УДК 657.1.011.56

ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ БУХГАТЕРСКОГО УЧЕТА И ПУТИ ИХ РЕШЕНИЯ

Е.И. Пушкин, 3 курс
Научный руководитель – **Ю.Е. Климова,** ст. преподаватель
Белорусский государственный университет пищевых и химических технологий

Цифровизация бухгалтерского учета и аудита в Республике Беларусь – это процесс перехода от традиционных форм ведения и контроля учетной информации к современным электронным средствам и технологиям.

В Республике Беларусь цифровизация бухгалтерского учета и аудита находится на стадии развития и совершенствования. Существует ряд нормативных актов, регулирующих использование электронных документов, электронно-цифровой подписи, электронного документооборота в сфере учета и аудита.

Существует государственная программа “Цифровое развитие Беларуси” на 2021-2025 годы. Одним из направлений программы цифровизации бухгалтерского учета и аудита в Республике Беларусь является создание единой бухгалтерской информационной сети, которая позволит обеспечить взаимодействие всех участников учетного процесса – организаций, государственных органов, налоговых инспекций, аудиторских фирм, банков и т.д. – посредством электронных документов, обладающих юридической силой и защищенных от подделки и несанкционированного доступа. Такая сеть способна повысить оперативность, достоверность и полноту предоставления учетной информации, а также сократить издержки на ее подготовку и проверку.

Использование IT в бухгалтерском учете, анализе и аудите актуально по следующим причинам: 1. Эффективность: автоматизация учетных процессов сокращает время выполнения задач и снижает вероятность ошибок. 2. Точность: компьютерные программы обеспечивают высокую точность расчетов, исключая ошибки, связанные с человеческим фактором. 3. Обработка больших объемов данных: IT-системы позволяют обрабатывать и анализировать огромные массивы информации, что повышает качество принимаемых решений. 4. Взаимодействие с другими системами: интеграция с другими IT-системами и облачными сервисами обеспечивает централизованный доступ к информации и упрощает совместную работу. 5. Соблюдение законодательства: IT-решения облегчают соблюдение требований законодательства, обеспечивая актуальность и полноту дан-

ных. 6. Безопасность: современные IT-системы предоставляют средства защиты информации от несанкционированного доступа и потери данных. 7. Гибкость и масштабируемость: IT-решения позволяют адаптироваться к изменяющимся бизнес-потребностям и росту компании.

Однако использование ITтехнологий имеет ряд существенных недостатков:

1. Потеря данных. Любое прерывание обслуживания, вызванное неисправностью компьютера или отключением электроэнергии, влияющее на бизнес, зависящий от программного обеспечения для бухгалтерского учета, может привести к сбоям в работе. Перебои в работе могут ограничить как доступ к сохраненной информации, так и ввод новой информации. Финансовые данные также могут быть потеряны в результате сбоя компьютера, если их резервное копирование не выполнено надлежащим образом.

2. Неточная информация. Данные системы бухгалтерского учета настолько надежны, насколько надежны данные, которые в нее вводятся. Финансовые результаты могут быть ошибочными, если будут проверены все входные данные, поскольку большинство систем бухгалтерского учета предполагают ввод данных вручную. Выявить неточную информацию может быть непросто, если существует склонность оценивать окончательные отчеты или выходные данные системы бухгалтерского учета.

3. Конфигурация системы. У каждой компании есть отличительные особенности, которые могут затруднить настройку универсального программного обеспечения для ведения бухгалтерского учета в соответствии с ее требованиями. Многие приложения допускают настройку; однако, если все сделано неправильно, это может привести к простою и ошибкам. Кроме того, если бизнес расширяется, может возникнуть необходимость в смене бухгалтерских программ; это может привести к значительным перерывам в работе, поскольку необходимо передавать информацию, а сотрудникам требуется новое обучение.

4. Стоимость. Расходы, связанные с использованием бухгалтерского программного обеспечения, являются недостатком. В дополнение к первоначальной стоимости программного обеспечения существуют расходы, связанные с обслуживанием, модификацией, обучением и компьютерным оборудованием.

5. Мошенничество и кибербезопасность. Информация, хранящаяся в электронном виде, может быть доступна, изменена и использована не по назначению, если не приняты надлежащие меры контроля и безопасности. Должны быть предусмотрены определенные полномочия для обеспечения того, чтобы только уполномоченные лица использовали бухгалтерское программное обеспечение и имели доступ к отчетам. Бухгалтерское программное обеспечение увеличивает риск мошенничества, поскольку финансовые данные могут быть конфиденциальными.

В наше время встает вопрос о кибербезопасности в цифровом бухгалтерском учете. Цифровая архитектура должна быть настроена, организована и подключена таким образом, чтобы обеспечить как безопасность, так и работоспособность.

Существует ряд мер, которые помогут снизить потери информации, риски взлома или несанкционированного доступа:

1. Резервные копии. Резервное копирование гарантирует, что данные и информация хранятся в облаке и регулярно создаются резервные копии. Виртуализация позволяет получить доступ к резервным копиям за считанные минуты в случае кибератаки или другой проблемы.

2. Безопасность электронной почты. Все чаще бизнес ведется по электронной почте. Однако электронная почта также является основным источником фишинговых атак, во время которых хакеры рассылают поддельные электронные письма, часто с призывом к срочным действиям. Когда ничего не подозревающий читатель нажимает на ссылку или прикрепленный файл, он может спровоцировать кибератаку, которая внедряет файлы в устройства и сети, которые могут быть активированы позже для кражи файлов или отключения систем. Чтобы защитить электронную почту, нужно обучить сотрудников и использовать программное обеспечение для защиты от вредоносных программ, фишинга, спама и фильтрации контента, чтобы предотвратить попадание вредоносного контента в электронную почту.

3. Пароли и аутентификация. В бухгалтерской фирме должна действовать строгая политика в отношении паролей. Регулярная смена паролей включающих цифры, специальные символы, а также заглавные и строчные буквы. Рекомендации по длине и сложности имеют первостепенное значение.

4. Шифрование. Шифрование гарантирует, что данные защищены от внешних воздействий. Как правило, бухгалтерские фирмы уделяют особое внимание шифрованию передаваемых данных, например, используя зашифрованные системы электронной почты.

5. Средства контроля доступа. Убедитесь, что у вас есть всеобъемлющая и хорошо спланированная стратегия управления доступом. Предоставляйте доступ к системам и информации только тем, кто абсолютно обязан иметь доступ к этой информации, в зависимости от роли, группы или должности. Убедитесь, что в руководстве по доступу также указано, что делать, когда кто-то покидает организацию.

6.Обучение сотрудников. Сотрудники — это первая линия обороны. Убедитесь, что они знают, как выявлять проблемы ИТ-безопасности и сообщать о них, а также помогают обезопасить вашу бухгалтерскую фирму от потенциальных атак.

У всего есть недостатки, и бухгалтерское программное обеспечение не исключение. Если вы владелец малого бизнеса, у вас может не быть достаточно средств для использования программного обеспечения для ведения бухгалтерского учета. Однако, если компания становится больше и начинает расти, возможно, пришло время подумать о том, какое программное обеспечение для бухгалтерского учета может помочь вести дела более эффективно и точно.

Одним из самых простых шагов, которые следует предпринять, чтобы повысить безопасность фирмы, является инвестирование в систему управления бухгалтерской практикой, которая изначально включает в себя множество функций кибербезопасности, а также обучение сотрудников базовым навыкам киберзащиты.