DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.3.6

УДК 004.7
ББК 32.81

ПРОБЛЕМЫ И РЕШЕНИЯ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Руслан Берикович Сеналиев

Магистрант, кафедра информационной безопасности,
Волгоградский государственный университет
senalievruslan01@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владислав Георгиевич Яриков

Кандидат педагогических наук,
доцент кафедры методики преподавания математики и физики, ИКТ,
Волгоградский государственный социально-педагогический университет
yarikov_vg@mail.ru
просп. им. В.И. Ленина, 27, 400005 г. Волгоград, Российская Федерация

Аннотация. В данной статье рассматриваются проблемы безопасности в облачных вычислениях, подчеркиваемые удвоением рыночных доходов за пять лет. Обсуждаются ключевые вопросы, такие как управление идентификацией, угрозы данных и соответствие регуляторным требованиям, предлагаются решения вроде шифрования и многофакторной аутентификации. Исследование выступает за комплексный подход к обеспечению надежной безопасности облачных сред.

Ключевые слова: облачные вычисления, безопасность облачных данных, управление идентификацией, многофакторная аутентификация, шифрование данных, стандартизация протоколов, интеграция облачных сервисов.

В современном мире информационных технологий облачные вычисления заняли ключевую роль, позволяя организациям и индивидуальным пользователям получать доступ к мощным вычислительным ресурсам, хранению данных и приложениям через интернет. Эта модель предоставляет гибкость, масштабируемость и экономию, открывая новые возможности для развития бизнеса, научных исследований и общественной жизни. Однако вместе с беспрецедентными преимуществами облачные технологии привносят и новые вызовы в области безопасности.

Важность безопасности в облачных вычислениях трудно переоценить. Данные и приложения, хранящиеся в облаке, становятся мишенями для кибератак, утечек информации и нарушений нормативной совместимости [3]. С учетом того, что облачные сервисы часто используются для обработки и хранения конфиденциальной информации, включая личные данные, финансовые отчеты и интеллектуальную собственность, риски, связанные с безопасностью, могут иметь серьезные последствия. Это делает актуальным поиск надежных решений для защиты облачных сред и данных, а также требует постоянного внима-

ния и адаптации к меняющемуся ландшафту угроз.

Особую роль защита облачных вычислений играет в банковском секторе. Банки сталкиваются с повышенным риском кибератак, утечек конфиденциальной информации, требованиями к нормативной совместимости, а также необходимостью защиты финансовых данных и личной информации клиентов. В контексте банковской безопасности облачные сервисы должны обеспечивать не только защиту от внешних угроз, но и соответствовать строгим нормативным и регуляторным требованиям. Решения облачной безопасности можно разделить на три основные категории:

– **безопасность инфраструктуры:** как брандмауэры, системы обнаружения / предотвращения вторжений и безопасное хранение данных;

– **безопасность операций:** как контроль доступа, аутентификация и авторизация;

– **безопасность приложений:** как сканирование уязвимостей, тестирование на проникновение и проверка кода.

Таким образом, введение в облачные вычисления и их безопасность является не только актуальной, но и необходимой частью дискуссии о будущем информационных и финансовых технологий. Осознавая эти вызовы, мы можем стремиться к разработке и внедрению эффективных стратегий и технологий, которые обеспечат безопасность и устойчивость облачных сервисов в долгосрочной перспективе.

Облачные вычисления представляют собой модель предоставления разнообразных информационных и вычислительных сервисов через Интернет, позволяя пользователям хранить файлы, использовать программное обеспечение и обрабатывать данные на удаленных серверах. Эта технология позволяет организациям и отдельным пользователям избавиться от необходимости поддерживать собственную вычислительную инфраструктуру или центры обработки данных, предоставляя доступ к вычислительным ресурсам по мере необходимости.

