УДК 336:657.37

В. В. Башкатов
Кубанский государственный аграрный университет им. И.Т. Трубилина, Краснодар,
e-mail: bashkatov.v@kubsau.ru

В. Е. Литун
Кубанский государственный аграрный университет им. И.Т. Трубилина, Краснодар,
e-mail: evdoha.litun03@gmail.com

О. Д. Вендина
Кубанский государственный аграрный университет им. И.Т. Трубилина, Краснодар,
e-mail: olgadv1605@gmail.com

КИБЕРБЕЗОПАСНОСТЬ В БУХГАЛТЕРИИ: ВАЖНОСТЬ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ КИБЕРАТАК И СПОСОБЫ ЕЁ ОБЕСПЕЧЕНИЯ

Ключевые слова: бухгалтерский учет, кибербезопасность, хакерство, конфиденциальность, организация, цифровизация.

В современном мире цифровых финансов взаимосвязь бухгалтерского учета и кибербезопасности приобретает все большее значение. В этой статье подчеркивается необходимость защиты конфиденциальной информации в системах бухгалтерского учета от киберугроз и излагаются стратегии обеспечения надежной защиты. Учитывая сложность и разнообразие киберугроз, рекомендуется применять целостный подход к обеспечению информационной безопасности. Этот подход включает в себя не только технологические меры предосторожности, но и политику организации, обучение сотрудников и проактивное управление рисками. Особое внимание уделяется выявлению уязвимостей и внедрению эффективных средств контроля для предотвращения потенциальных нарушений. Применяя комплексные меры кибербезопасности и превентивные стратегии, организации могут снизить риски, укрепить доверие и обеспечить целостность финансовых данных во все более цифровой среде.

V. V. Bashkatov
Kuban State Agrarian University named after. I.T. Trubilina, Krasnodar,
e-mail: bashkatov.v@kubsau.ru

V. E. Litun
Kuban State Agrarian University named after. I.T. Trubilina, Krasnodar,
e-mail: evdoha.litun03@gmail.com

O. D. Vendina
Kuban State Agrarian University named after. I.T. Trubilina, Krasnodar,
e-mail: olgadv1605@gmail.com

CYBERSECURITY IN ACCOUNTING: THE IMPORTANCE OF PROTECTING CONFIDENTIAL INFORMATION FROM CYBER ATTACKS AND HOW TO ENSURE IT

Keywords: accounting, cybersecurity, hacking, confidentiality, organization, digitalization.

In the modern world of digital finance, the relationship between accounting and cybersecurity is becoming increasingly important. This article highlights the need to protect confidential information in accounting systems from cyber threats and outlines strategies to ensure reliable protection. Given the complexity and diversity of cyber threats, it is recommended to apply a holistic approach to information security. This approach includes not only technological precautions, but also organizational policies, employee training, and proactive risk management. Special attention is paid to identifying vulnerabilities and implementing effective controls to prevent potential violations. By applying comprehensive cybersecurity measures and preventive strategies, organizations can reduce risks, build trust and ensure the integrity of financial data in an increasingly digital environment.

Быстрое внедрение цифровых технологий предприятиями подчеркивает растущую важность кибербезопасности как фундаментального аспекта управления рисками. Эта тенденция повысила осведомленность общественности о киберугрозах и связанных с ними проблемах. Организации, ставшие объектами кибератак, подвержены значительному долгосрочному финансовому ущербу и испорченной репутации. Недавние опросы показывают, что кибербезопасность становится основной проблемой, связанной с рисками, для бизнеса и общества в целом.

Кибератаки часто нацелены на специалистов по бухгалтерскому учету, чтобы получить доступ к конфиденциальной информации путем компрометации их учетных данных и проникновения в системы. Такая целенаправленность в первую очередь обусловлена привилегированным доступом бухгалтеров к конфиденциальным данным клиентов, которые имеют большое значение в даркнете. На рисунке 1 представлена классификация угроз корпоративной информационной безопасности в секторе бухгалтерского учета.

Утечка данных имеет серьезные последствия для бизнеса, включая финансовые, репутационные и экономические последствия, некоторые из которых могут быть серьезными. Эксперты утверждают, что утрата всего 20% коммерческой тайны организации может привести к банкротству. Аналогичным образом, компрометация даже 5% конфиденциальных данных может привести к потере организацией статуса лидера рынка.

