В данной модели в графе «логистика до WB и др. расходы» рассчитывается процент транспортных расходов от селлера до сортировочного центра. Он может рассчитываться прямым методом, но, если данные затраты незначительны, тогда можно прибегнуть к коэффициентам, как в данной модели. В графе «логистика WB в бел. руб.» указано стоимостное значение данных затрат.

Исходя из вышеизложенного можно сделать вывод, что логистические затраты при работе через онлайн платформы имеют большое значение. Анализ и расчет данного вида затрат может помочь при выборе схемы работы, а также рационального использования денежных средств на логистику.

Список использованных источников

1. Об утверждении Инструкции по бухгалтерскому учету доходов и расходов и признании утратившими силу некоторых постановлений Министерства финансов Республики Беларусь и их отдельных структурных элементов [Электронный ресурс]: пост. Мин-ва финансов Респ. Беларусь, 30 сент. 2011 г. № 102. – Режим доступа: https://pravo.by – Дата доступа: 01.01.2024.

2. Караева, Е. Д. Планирование логистических затрат при реализации товаров через маркетплейс [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/planirovanie-logisticheskih-zatrat-pri-realizatsii-tovarov-cherez-marketpleys/ viewer. – Дата доступа: 01.01.2024 г.

3. Что нужно знать о логистических затратах на маркетплейсах [Электронный ресурс]. – Режим доступа: https://betapro.ru/blog/chto-nuzhno-znat-o-logisticheskih-zatratah-na-marketplejsah/. – Дата доступа: 01.01.2024 г.

УДК 657

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ БУХГАЛТЕРА

Богдан М. П.
Прудникова А. Н., м. э. н.
Барановичский государственный университет, г. Барановичи, Республика Беларусь

Аннотация. *Раскрывается важность знаний и навыков кибербезопасности в деятельности бухгалтера. При выполнении своих трудовых обязанностей работники бухгалтерии должны владеть способами защиты информации от различных кибеугроз. Бухгалтерский учет и безопасность в цифровом мире неразрывно связаны, бухгалтерам необходимы системы кибербезопасности и планы управления рисками, которые будут защищать их от некоторых рисков кибератак и утечки данных.*

Ключевые слова: *кибербезопасность, киберугрозы, бухгалтер, цифровые угрозы, риски, информационные технологии.*

CYBERSECURITY FOR ACCOUNTANT

Bogdan M. P.
Prudnikova A. N., M. Econ.
Baranovichi State University, Baranovichi, Republic of Belarus

Annotation. *The importance of cybersecurity knowledge and skills in the activities of an accountant is revealed. When performing their job duties, accounting employees must know how to protect information from various cyber threats. Accounting and security go hand in hand in the digital world, and accountants need cybersecurity systems and risk management plans that will protect them from some of the risks of cyber attacks and data breaches.*

Keywords: *cybersecurity, cyberthreats, accountant, digital threats, risks, information technology.*

Кибератаки становятся серьезной проблемой XXI века, глобальным вызовом всему обществу, несущим реальные угрозы и риски как для государства, так и для отдельно взятого субъекта. Вредоносные вмешательства в информационные системы субъектов хозяйствования могут парализовать целые отрасли, причинить вред многим организациям. В связи с этим Республика Беларусь не может оставаться безучастной и вынуждена на всех уровнях выстраивать защитные механизмы по обеспечению информационной безопасности государства и общества.

В настоящее время процессы информатизации и обеспечения безопасности имеют существенное значение в деятельности бухгалтера, поэтому тематика кибербезопасности для него является очень актуальной, поскольку данные работники при выполнении своих трудовых функций в области бухгалтерского учета должны обладать соответствующими знаниями и навыками, позволяющими обеспечить защиту экономической информации при ее обработке.

Цель исследования — обосновать важность соблюдения бухгалтерами основных принципов кибербезопасности в связи с возникновением новых цифровых угроз и рисков как на уровне отдельных субъектов хозяйствования, так и на уровне государства в целом. Основой исследования стали научные труды и публикации зарубежных, белорусских и российских авторов, нормативные правовые акты акты, статьи периодической печати, информация интернет-ресурсов [1–8]. Исследование публикаций в области исследуемой темы позволяет сделать вывод о том, что тема является актуальной, практически значимой, поскольку бухгалтеры при выполнении трудовых функций в современных условиях бизнес-среды должны обеспечивать исполнение мер, направленных на реагирование на риски информационной безопасности по защите информации и обеспечению кибербезопасности.

