УДК 657.1.011.56

А.Ю. Юркова, Н.И. Белодед
Академия управления при Президенте Республики Беларусь
Минск, Беларусь

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА БУХГАЛТЕРСКИХ ДАННЫХ В УСЛОВИЯХ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. *Кибербезопасность также известна как безопасность информационных технологий. Быстрое развитие информационных технологий и их последующее внедрение в ведение бухгалтерского учета поставили под угрозу безопасность учетных данных и вывели на передний план проблемы определения мероприятий по повышению их кибербезопасности.*

A.Yu. Yurkova, N.I. Beloded
Academy of Public Administration under the aegis of President
of the Republic of Belarus
Minsk, Belarus

CYBERSECURITY AND PROTECTION OF ACCOUNTING DATA IN THE CONTEXT OF THE USE OF MODERN INFORMATION TECHNOLOGIES

Abstract. *Cybersecurity is also known as information technology security. The rapid development of information technologies and their introduction into accounting have jeopardized the security of accounting data and brought to the fore the problems of determining measures to improve their cybersecurity.*

Целью данной статьи является выявление современного состояния безопасности информационных технологий, а также распознание киберугроз в сфере использования бухгалтерской информации. Основная задача – основываясь на анализе статистических данных, опубликованных в отечественных и иностранных исследованиях, описать состояние кибербезопасности, основные источники киберугроз для учетной информации на предприятии, определить системы мер обеспечения кибербезопасности бухгалтерской информации на предприятии.

Стремительное развитие информационных технологий, которое началось в конце XX-начале XX1 веков, способствовало их внедрению практически во все сферы человеческой жизнедеятельности и массовому (часто даже неконтролируемом) использованию, а также формированию единого информационного и цифрового пространства. При этом быстрыми темпами возросла и количество злоупотреблений,

правонарушений и других киберугроз, направленных на различные аспекты деятельности предприятий, которые функционируют в каждом из этих пространств.

Информация обо всех фактах хозяйственной деятельности предприятия, которая формируется в системе бухгалтерского учета, характеризуется высокой степенью ценности и является залогом устойчивости, развития и эффективности деятельности такого предприятия, но только при условии надежной защиты. Однако тотальная автоматизация, которая не обошла и сферу бухгалтерского учета и предусматривает внедрение специализированных современных технологий и программ для его ведение, несмотря на неоспоримые преимущества, ставит под угрозу утечки информации, хакерских атак, взлома информационных сетей, различного рода мошенничества и тому подобное все учетные данные, которые обрабатываются и сохраняются в цифровой среде. На первый план при таких условий получается обеспечение предприятием особого вида безопасности информации-кибербезопасности.

В рамках данной статьи рассмотрим кибербезопасность лишь в сфере защиты бухгалтерской информации, которая не просто хранится на отдельном компьютере пользователя, а циркулирует в киберпространстве – среде, состоящей из информационных систем по всему миру, включая сети, которые сочетают эти системы.

В процессе опроса работников, занимающихся безопасностью информационных технологий, проведенного CyberEdge Group, выявлено, что в 2019 г. в среднем 78% киберугроз были удачными (около 63% всех предприятий подверглись таким угрозам [1]), причем странами-лидерами в этом контексте выступили Испания (93,7%), Саудовская Аравия (91,5%) и Колумбия (87,9%). Источниками основной опасности есть вредоносные программы, фишинговые атаки, программы-вымогатели, злоупотребления, связанные с учетными записями пользователей (в т. ч. кража личных данных), отказами в обслуживании (DoS/DDoS-атаки), атаки на веб-приложения, спам, ботнеты, нарушение данных, инсайдерские угрозы, физические манипуляции (повреждение, похищение, потеря данных), утечка информации, криптоджекинг (новый вид угроз, который заключается в несанкционированном использовании чужого компьютера для добычи криптовалюты), кибершпионаж и др., а поставщиками средств киберзащиты по состоянию на второй квартал 2018 г. – Cisco, Palo Alto Networks, Fortinet, Check Point [2].

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 [3].

Отметим, что для формирования эффективной системы мер по минимизации киберугроз и адекватной защиты бухгалтерской информации прежде всего следует определиться с пониманием понятия «угроза» и производной от угрозы – киберугроза, под которой в контексте данной статьи предполагается имеющееся или потенциальное событие, которое несет опасность участникам киберпространства в сфере функционирования системы бухгалтерского учета, приводит к потере, повреждению, уничтожению или несанкционированному использованию учетной информации.