Программный комплекс «1С: Предприятие» является неотъемлемой частью процесса цифровизации бухгалтерских процессов. На рисунке 2 представлен обзор российского рынка информационных систем бухгалтерского учета.

Во-первых, «1С:Предприятие» сохраняет значительную долю рынка в 38,5%, что отражает широкое признание и доверие среди российских предприятий.

Во-вторых, Buhsoft, занимающая заметную долю рынка в 17,7%, становится серьезным конкурентом, что свидетельствует о конкурентной среде, в которой альтернативные решения набирают обороты.

Несмотря на то, что рыночные доли Microsoft Dynamics AX и аналогичных конкурентов колеблются от 5,4% до 6,2%, эти компании продолжают предоставлять разнообразные функциональные возможности, отвечающие различным требованиям бизнеса. По состоянию на 2022 г. «1С:Предприятие» занимает лидирующие позиции на рынке систем бухгалтерского учета [4].

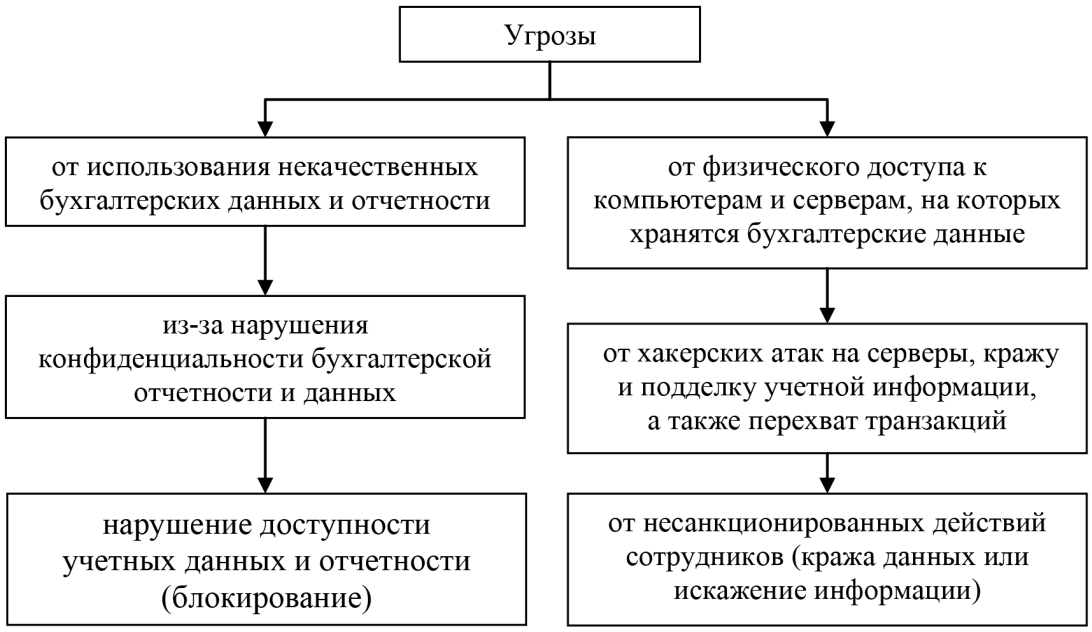

Рис. 1. Классификация угроз информационной безопасности в сфере бухгалтерского учета