Согласно данным [5] (рис. 1) рынок облачных услуг растет глобально, с наибольшим вкладом от Северной Америки и значительным ростом в Азиатско-Тихоокеанском регионе. Европа стабильна, а Ближний Восток, Африка и Латинская Америка, хотя и меньше, также растут. Глобальные доходы сектора облачных услуг увеличиваются, с прогнозом роста с 73 млрд долл. в 2019 г. до 166,6 млрд в 2024 году. С ростом облачных платформ усиливается необходимость рассмотрения вопросов безопасности. Этот рост подчеркивает необходимость разработки и внедрения надежных мер безопасности, чтобы предотвратить утечки данных, нарушения конфиденциальности и другие угрозы безопасности, которые могут возникнуть в облачной среде.

Облачные вычисления классифицируются по нескольким ключевым моделям сервисов и развертывания [1]:

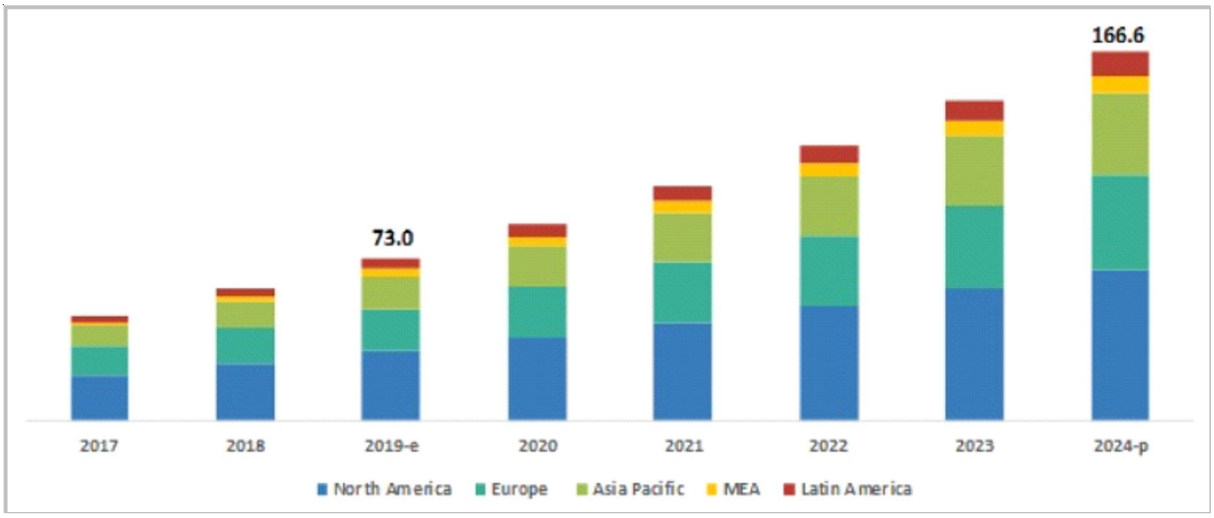

Рис. 1. Рынок облачных сервисов по регионам

Модели сервисов:

1. Infrastructure as a Service (IaaS). Предоставляет базовые вычислительные ресурсы, такие как виртуальные машины, сетевые ресурсы и хранилище данных, которыми можно управлять через Интернет.

2. Platform as a Service (PaaS). Предлагает среду разработки и развертывания приложений, где разработчики могут создавать, тестировать и запускать свои приложения, используя облачные инструменты без необходимости управления базовой инфраструктурой.

3. Software as a Service (SaaS). Позволяет пользователям подключаться и использовать облачные приложения через интернет, избавляя их от необходимости установки и обслуживания программного обеспечения на личных компьютерах или в корпоративной сети.

4. Function as a Service (FaaS). Обеспечивает возможность разработчикам запускать и управлять приложениями и функциями без необходимости заботиться об инфраструктуре, предоставляя высокую степень масштабируемости и гибкости. Это позволяет организациям сократить время и ресурсы, затрачиваемые на поддержку серверов и инфраструктуры, и сосредоточиться на разработке кода и инновациях.

Модели развертывания:

1. Общедоступное облако. Ресурсы предоставляются через интернет и доступны всем желающим. Примеры включают сервисы, предлагаемые Amazon Web Services, Microsoft Azure и Google Cloud Platform.

2. Частное облако. Инфраструктура облачных вычислений используется исключительно одной организацией. Частное облако может быть размещено в центре данных организации или у третьей стороны.

