УДК 657

БУХГАЛТЕРСКИЙ УЧЕТ В ЭПОХУ КИБЕРУГРОЗ: ВЫЗОВЫ И РЕШЕНИЯ

Сак А. Г., Сафроненко В. И.
Дорошкевич Н. М., к. э. н., доцент
Белорусский государственный экономический университет, Минск, Республика Беларусь

Аннотация. *В условиях стремительного развития информационных технологий кибератаки становятся все более изощренными, что делает защиту бухгалтерских данных критически важной задачей. В статье рассматриваются основные виды угроз и акцентируется внимание на необходимости внедрения комплексных мер защиты. В заключение подчеркивается важность формирования культуры кибербезопасности и разработки стратегий, направленных на минимизацию рисков, связанных с киберугрозами в бухгалтерском учете.*

Ключевые слова: *киберугрозы, защита данных, фишинг, риски, бухгалтерский учет, анализ угроз, хакеры.*

ACCOUNTING IN THE ERA OF CYBER THREATS: CHALLENGES AND SOLUTIONS

Sak A. G., Safronenko V. I.
Doroshkevich N. M., Ph. D., Associate Professor
Belarusian State Economic University, Minsk, Republic of Belarus

Annotation. *In the context of the rapid development of information technology, cyberattacks are becoming more sophisticated, which makes the protection of accounting data a critical task. The article discusses the main types of threats and focuses on the need to implement comprehensive protection measures. It concludes by emphasizing the importance of building a culture of cybersecurity and developing strategies to minimize the risks posed by cyber threats in accounting.*

Keywords: *cyber threats, data protection, phishing, risks, accounting, threat analysis, hackers.*

В современном мире, где технологии развиваются с небывалыми темпами, бухгалтерский учет сталкивается с новыми вызовами, связанными с киберугрозами. Переход на цифровые платформы и автоматизация бухгалтерских процессов значительно повысили эффективность работы, однако они также сделали финансовую информацию более уязвимой для различных видов атак.

С каждым годом наблюдается значительный рост числа кибератак на организации различных секторов. Бухгалтерия, как хранилище конфиденциальной финансовой информации, становится одной из главных мишеней для злоумышленников. Утечки данных могут привести к серьезным финансовым потерям и ущербу репутации, что делает защиту бухгалтерских систем приоритетной задачей.

Киберугрозы, такие как фишинг, вредоносное программное обеспечение и атаки на сети, представляют собой серьезные риски для организаций всех размеров. Утечка конфиденциальной информации или манипуляция с данными может привести не только к финансовым потерям, но и к серьезным репутационным последствиям.

Информация о всех аспектах хозяйственной деятельности предприятия, формируемая в системе бухгалтерского учета, обладает высокой ценностью и является основой его устойчивости, развития и эффективности, при условии надежной защиты.

Тем не менее, полная автоматизация, затронувшая и бухгалтерский учет с внедрением современных технологий и программ, хотя и имеет свои неоспоримые преимущества, создает риски утечек информации, хакерских атак, взломов информационных систем и различных форм мошенничества. Все данные, обрабатываемые и хранящиеся в цифровом формате, становятся уязвимыми. В таких условиях ключевым становится обеспечение кибербезопасности предприятия.

Цель данной статьи – рассмотреть ключевые вызовы, с которыми сталкивается бухгалтерский учет в эпоху киберугроз, а также возможные решения для повышения безопасности и устойчивости финансовых процессов.

Киберугрозы в бухгалтерском учете представляют собой риски, связанные с использованием цифровых технологий и информационных систем для управления финансовыми данными. Они могут проявляться в различных формах.

Один из самых распространенных методов киберугроз – это фишинг. Он нацелен на получение конфиденциальной информации, например, логины, пароли и финансовые данные. Хакеры могут быстро получить доступ к ряду конфиденциальной информации, когда будут иметь доступ к учетным данным бухгалтера. Огромным количеством информации владеют специалисты в области бухгалтерского учета.

Так какие типы информации могут быть необходимы для хакеров?

1. Адрес, номер телефона, дата рождения – это стандартные поля в формах 1040, захватывая существующие данные, хакеры могут создавать фиктивные учетные записи.

2. Номер социального страхования клиента может понадобиться хакерам, чтобы была возможность оформить кредитную карту или же взломать банковские счета клиента.

3. Медицинские записи сейчас являются самой высокооплачиваемой при обмене украденной информацией.

4. Финансовые отчеты и финансовые документы на конец года имеют номера счетов клиентов.

5. Адрес электронной почты – самый частый случай, когда через процедуру «забыли пароль» можно получить доступ к банковским и биржевым счетам [1].

Еще одна не менее опасная угроза, которая может привести к серьезным финансовым потерям и юридическим последствиям для организации – это изменение данных. Неправильные данные могут привести к ошибкам в финансовых отчетах, что может повлечь за собой неверные решения управленцев и впоследствии серьезные финансовые потери, например, в результате неправомерных платежей. А также серьезными последствиями изменения данных мошенниками являются возможные штрафы и санкции за искажение отчетности или нарушение законов о защите данных. Нельзя не учитывать риск заражения системы вирусами вредоносными программами, которые могут модифицировать бухгалтерские записи или создавать ложные документы.