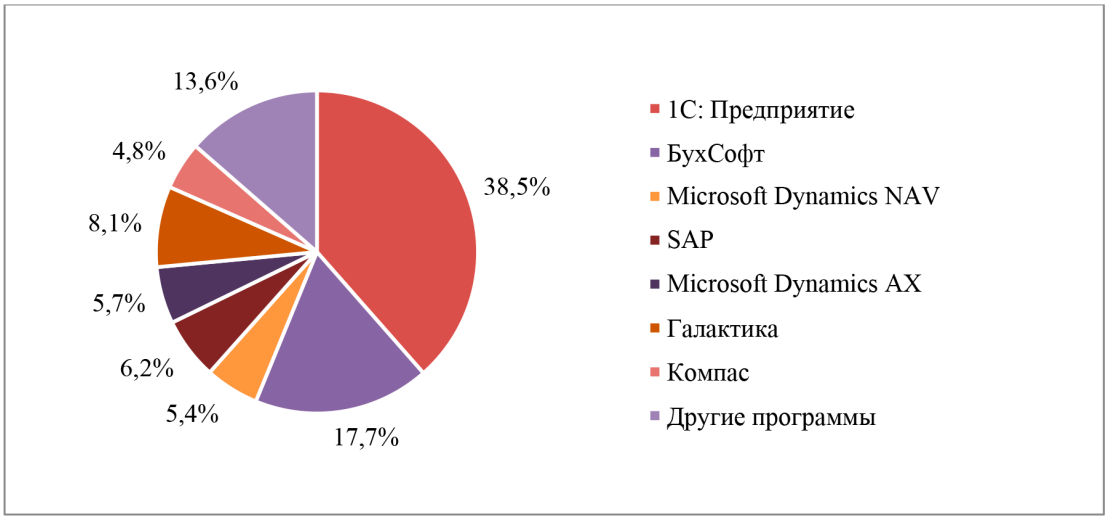

Рис. 2. Структура российского рынка цифровых систем учета за 2022 г. [5]

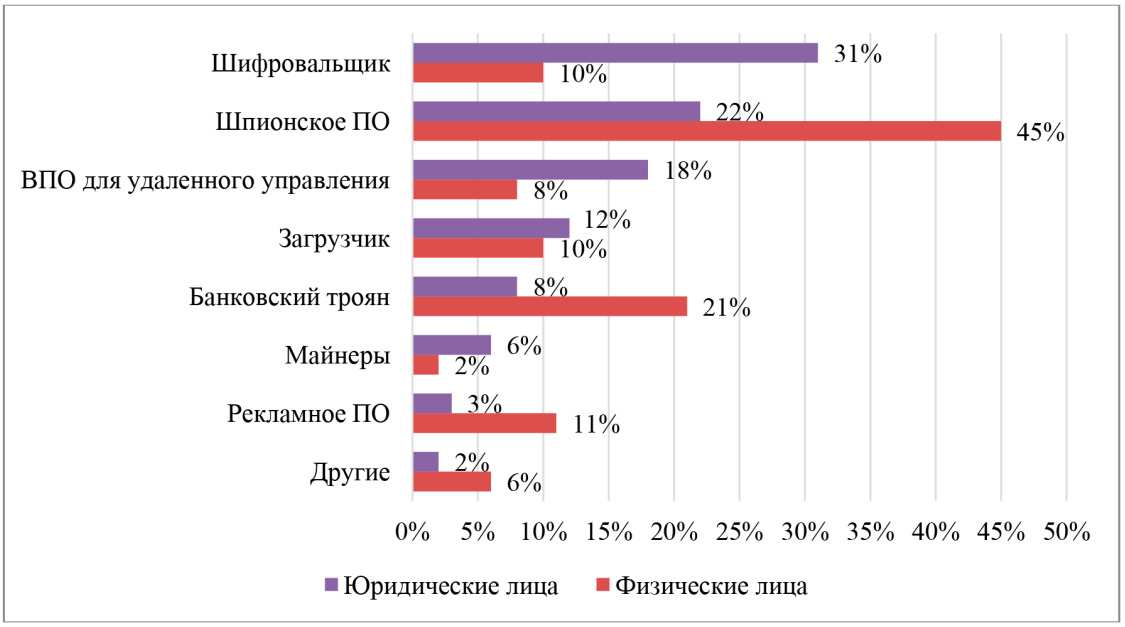

Рис. 3. Основные категории вредоносных программ, на долю которых приходится процент атак, % [3]

Наиболее распространенной угрозой является шпионское ПО, на долю которого приходится 45% атак и 22% при использовании VPO (виртуальной торговой точки). Эта статистика подчеркивает частоту проникновения шпионских программ в системы и компрометации персональных данных, подчеркивая необходимость принятия надежных мер защиты для противодействия этой скрытой угрозе (рис. 3).

Банковские трояны представляют собой еще одну серьезную угрозу, на их долю приходится 21% кибератак, причем 8% из них связаны с виртуальными частными лицами. Эти вредоносные программы подчеркивают острую необходимость принятия строгих мер безопасности для предотвращения кражи средств и несанкционированного доступа к данным, особенно учитывая их целенаправленную направленность на частных лиц и финансовые учреждения.

Чтобы снизить риски, связанные с вредоносным ПО в цифровой сфере, необходимо разработать надежные решения для обеспечения кибербезопасности. Эти решения должны включать оценку угроз, комплекс-

ные меры безопасности и образовательные программы для пользователей.

