого ЦБ будет поддерживать жесткие денежно-кредитные условия, в том числе высокую ключевую ставку. Средняя ключевая ставка в 2024 году составит 16,9–17,4%, в 2025 году — 14–16%, в 2026 году — 10–11%. К 2027 году она снизится до 7,5–8,5%.

Дезинфляционный сценарий позитивнее. При нем регулятор сможет быстрее снизить ключевую ставку. Предполагается, что средняя ключевая ставка в 2025 году будет 12–14%, в 2026 году — 9–10%. В 2027 году, как и в базовом сценарии, она составит 7,5–8,5%.

В проинфляционном сценарии возможно усиление давления на инфляцию. ЦБ начнет проводить еще более жесткую денежно-кредитную политику. Ключевая ставка в 2025 году составит 16–18%, в 2026 году — 11,5–12,5%, а к 2027 она снизится до 8,5–9,5%.

В рисковом сценарии значительно ухудшаются внешние условия. Регулятор допустил возникновение дисбаланса на финрынках развитых стран, который приведет к мировому финансовому кризису в 2025 году. Инфляция вырастет до 13–15%, ключевая ставка составит 20–22%.

https://www.consultant.ru/legalnews/26224/
29 августа 2024 г.