Взлом бухгалтерской системы представляет собой серьезную угрозу для репутации организации. Утечка конфиденциальной информации о клиентах и сотрудниках может повлечь за собой негативные последствия. Например, в случае взлома может произойти утрата доверия, что приведет к потере клиентов и снижению доходов. Партнеры и поставщики могут поменять мнение о организации, которая подверглась кибератакам, и пересмотреть свои отношения с ней, разорвав контракты. Так как инциденты, связанные с киберугрозами, часто становятся новостями, то публикации в средствах массовой информации могут значительно подорвать деловую репутацию компании. Даже после устранения последствий после кибератак, восстановление репутации может занять много времени и ресурсов, поэтому организация может столкнуться с трудностями в привлечении новых клиентов и партнеров.

К следующему негативному последствию можно отнести эксплуатацию уязвимостей в системах бухучета. Злоумышленники используют слабые места в программном обеспечении или недостатки в процессах для получения несанкционированного доступа к данным. Например, ошибки в коде или конфигурации бухгалтерских систем могут позволить обойти системы безопасности. Использование устаревших систем и программ, которые не получают обновлений безопасности, приводит к уязвимости для атак.

Бухгалтерские системы могут стать недоступными для сотрудников в результате DDoS (Distributed Denial of Service) атак – это тип кибератаки, при котором хакеры пытаются перегрузить сервер или сеть, делая их недоступными для пользователей. Мошенники используют множество скомпрометированных устройств (ботнетов), чтобы отправлять огромное количество запросов к серверу, перегружая его. Такие атаки могут быть нацелены на конкретные приложения, например, веб-интерфейсы бухгалтерского ПО, чтобы истощить ресурсы и вызвать сбои. В результате простоя в работе может привести к потере дохода и дополнительных затрат на восстановление систем.

Наиболее защищенными от киберугроз на предприятиях являются веб-сайты и веб-приложения, серверы (физические и виртуальные) и хранилища данных, а менее всего – ноутбуки и мобильные устройства [2, с. 50].

Рассмотренные киберугрозы в бухгалтерском учете подчеркивают необходимость внедрения эффективных мер защиты.

1. Обучение сотрудников – регулярные тренинги по кибербезопасности помогут повысить знания в области рисков. Ограничение прав доступа к бухгалтерским системам только для необходимых сотрудников позволяет повысить уровень безопасности данных и минимизировать риск несанкционированного доступа к конфиденциальной информации.

2. Использование шифрования – можно защитить конфиденциальную информацию при помощи шифрования данных и парольной политики.

3. Следует регулярно обновлять программное обеспечение для устранения уязвимости, устанавливать системы мониторинга, которые могут выявлять аномалии в трафике и запускать автоматические меры защиты.

4. Мониторинг подозрительной активности и проведение регулярных проверок систем безопасности для выявления и устранения уязвимостей.

5. Регулярное создание резервных копий данных и их хранение в защищенном месте для восстановления в случае атаки.

Анализ киберугроз в бухгалтерском учете подчеркивает важность внедрения комплексной стратегии защиты данных. Перечисленные инициативы не только укрепляют защиту конфиденциальной информации, но и формируют культуру безопасности в организации. Таким образом, организациям следует воспринимать кибербезопасность как неотъемлемую часть своей стратегии управления рисками, что позволит обеспечить стабильность и безопасность бухгалтерского учета в условиях растущих киберугроз.

К сожалению, киберпреступность развивается вместе с технологиями, что усложняет выявление и противодействие этим незаконным действиям. Важно осознавать, что риск кибератак представляет собой проблему не только для государства, но и для каждого отдельного предприятия.

Хотя достичь абсолютной безопасности защиты учетных данных невозможно, индивидуальная ответственность каждого сотрудника бухгалтерской службы является ключевым фактором в защите ценной информации. Поэтому каждое предприятие должно разработать программу действий, направленную на создание киберзащиты бухгалтерских данных, которая охватывает как человеческие ресурсы, так и технологические аспекты.

Перспективой для дальнейших исследований может стать анализ угроз и современных инструментов поддержки кибербезопасности в сфере бухгалтерской информации.

Список использованных источников

1. Why hackers want your personal information – and how to protect it [Electronic resource] // F-Secure. – Mode of access: https://www.f-secure.com/en/articles/why-do-hackers-want-your-personal-information (date of access: 06.12.2024).

2. Cyberthreat Defense Report // CyberEdge Group. Annapolis: CyberEdge Group. – 2019. – P. 50.

УДК 657.3

СОВЕРШЕНСТВОВАНИЕ УЧЕТНОЙ ПОЛИТИКИ В СТРАТЕГИИ РАЗВИТИЯ ОРГАНИЗАЦИЙ РЕСПУБЛИКИ БЕЛАРУСЬ

Мурашко Д. А.
Гридюшко Е. Н., к. э. н., доцент
Белорусская государственная сельскохозяйственная академия, Горки, Республика Беларусь

Аннотация. *Статья посвящена экономическому значению учетной политики, ее влиянию на принятие управленческих решений и повышение конкурентоспособности предприятий. Анализируются текущие проблемы учетной политики в Беларуси, выявляемые в ходе аудиторских проверок, такие как несоответствие законодательству, недостаточная методология учета, изменения в учетной политике в течение года и использование*