Ниже представлено несколько способов, с помощью которых технология блокчейн (рис. 4) может улучшить процедуры учета:

– минимизация ошибок за счет автоматического выполнения различных вычислительных операций, что снижает вероятность человеческих ошибок;

– снижение затрат, связанных с процессами бухгалтерского учета, при одновременном повышении их точности;

– снижение вероятности мошеннических действий за счет обеспечения неизменности распределенных записей;

– автоматизация многочисленных задач для упрощения процедур аудита и сокращения времени, необходимого для их выполнения [1].

Ожидается, что внедрение технологии блокчейн ускорит переход к автоматизированным процессам аудита и бухгалтерского учета, в первую очередь благодаря ее простоте интеграции с традиционными методологиями бухгалтерского учета. Учитывая необратимый характер документов, хранящихся на блокчейне, бухгалтерские организации могут использовать эту технологию для повышения безопасности записей клиентов.

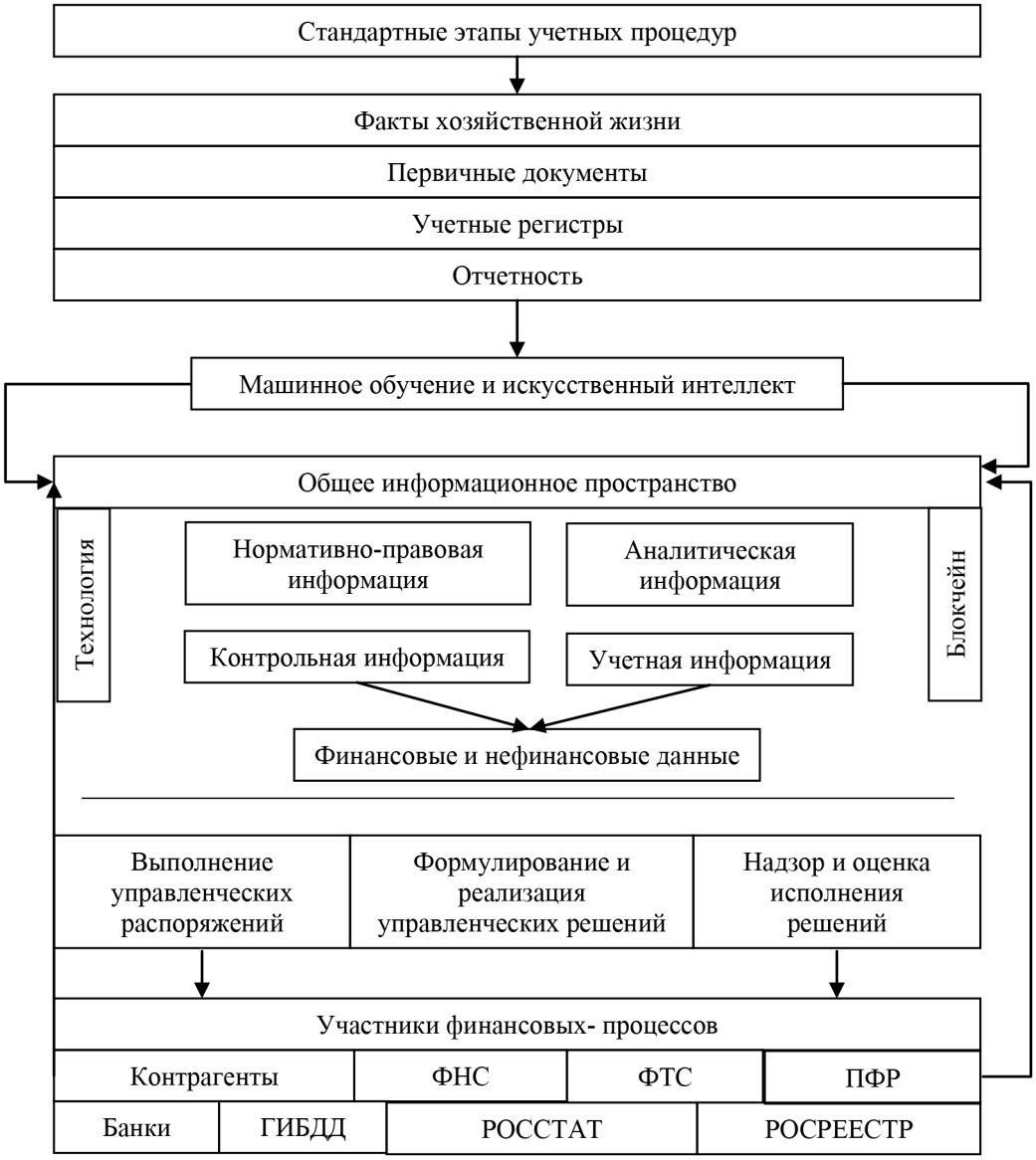

Рис. 4. Платформа для информационно-аналитической поддержки при внедрении технологии блокчейн [1]