3. Гибридное облако. Сочетает элементы как общедоступных, так и частных облаков, позволяя данным и приложениям перемещаться между частными и общедоступными облачными средами. Такой подход обеспечивает большую гибкость и оптимизацию существующей инфраструктуры, безопасности и соответствия требованиям.

Каждая из этих моделей предлагает различные уровни управления, гибкости и масштабируемости, позволяя организациям выбирать решение, наиболее подходящее для их потребностей и целей, основные проблемы каждой модели представлены в таблице 1.

В области облачных вычислений безопасность данных и инфраструктуры является критически важной, учитывая растущую зависимость от облачных технологий в бизнесе и повседневной жизни. В таблице 2 представлены несколько основных проблем безопасности, с которыми сталкиваются облачные вычисления.

В таблице 2 рассматриваются ключевые проблемы безопасности в области облачных вычислений, их детализированное описание и предложения по решению данных проблематик. Анализ подчеркивает, что обеспечение безопасности в облачных средах требует всестороннего подхода, охватывающего различные аспекты, начиная от управления идентификацией и доступом и заканчивая обеспечением соответствия регуляторным требованиям.

Таблица 1

Проблемы облачных технологий

Виды облачных технологий	Актуальные проблемы
IaaS – Инфраструктура как услуга	Управление и масштабирование ресурсов, безопасность инфраструктуры
PaaS – Платформа как услуга	Совместимость и интеграция с различными средами и инструментами разработки
SaaS – Программное обеспечение как услуга	Зависимость от провайдера, конфиденциальность и безопасность данных
FaaS – Функция как услуга	Управление и мониторинг без серверных вычислений, холодный старт функций
Частное облако	Высокие затраты на управление и поддержание инфраструктуры, безопасность
Общедоступное облако	Управление данными и приложениями, соответствие регулированиям
Гибридное облако	Комплексность управления, интеграция и соответствие требованиям безопасности

Таблица 2

Проблемы и решения облачных технологий

Основные проблемы	Описание	Решение
Недостаточное управление идентификацией и доступом	– учетные данные слабой сложности и повторное использование; – недостаток многофакторной аутентификации; – привилегированный доступ без адекватного управления; – недостаточное разделение доступа; – управление идентификационными данными в облачных сервисах	– внедрение многофакторной аутентификации; – использование управления идентификацией и доступом (IAM); – применение принципа наименьших привилегий
Угрозы защите данных	– потеря данных; – утечка информации; – вредоносные программы; – межсайтовый скриптинг и инъекции SQL	– шифрование данных; – резервное копирование; – антивирусные и противовредоносные решения; – обновление программного обеспечения
Недостаточная видимость и мониторинг	– сложность облачных сред; – динамичность облачных ресурсов; – разделение ответственности; – интеграция с существующими системами безопасности; – непрозрачность облачных сервисов	– использование специализированных инструментов мониторинга; – автоматизация сбора и анализа данных; – регулярное обновление и настройка инструментов безопасности; – сотрудничество с провайдерами облачных услуг
Совместимость и межсетевое взаимодействие	– интеграция систем; – конфигурационные различия; – соответствие требованиям безопасности и регуляциям; – управление идентификацией и доступом (IAM); – транзитные данные	– использование стандартизированных протоколов и API; – централизованное управление безопасностью; – расширенное управление идентификацией и доступом; – шифрование и защита данных; – согласование политик безопасности; – автоматизация и оркестрация; – активное тестирование и мониторинг
Регуляторное соответствие и управление	– многообразие нормативных требований; – динамичность регуляторного ландшафта; – разделение ответственности; – защита данных и конфиденциальность; – отчетность и аудит	– понимание нормативных требований; – сотрудничество с надежными провайдерами; – централизованное управление данными; – разработка и внедрение политик и процедур; – регулярные аудиты и оценки соответствия

Проблематика управления идентификацией и доступом

Исследование выявило, что одной из фундаментальных проблем безопасности является недостаточное управление идентификацией и доступом. Проблематика связана с использованием учетных данных слабой сложности, отсутствием многофакторной аутентификации, недостаточным контролем за привилегированным доступом и неадекватным разделением доступа [6]. В качестве решения предлагается внедрение многофакторной аутентификации, использование систем управления идентификацией и доступом (IAM) и применение принципа наименьших привилегий.