Умение работать с объемными информационными массивами и анализировать большие потоки инфоромации в условиях обеспечения информационной безопасности — один из основных профессиональных навыков бухгалтера [5, с. 172].

Существуют различные походы к определению кибербезопасности, но в основном под кибербезопасностью подразумевают набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от потенциальных цифровых угроз. К киберпреступлениям относят несанкционированный доступ к информации, неправомерное завладение ей, разработку, использование либо распространение вредоносных программ, клевету, оскорбление, шпионаж и др. [1–4].

Одним из самых распространенных видов киберпреступлений является мошенничество и хищение денежных средств. В целом следует констатировать, что в последнее время количество киберугроз стремительно увеличивается на фоне роста цифровой экономики и геополитической напряженности [3].

Поскольку вопрос кибербезопасности касается каждой организации, у которой есть доступ в Интернет, возникла необходимость мгновенного реагирования на различные цифровые угрозы как на уровне отдельных субъектов хозяйствования, так и на уровне государства в целом. Ключевым драйвером белорусского рынка кибербезопасности являются законодательные изменения. Так, 14 февраля 2023 года Президент Республики Беларусь Александр Лукашенко подписал соответствующий указ [6]. Указ № 40 «О кибербезопасности» взаимосвязан с Концепцией информационной безопасности и направлен на дальнейшую реализацию ее положений. Таким образом, среди глобальных целей Республики Беларусь — формирование системы кибербезопасности, конкретизация функций и задач государственных органов и иных организаций является одной из главных задач государства на сегодняшний день.

В век информационных технологий соблюдение кибергигиены является необходимым условием практически во всех сферах деятельности человека. В Республике Беларусь

регулярно выявляются случаи кибератак на различные белорусские организации и на этом фоне растут и их расходы на усовершенствование системы кибербезопасности [3; 8].

Бухгалтерия занимает особое место среди целей хакеров. Ведь именно она причастна к информации, которая больше всего ценится. Это же, в свою очередь, делает бухгалтеров главной целью киберпреступников. Также особо уязвимы и организации, оказывающие бухгалтерские услуги, к нападению киберворов, ведь им клиенты предоставляют важную информацию, а взлом может нанести огромный вред клиентам, а также погубить репутацию организации, оказывающей бухгалтерские услуги.

Почему же кибербезопасность бухгалтерского учета должна стоять в центре внимания? Во-первых, потому что практически все организации используют специализированное программное обеспечение для ведения бухгалтерского учета и, по данным Следственного комитета Республики Беларусь, вирусы-шифровальщики чаще всего атакуют корпоративный бизнес. Цель таких атак – получить выкуп за разблокировку сведений, хранящихся в бухгалтерии 1С, архивах. Хакеры пользуются небрежным отношением сотрудников к информационной безопасности (например, сотрудники на рабочих компьютерах открывают вложения, замаскированные под письма из налоговой, при этом антивирусы у них часто отключены).

Во-вторых, сейчас идет тенденция к хранению информации в облаке, и бухгалтеры не проходят мимо всемирного тренда, ведь это удобно. Хоть хранение информации в облаке и облегчило доступность к данным бухгалтерского учета, оно также создало больше угроз, чем записи в обычной бумажной книге. Угрозы данным бухгалтерского учета обходятся дорого. Ведь кроме взлома, зачастую происходит и утечка информации, которую устранить еще сложнее. Украденные бухгалтерские данные обычно включают в себя номера счетов, детали транзакции, номера кредитных карт, банковские счета, имена пользователей, пароли, личную и конфиденциальную информацию.