Рис. 5. Динамика преступности, связанной с информационными технологиями и компьютерами, в 2019-2022 гг. [3]

Рис. 6. Динамика количества киберпреступлений в России за 2019-2022 гг. [1]

Интеграция технологии блокчейн в систему бухгалтерского учета организации требует переподготовки и повышения квалификации сотрудников. Бухгалтеры должны обладать аналитическими навыками и пониманием основных бизнес-процессов компании.

За последние годы количество зарегистрированных киберпреступлений значительно возросло (рис. 5). Если сравнивать данные за 2019 и 2020 годы, то они составили 48,5%, а в 2021 году – еще 16,4%. Несмотря на то, что в 2022 году количество зарегистрированных правонарушений

снизилось на 5,3% по сравнению с предыдущим годом, общая тенденция указывает на устойчивый рост, что подчеркивает сохраняющуюся актуальность борьбы с киберпреступностью.

Несмотря на активизацию усилий по борьбе с киберугрозами, постоянный рост числа зарегистрированных преступлений подчеркивает важность тщательного внимания к деталям, финансовой поддержки возможностей обеспечения кибербезопасности и упреждающих мер для эффективного противодействия угрозам. Также будут рассмотрены различные виды правонарушений, связанных с несанкционированным доступом к компьютерной информации, как показано на рисунке 6.

На рисунке 6 наглядно показан значительный рост числа случаев несанкционированного доступа к компьютерным данным. Число киберпреступлений выросло с 874 случаев в 2020 году до 4567 случаев в 2022 году, что подчеркивает стремительно растущую угрозу кибератак, несмотря на усиленные усилия по обеспечению кибербезопасности [1].

Атаки на электронную почту с использованием вредоносных вложений являются распространенным явлением в корпоративных хакерских атаках. Лица, ведущие рискованный онлайн-образ жизни, подвергаются повышенному риску сбоев в работе оборудования (рис. 7).

К основным методам распространения вредоносного ПО относятся:

1. Вложения в электронную почту: киберпреступники обычно распространяют вредоносное ПО с помощью вложений в электронную почту, часто маскируя их под законные файлы или документы.

2. Фишинговые атаки: фишинговые электронные письма и сообщения создаются с целью обмана получателей с целью разглашения конфиденциальной информации или перехода по вредоносным ссылкам.

3. Вредоносные веб-сайты: вредоносное ПО может распространяться через скомпрометированные или злонамеренно настроенные веб-сайты.

4. Зараженные съемные носители: вредоносное ПО может распространяться через зараженные USB-накопители, внешние жесткие диски или другие съемные носители.

5. Уязвимости программного обеспечения: Использование уязвимостей в программных приложениях или операционных системах является еще одним распространенным методом распространения вредоносного ПО.

6. Случайная загрузка: вредоносное ПО может быть автоматически загружено на устройство пользователя без его согласия при посещении взломанного веб-сайта.

7. Файлообменные сети: вредоносное ПО может маскироваться под законные файлы и распространяться через одноранговые (P2P) файлообменные сети.