Угрозы защите данных

Дальнейший анализ показывает, что угрозы защите данных, включая потерю данных, утечку информации, воздействие вредоносных программ, а также межсайтовый скриптинг и SQL-инъекции, представляют собой значительный риск [4]. Решение данной проблемы включает в себя шифрование данных, резервное копирование, применение антивирусных и противовредоносных решений, а также обновление программного обеспечения.

Недостаточная видимость и мониторинг

Недостаточная видимость и мониторинг в облачных средах, обусловленная сложностью облачных архитектур, динамичностью ресурсов, разделением ответственности, сложностями интеграции с существующими системами безопасности и непрозрачностью облачных сервисов, являются критическими факторами риска. Предложенные решения включают использование специализированных инструментов мониторинга, автоматизацию сбора и анализа данных, регулярное обновление и настройку инструментов безопасности, а также сотрудничество с провайдерами облачных услуг.

Проблемы совместимости и межсетевого взаимодействия

Совместимость и межсетевое взаимодействие, сталкивающиеся с проблемами интеграции систем, конфигурационных различий, требований безопасности и регуляций, управления идентификацией и доступом (IAM) и безопасности транзитных данных, требуют комплексного подхода к решению. Ключевые решения включают использование стандартизированных протоколов и API, централизованное управление безопасностью, расширенное управление IAM, шифрование и защиту данных, согласование политик безопасности, а также автоматизацию и оркестрацию процессов безопасности [2].

Регуляторное соответствие и управление

Завершающий аспект исследования касается проблем регуляторного соответствия и управления, выделяя сложности, связанные с многообразием нормативных требований и динамичностью регуляторного ландшафта. Выявлено, что разделение ответственности между провайдерами облачных услуг и их клиентами, а также обеспечение защиты данных и конфиденциальности, представляют собой значительные вызовы. В ответ на эти проблемы рекомендуется тщательное понимание нормативных требований, сотрудничество с надежными провайдерами облачных услуг, централизованное управление данными, разработка и внедрение соответствующих политик и процедур, а также проведение регулярных аудитов и оценок соответствия.

Обеспечение безопасности в облачных вычислениях требует интегрированного подхода, включающего как технические решения, так и стратегическое планирование. Анализ показывает, что успешное решение проблем безопасности достижимо через комплексное применение мер, направленных на укрепление управления идентификацией и доступом, защиту данных, повышение видимости и мониторинга, улучшение совместимости и межсетевого взаимодействия, а также обеспечение регуляторного соответствия. Особое внимание следует уделить развитию сотрудничества с провайдерами облачных услуг и внедрению централизованных систем управления данными и безопасностью. Таким образом, организации могут значительно снизить риски, связанные с безопасностью в облачных средах, и обеспечить защиту своих информационных активов в соответствии с высокими стандартами безопасности и регуляторными требованиями.

В статье освещены вопросы, связанные с ключевыми аспектами безопасности в современных облачных средах. Систематизированный обзор видов облачных технологий и их актуальных проблем безопасности подчеркивает значимость и сложность угроз, с которыми сталкиваются организации при переходе к облачным решениям.

Проведенный анализ позволяет сделать вывод о том, что несмотря на преимущества гибкости, масштабируемости и экономии, которые предоставляют облачные сервисы, необходимы осмысленные стратегии и меры по обеспечению безопасности данных и инфраструктуры. Недостаточное управление идентификацией и доступом, угрозы защите данных, недостаточная видимость и мониторинг, проблемы совместимости и межсетевого взаимодействия, а также регуляторное соответствие и управление требуют всестороннего подхода и постоянного адаптирования к новым угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев, В. Н. Безопасность в облачных вычислениях / В. Н. Васильев // Теория и практика современной науки. –2017. – № 3 (21). – С. 158–166.

2. Гюнтер, Е. С. «Облачные» вычисления и проблемы их безопасности / Е. С. Гюнтер, Н. Н. Нарутта, В. Г. Шахов // Омский научный вестник. – 2013. – № 2 (120). – С. 278–282.