Поскольку данные бухгалтерского учета являются столь желанной целью киберпреступников, возникает вопрос, можно ли объединить кибербезопасность и бухгалтерскую деятельность? Ответ положителен, поскольку сектор кибербезопасности создает все более усовершенствованные программы и инструменты для защиты конфиденциальной информации. А как же бухгалтер может помочь усовершенствованию методов киберзащиты? В связи с этим появляется новое ответвление бухгалтерской деятельности. Например, уже выделяют так называемых бухгалтеров-криминалистов, которых обучают разбираться в данных, анализировать системы и процессы, а также исследовать технологии, используемые организациями. Эти навыки делают бухгалтеров-криминалистов высококвалифицированными специалистами для расследований киберпреступлений. Бухгалтеры-криминалисты чаще всего работают с командой по кибербезопасности для расследований и составления отчетов финансовых потерь от кибератак. Финансовый опыт и умение анализировать данные помогают таким специалистам преобразовывать сложную информацию и снижать риски цифровых угроз.

Киберпреступления являются всемирной угрозой и нужно принимать во внимание основные советы, способные помочь, в том числе и бухгалтерам, не допускать утечки информации. Для этого необходимо:

– применять надежные пароли. К этому пункту относится несколько подпунктов. Например, всегда можно включать двухуровневую аутентификацию и с помощью этого усложнить задачу взлома. Нельзя использовать одинаковый пароль в разных местах, поскольку злоумышленникам создаются условия для получения доступа ко всем данным. В целом, необходимо чаще менять пароли, хотя бы раз в пару месяцев;

– использовать лицензированные средства защиты. При этом не следует соблазняться бесплатными версиями таких программ, ведь при скачивании бесплатной антивирусной программы возникает риск скачать и сам вирус;

– делать резервные копии документов. Ни одно электронное устройство не застраховано от внезапной остановки, в связи с этим теряются данные, которые не удалось

сохранить. Поэтому стоит копировать данные на переносимые носители, стоит использовать программы, которые делают это автоматически;

– обучать работников, в частности, работников бухгалтерии, кибербезопасности. Также стоит разрабатывать политику кибербезопасности организации и повышать уровень знаний в этой области;

– рассмотреть возможность перевода бухгалтерии на удаленные сервера, так называемые дата-центры, которые подходят для хранения информации. Еще одним плюсом этого является то, что на сервер можно зайти откуда угодно, даже если вы взяли работу на дом или в поездку [1–4; 7].

Таким образом, кибербезопасность играет важную роль в современном мире бухгалтерии. Поддержание безопасности данных и информационных систем стало неотъемлемой частью профессиональной ответственности бухгалтеров. В свете постоянно возрастающих угроз кибербезопасност, бухгалтерам необходимо быть готовыми к применению соответствующих мер предосторожности, чтобы защитить финансовую информацию своих организаций и клиентов. Обучение работников бухгалтерии, установка современных систем защиты, регулярный аудит и осведомленность о последних тенденциях в области кибербезопасности – все это является ключевыми компонентами эффективной стратегии защиты данных работниками бухгалтерии. Развитие навыков в области кибербезопасности поможет бухгалтерам не только защитить финансовые интересы своих организаций, но и поддержать доверие своих клиентов и партнеров.

Мировой опыт свидетельствует, что крупнейшими проблемами использования эффективных средств борьбы с киберугрозами сегодня являются сложности их внедрения и интеграции, нехватка соответствующих специалистов (низкий уровень осознания ими проблем кибербезопасности), финансовых ресурсов, эффективных решений на рынке, поддержки со стороны системы руководства организаций.

Система киберзащиты бухгалтерской информации – это комплекс мероприятий как на государственном уровне, так и на уровне отдельного субъекта хозяйствования, призванных гарантировать защиту бухгалтерской информации, как и автоматизированной системы ведения бухгалтерского учета в целом, от киберугроз. Одной из основных сложностей при борьбе с киберугрозами является и то, что, по данным различных источников, около 70 % организаций сегодня не имеют четкого плана реагирования на возможные опасности.

Таким образом, сейчас в мире киберберугрозам подвергается значительная часть организаций, причем независимо от их размера и вида деятельности. Для минимизации негативного влияния киберугроз необходима комплексная система общих и специфических мероприятий организационного, технического, кадрового и юридического характера, что актуализирует необходимость дальнейших исследований, в том числе направленных на поиск критериев и оценки успешности внедрения мероприятий по защите бухгалтерской информации и обеспечения ее кибербезопасности.

Список использованных источников

1. Accounting Cybersecurity: How To Keep Financial Data Secure And Safe [Electronic resource]. – Mode of access: https://www.accountingseed.com/resource/blog/accounting-cybersecurity-how-to-keep-financial-data-secure-and-safe/. – Date of access: 03.12.2023.