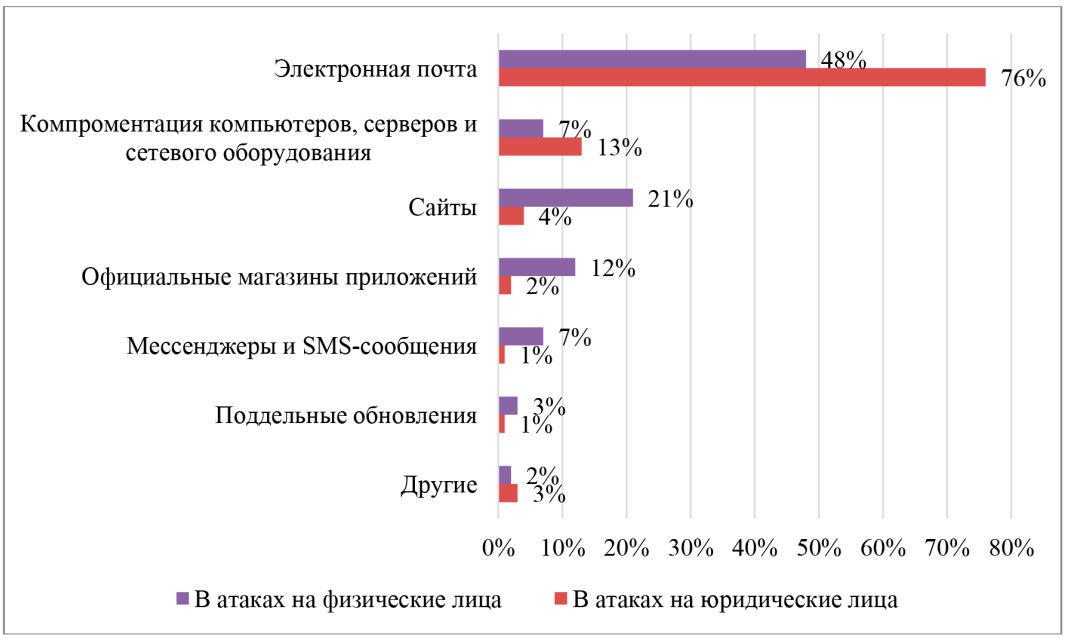

Рис. 7. Основные способы распространения вредоносных ПО, % [6]

