Е.В.БЕГЛЯК[1], В.А.МАРЦИНКЕВИЧ[2]

БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ: ТЕКУЩИЕ ВЫЗОВЫ И БУДУЩЕЕ

[1]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», старший преподаватель кафедры ВМиП
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ассистент кафедры ЭВМ

Облачные вычисления стали неотъемлемой частью цифровой инфраструктуры современного общества, предоставляя масштабируемые и гибкие решения для хранения и обработки данных. Однако широкое распространение облачных сервисов сопровождается ростом угроз информационной безопасности. Возникает необходимость в системном подходе к защите данных и ресурсов в облачной среде, что делает данную тему крайне актуальной для научного и практического сообщества.

Облачные вычисления предоставляют организациям множество преимуществ: снижение затрат на инфраструктуру, масштабируемость ресурсов, упрощенный доступ к данным. Однако вместе с этими плюсами возрастают и риски, связанные с обеспечением информационной безопасности.

Одной из главных проблем остается конфиденциальность данных. Пользователи доверяют облачным провайдерам хранение информации, при этом не всегда имеют полный контроль над ее использованием и перемещением. Утечки данных в облаке могут происходить из-за уязвимостей в программном обеспечении, ошибок конфигурации или злоумышленных действий со стороны инсайдеров [1].

Вторым значимым вызовом является управление доступом и идентификацией. В условиях многоуровневой архитектуры облака важно точно разграничивать права доступа между пользователями и сервисами. Роль многофакторной аутентификации и решений типа Identity and Access Management (IAM) становится критически важной для предотвращения несанкционированного доступа [2].

Кроме того, растет угроза целенаправленных атак, включая DDoS и атаки на цепочки поставок. Киберпреступники все чаще используют слабые места в системах облачных провайдеров для масштабных атак, затрагивающих миллионы пользователей [1].

Среди перспективных направлений повышения безопасности можно выделить гомоморфное шифрование, конфиденциальные вычисления и Zero Trust-модели. Эти технологии позволяют обрабатывать зашифрованные данные без их раскрытия, минимизируя риски в случае компрометации среды [3].

Также важно развитие стандартов и нормативной базы в области облачной безопасности. Международные инициативы, такие как ISO/IEC 27017 и рекомендации NIST, формируют основу для надежного внедрения облачных решений [4].

Таким образом, обеспечение безопасности в облачных вычислениях требует комплексного подхода, включающего технические, организационные и регуляторные меры.

Практика эксплуатации облачных платформ показывает, что применение отдельных механизмов защиты не обеспечивает требуемого уровня информационной безопасности. Даже использование современных средств аутентификации или криптографической защиты не позволяет полностью исключить риски, связанные с ошибками конфигурации, человеческим фактором, уязвимостями программного обеспечения или нарушением требований нормативных документов. По этой причине безопасность облачной инфраструктуры должна рассматриваться как совокупность взаимосвязанных уровней защиты, каждый из которых выполняет собственную функцию и компенсирует недостатки других уровней. Кроме того, эффективность системы безопасности определяется не только наличием отдельных средств защиты, но и правильностью их интеграции в единую архитектуру. Такой подход позволяет обеспечить непрерывность защитных механизмов на всех этапах жизненного цикла данных.

Особое значение приобретает согласованное применение организационных процедур, технических средств защиты и требований международных стандартов. Такой подход позволяет обеспечить защиту данных на всех этапах их хранения, обработки и передачи, а также повысить устойчивость облачной среды к современным киберугрозам. В результате формируется многоуровневая система безопасности, в которой каждый уровень выполняет собственную защитную функцию и дополняет остальные компоненты. Для наглядного представления комплексного подхода к обеспечению безопасности облачных вычислений используется многоуровневая модель защиты, представленная на рисунке 1.



Рисунок 1 – Многоуровневая модель обеспечения информационной безопасности в облачных вычислениях

Безопасность в облачных вычислениях – это многогранная задача, требующая постоянного внимания на фоне стремительного развития технологий и киберугроз. Современные вызовы, такие как защита конфиденциальности, управление доступом и противодействие атакам, требуют внедрения инновационных решений и соблюдения международных стандартов. Будущее облачной безопасности заключается в интеграции передовых технологий и построении доверенной цифровой среды.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Тонких, А. С. Угрозы безопасности в облачных технологиях и методы их устранения / А. С. Тонких, Е. Ю. Авксентьева // Международный журнал гуманитарных и естественных наук. – 2024. – № 1-2 (88). – С. 232–237.

2. Architecture of Identity Access Management in Cloud Computing | GeeksforGeeks [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/architecture-of-identity-access-management-in-cloud-computing/. – (дата обращения: 18.08.2026).

3. Компьютерная безопасность в облачных информационных системах: риски и способы их минимизации / Д.В. Солодовников Д.В. [и др.] // Human Progress. – 2024. – Т. 10, № 5. – С. 14

4. ISO/IEC 27017:2015 - Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/43757.html. – (дата обращения: 18.08.2026).