3. Кодолов, П. А. Проблемы безопасности облачных вычислений // Наука, техника и образование. – 2016. – №. 4 (22). – С. 54–55.

4. Малюк, А. А. Перспективы развития «облачных» технологий. Риски информационной безопасности в «облачной» среде / А. А. Малюк, И. В. Ожеред // Международный научно-исследовательский журнал. – 2013. – № 3-1 (10). – С. 62–65.

5. Объем мирового облачного рынка увеличился на 20 % в I квартале 2023 года // ServerNews. – URL: https://servernews.ru/1085966

6. Что такое многофакторная аутентификация (MFA)? // Keeper Security: Password Management and Privileged Access Management (PAM) Solution. – URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-multi-factor-authentication/

REFERENCES

1. Vasiliev, V.N. Bezopasnost' v oblachnyh vychislenijah [Security in Cloud Computing]. *Teorija i praktika sovremennoj nauki* [Theory and Practice of Modern Science], 2017, no. 3 (21), pp. 158-166.

2. Gunter E.S., Narutta N.N., Shakhov V.G. "Oblachnye" vychislenija i problemy ih bezopasnosti [Cloud Computing and Problems of Its Security]. *Omskij nauchnyj vestnik* [Omsk Scientific Bulletin], 2013, no. 2 (120), pp. 278-282.

3. Kodolov P.A. Problemy bezopasnosti oblachnyh vychislenij [Problems of Cloud Computing Security]. *Nauka, tehnika i obrazovanie* [Science, Technology and Education], 2016, no. 4 (22), pp. 54-55.

4. Malyuk A.A., Ozhered I.V. Perspektivy razvitija "oblachnyh" tehnologij. Riski informacionnoj bezopasnosti v "oblachnoj" srede [Prospects for the Development of Cloud Technologies. Information Security Risks in the "Cloud" Environment]. *Mezhdunar. nauch.-issled. zhurn.* [International Research Journal], 2013, no. 3-1 (10), pp. 62-65.

5. Objom mirovogo oblachnogo rynka uvelichilsja na 20 % v I kvartale 2023 goda [The Volume of the Global Cloud Market Increased by 20% in the First Quarter of 2023]. *ServerNews*. URL: https://servernews.ru/1085966

6. Chto takoe mnogofaktornaja autentifikacija (MFA)? [What is Multi-Factor Authentication (MFA)?]. *Keeper Security: Password Management and Privileged Access Management (PAM) Solution*. URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-multi-factor-authentication/

CLOUD COMPUTING SECURITY ISSUES AND SOLUTIONS

Ruslan B. Senaliev

Master's Student, Department of Information Security,
Volgograd State University
Senalievruslan01@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Mathematics and Physics Teaching Methods, ICT,
Volgograd State Social and Pedagogical University
yarikov_vg@mail.ru
Prosp. Lenina, 27, 400005 Volgograd, Russian Federation

Abstract. The article highlights issues related to key security aspects in modern cloud environments. The systematized review of the types of cloud technologies and their current security issues highlights the significance and complexity of threats that organizations face when moving to cloud solutions. In today's world of information technology, cloud computing has taken a key role, allowing organizations and individuals to access powerful computing resources, data storage and applications over the Internet. This model offers flexibility, scalability

and economy, opening up new opportunities for business development, research and social life. However, along with unprecedented benefits, cloud technology brings new security challenges. The importance of security in cloud computing cannot be overemphasized. Data and applications stored in the cloud become targets for cyber-attacks, information leaks, and regulatory compliance breaches. Given that cloud services are often used to process and store sensitive information, including personal data, financial records, and intellectual property, security risks can have serious implications. The analysis concludes that despite the benefits of flexibility, scalability, and economy that cloud services offer, meaningful strategies and measures are needed to secure data and infrastructure. Inadequate identity and access management, threats to data protection, lack of visibility and monitoring, interoperability and interconnectivity issues, and regulatory compliance and governance require a comprehensive approach and continuous adaptation to new threats.

Key words: cloud computing, cloud data security, identity management, multifactor authentication, data encryption, protocol standardization, cloud services integration.