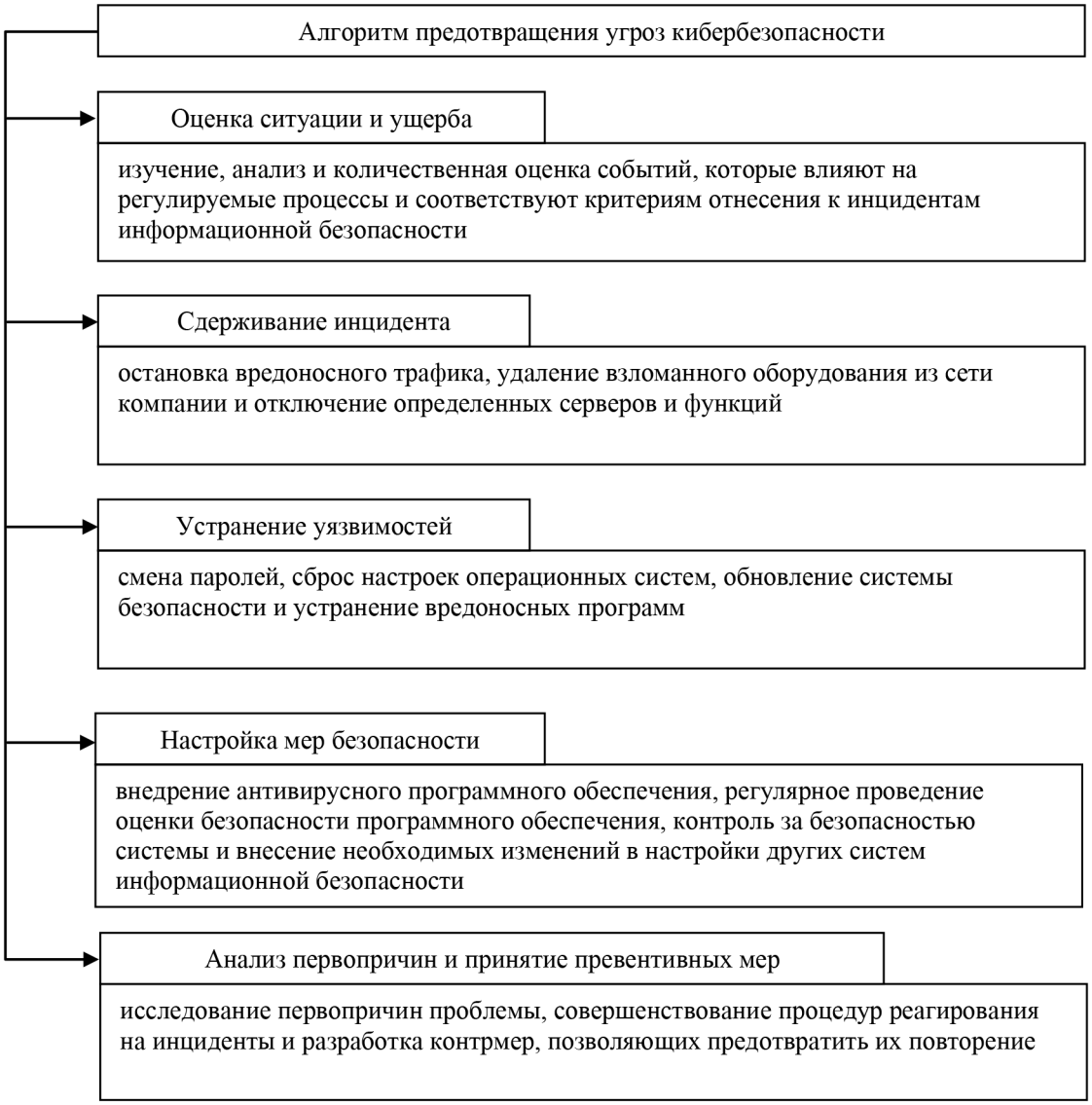

Рис. 8. Протокол для управления инцидентами информационной безопасности
Источник: составлено авторами

Понимание распространенных методов распространения вредоносных программ имеет решающее значение для пользователей и организаций в целях снижения рисков и защиты своих систем и данных от угроз.

Защита информации от киберугроз имеет первостепенное значение, особенно в свете растущей частоты компьютерных атак и вредоносного программного обеспечения.

На рисунке 8 показаны необходимые шаги, которые необходимо предпринять в случае возникновения проблемы с безопасностью в компьютерной системе компании.

Использование алгоритмов для решения задач информационной безопасности упрощает разработку стратегии, позволяя точно и оперативно реагировать на кибератаки. Интеграция блокчейна в бухгалтерский учет повышает безопасность, обеспечивая необратимое хранение данных. Однако эффективная интеграция требует переподготовки сотрудников, что требует владения как традиционными методами ведения бухгалтерского учета, так и глубокого понимания основных бизнес-операций [2].

Учитывая растущую угрозу киберпреступности, важно разработать план по предотвращению угроз кибербезопасности. Это предполагает выявление характера и масштабов нарушений информационной безопасности, расследование и оценку инцидентов, которые противоречат нормативным проце-

дурам, и количественную оценку ущерба, причиненного в результате. Последующие меры включают локализацию инцидентов путем блокирования вредоносного трафика, изоляции затронутых систем и деактивации скомпрометированных серверов и функциональных возможностей. Затем уязвимости устраняются с помощью таких процедур, как: анализ безопасности программного обеспечения, мониторинг безопасности системы, удаление вредоносных программ и смена паролей. В конечном счете, цель состоит в разработке надежных протоколов информационной безопасности, которые минимизируют риск несанкционированного доступа, изменения или неправомерного использования учетных данных, обеспечивая тем самым непрерывность работы организации.

Библиографический список

1. Варнакова Г.Ф., Васильева Е.В., Горловская Е.А., Клепикова М.В. Внедрение блокчейн технологии в бухгалтерский учет // Финансовая экономика. 2020. № 10. С. 27-29.

2. Башкатов В.В., Брык В.Ю., Зеленская А.М. Особенности бухгалтерского учета и отчетности в условиях цифровой экономики // Вестник Алтайской академии экономики и права. 2022. № 5-1. С. 5-10.

3. Кузнецова М.А. Хакерство как современная проблема в сфере бухгалтерского учёта // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей LVI Международной научно-практической конференции, Пенза, 15 мая 2022 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 136-139.

4. Миронова Н.Г., Мифтахова Л.И. Обеспечение безопасности конфиденциальной информации экономических субъектов с использованием интеллектуальных средств защиты // Chronos: естественные и технические науки. 2021. Т. 6, № 5(38). С. 17-20.

5. Нюхня И.В. Бухгалтерский учет в контексте цифровизации экономики // Инновации и инвестиции. 2022. № 10. С. 127-130.

6. Лошаков А.С., Щеглова Н.В. Экономические преступления, совершаемые с использованием информационных технологий и способы их предотвращения // Мировая экономика: проблемы безопасности. 2020. № 4. С. 16-20.