2. Cybersecurity for Accountant [Electronic resource]. – Mode of access: https://travasecurity.com/learn-with-trava/articles/cybersecurity-for-accountants. – Date of access: 03.12.2023.

3. Где хакеры находят уязвимости у компаний и как противостоять кибератакам [Электронный ресурс]. – Режим доступа: https://ilex.by/news/gde-hakery-nahodyat-uyazvimosti-u-kompanij-i-kak-protivostoyat-kiberatakam/. – Дата доступа: 03.12.2023.

4. Кибербезопасность в бухгалтерии и не только [Электронный ресурс]. – Режим доступа: https://buhta.com/kz/blog/post/cybersecurity-93. – Дата доступа: 03.12.2023.

5. Лопухов, В. М. Анализ требований профессионального стандарта «бухгалтер» к уровню грамотности по информационной безопасности / В. М. Лопухов // Алтайский вестник Финуниверситета. – 2016. – № 1. – С. 169–172.

6. О кибербезопасности [Электронный ресурс] : Указ Президента Респ. Беларусь, 14 фев. 2023 г. № 40 // Нац. правовой Интернет-портал Респ. Беларусь. – 15.02.2023. – 1/20733.

7. Роль бухгалтера в обеспечении кибербезопасности [Электронный ресурс]. – Режим доступа: https://ru.rup.ee/bukhgalterskie-novosti/anonsy/rol-bukhgaltera-v-obespechenii-kiberbezopas nosti. – Дата доступа: 03.12.2023.

8. Юркова, А. Ю. Кибербезопасность и защита бухгалтерских данных в условиях применения современных информационных технологий / А. Ю. Юркова, Н. И. Белодед // Импортозамещение, научно-техническая и экономическая безопасность : сб. ст. V Междунар. научн.-технич. конф. «Минские научные чтения-2022», в 3 т., Минск, 7–9 дек. 2022 г.; Т. 2. – Минск : БГТУ, 2022. – С. 399–403.

УДК 338

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОПЛАТЫ ТРУДА В ОРГАНИЗАЦИЯХ МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА И ПРОДОВОЛЬСТВИЯ

Казимирская А. Н.
Лебедева С. О., к. э. н., доцент
Белорусский государственный экономический университет, г. Минск, Республика Беларусь

Аннотация. *В статье рассматриваются проблемы системы оплаты труда в бюджетных организациях, на примере ветеринарной лаборатории. Особое внимание уделяется структуре заработной платы, а именно, окладу, компенсирующим и стимулирующим выплатам, совершенствованию оплаты труда при помощи модернизированной тарифной сетки в бюджетных организациях.*

Ключевые слова: *бюджетная организация, заработная плата, оклад, тарифная сетка, базовая ставка.*

IMPROVING THE REMUNERATION SYSTEM IN ORGANIZATIONS OF THE MINISTRY OF AGRICULTURE AND FOOD

Kazimirskaya A. N.
Lebedeva S. O., PhD, Associate Professor
Belarusian State University of Economics, Minsk, Republic of Belarus

Annotation. *The article discusses the problems of the wage system in budgetary organizations, using the example of a veterinary laboratory. Special attention is paid to the structure of wages, namely salaries, compensatory and incentive payments, and the improvement of wages, with the help of a modernized tariff grid in budget organizations.*

Keywords: *budget organization, salary, salary, tariff schedule, base rate.*

Бюджетные организации по сравнению с организациями реального и финансового сектора экономики функционируют с учетом большого количества особенностей, а именно, осуществляют свою финансово-хозяйственную деятельность в полном соответствии с утвержденными бюджетными сметами и сметами доходов и расходов внебюджетных средств; для большинства организаций функционирование осуществляется преимущественно за счет бюджетных ассигнований; ведут бухгалтерский учет в соответствии с планом счетов для бюджетных организаций; имеют существенные отличия в порядке формирования фонда оплаты труда.

Бюджетные организации выполняют различные функции и подчиняются различным министерствам, поэтому при планировании, анализе и контроле различных аспектов их деятельности необходимо учитывать особенности каждого вида непроизводственной сферы.