Следуя мировым тенденциям, бухгалтерский учет в большинстве отечественных предприятий поддается автоматизации с использованием таких современных инструментов и технологий, как блокчейн, облачные и туманные технологии, искусственный интеллект, мобильные вычисления, машинное обучение и прочее. Каждая из упомянутых характеризуется специфическими рисками для учетной информации, являющейся следствием сущности и особенностей функционирования той или иной технологии. Например, при использовании мобильных устройств для ведения учета специфическими рисками будут: плохая осведомленность и культура использования устройств, их потеря и хищение; неспособность сетевых инженеров быстро ликвидировать уязвимости; приобретение мобильного устройства с заранее установленным вредоносным программным обеспечением (каждый 36-й мобильное устройство подвергается такой угрозе [4]); проблемы взаимодействия с другими программами и тому подобное.

Облачные технологии ведения бухгалтерского учета и представления отчетности тоже не вполне безопасны. Специфическими угрозами для учетной информации здесь могут стать: невозможность использования предыдущих версий программного обеспечения, высокая зависимость от качества предоставления услуг провайдерами, неуверенность относительно приватности и права собственности на данные в облаке (нехватка соответствующей законодательной защиты прав на информацию в облачной среде), сложности идентификации источника угроз и тому подобное.

Говоря о технологии блокчейн, которой пророчат большое будущее в бухгалтерском учете и аудите, специфическими угрозами для информации, обусловленными особенностями этой технологии, является низкий уровень приватности и конфиденциальности данных о деятельность предприятия, отсутствие законодательно утвержденного

ответственного лица за ведение распределенной базы данных об операциях, перегрузке устройств хранения информацией как следствие неотвратимого роста ее объемов и тому подобное.

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 менеджмента предприятия, постоянное совершенствование способов выполнения вредоносных действий и тому подобное [3].

Отметим, что больше всего средств на кибербезопасность сегодня выделяют компании Мексики (15,9% от ИТ-бюджета), Бразилии (15,9%) и Южной Африки (14,9%) [3].

Система киберзащиты бухгалтерской информации – это комплекс мероприятий на государственном уровне и на уровне отдельного предприятия, призванных гарантировать защиту такой информации, как и автоматизированной системы ведения бухгалтерского учета на предприятии в целом, от киберугроз.

Наконец отметим, что одной из основных сложностей при борьбе с киберугрозами является то, что, по данным Telstra, 78% компаний сегодня не имеют четкого плана реагирования на возможные опасности [7, p. 9]. Для защиты от киберугроз предприятия чаще всего используют сетевые антивирусы (63,9%), контроль доступа к сети (59,8%), SSL/TLS устройства (платформы) для дешифрования (59,4%) и системы обнаружения (предотвращения) вторжений [3]. Как вариант рассматривается также передача отдельных функций защиты информации (тестирование проникновений, анализ угроз, мониторинг сетевой безопасности в режиме реального времени и др.) на аутсорсинг.

Таким образом, результаты данной статьи свидетельствуют, что сейчас в мире киберберугрозам подвергается значительная часть предприятий, причем независимо от их размера и вида деятельности. Для минимизации негативного влияния киберугроз предлагается комплексная система общих и специфических мероприятий организационного, технического, кадрового и юридического характера. При этом критерии оценки успешности внедрение этих мероприятий-направление наших дальнейших исследований.

Перспективами дальнейших исследований в данном направлении могут быть: поиск критериев и оценка успешности внедрения мероприятий по защите бухгалтерской информации и обеспечения её кибербезопасности.

Список использованных источников

1. Summary Report / Telstra Security Report 2019. Paddington: Telstra Corporation Limited, 2019. 20 p.

2. No Clear Leader in Cybersecurity Market [Электронный ресурс]. – Режим доступа: https://www.statista.com/chart/16651/cybersecurity-global-market/. – Дата доступа: 10.10.2022.

3. 2019 Cyberthreat Defense Report / CyberEdge Group. Annapolis: CyberEdge Group, 2019. 50 p.

4. . Internet Security Threat Report / Symantec. Mountain View: Symantec Corporation, 2019. 61 p.

УДК 681.3:553.98(574.4)

А.А. Овезова, К.Р. Аннамухаммедов,
К.Ш. Чарыев, А.Р. Аннаева
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ПРОГРАММА ЭЛЕКТРОННОГО ДОКУМЕНТА СОТРУДНИКА

Аннотация. *В статье рассматриваются разработка программного обеспечения автоматизированной системы электронной информации о гражданине и работнике. Созданная программа позволяет управлять множеством данной документации и в кратчайшие сроки создать необходимый электронный документ согласно установленного образца на основе базы данных, собранной в программе.*

A.A. Ovezova, K.R. Annamuhammedov,
K.S. Charyyev, A.R.Annayeva
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

EMPLOYEE ELECTRONIC DOCUMENT PROGRAM

Abstract. *The article deals with the development of software for an automated system of electronic information about a citizen and an employee. The created program allows you to manage a lot of this documentation and create the necessary electronic document in the shortest possible time according to the established sample based on the database collected in the program.*