***Тонковид Ирина Дмитриевна***
*студент, кафедра защищенных систем связи*
*Санкт-Петербургский государственный университет*
*РФ, г. Санкт-Петербург*
*E-mail: irtonkovid@yandex.ru*

# ОБЛАЧНЫЕ ТЕХНОЛОГИИ: НОВЫЕ ГОРИЗОНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИРЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Данная статья представляет обзор современных вызовов и инновационных подходов к обеспечению информационной безопасности в облачной среде. Рассматривается эволюция облачных технологий и их влияние на процессы цифровой трансформации, выявляют угрозы безопасности данных в облаке и предлагают решения для их эффективного преодоления. Статья подчеркивает важность соблюдения современных стандартов безопасности, внедрения инновационных методов защиты, а также обучения сотрудников по вопросам кибербезопасности для обеспечения надежной защиты данных в условиях цифровой трансформации.

This article provides an overview of current challenges and innovative approaches to ensuring information security in the cloud environment. It examines the evolution of cloud technologies and their impact on digital transformation processes, identifies data security threats in the cloud, and offers solutions to effectively address them. The article emphasizes the importance of complying with modern security standards, implementing innovative protection methods, and providing cybersecurity training to employees to ensure reliable data protection in the context of digital transformation.

**Ключевые слова:** облачные технологии; информационная безопасность; цифровая трансформация; инновационные подходы; масштабируемость; гибкость; шифрование; искусственный интеллект; машинное обучение.

**Keywords:** cloud technologies; information security; digital transformation; innovative approaches; scalability; flexibility; encryption; artificial intelligence; machine learning.

## Введение

В век цифровых технологий, переплетенных с нашей повседневной жизнью, облачные технологии выступают в роли катализатора цифровой революции. Они проникают в различные сферы деятельности, изменяя привычные процессы и открывая новые возможности. Однако с этими инновациями приходят и вызовы. В мире, где информация становится ключевым активом, обеспечение ее безопасности в облаке играет решающую роль в сохранении конфиденциальности и целостности данных. Давайте погружаемся в увлекательный мир облачных технологий, где каждое новое событие – это шаг вперед к обеспечению надежности и защиты в мире цифровой трансформации.

## Эволюция облачных технологий и их влияние на цифровую трансформацию

Эволюция облачных технологий сыграла значительную роль в цифровой трансформации бизнеса и общества в целом. Начав с простых онлайн хранилищ и веб-приложений, облачные решения превратились в универсальный инструмент, предоставляющий компаниям возможность эффективно использовать вычислительные ресурсы и данные. Первоначально ограниченные возможности облачных сервисов быстро эволюционировали, предлагая широкий спектр функциональности - от инфраструктуры как сервиса (IaaS) до платформы как сервиса (PaaS) и программного обеспечения как сервиса (SaaS) [1, с. 92-95].

***Таблица 1.***

**Сравнительная характеристика облачных сервисов**

| Характеристика | IaaS (Infrastructure as a Service) | PaaS (Platform as a Service) | SaaS (Software as a Service) |
|---|---|---|---|
| Определение | Облачный сервис, предоставляющий виртуализированные вычислительные ресурсы через интернет | Платформа для разработки, тестирования и развертывания приложений | Программное обеспечение, доступное через интернет на основе подписки |
| Уровень управления | Пользователь управляет ОС, приложениями и данными | Пользователь управляет приложениями и данными; провайдер управляет платформой | Пользователь использует приложение; провайдер управляет всем |
| Гибкость | Высокая: пользователи могут настраивать ресурсы под свои нужды | Умеренная: пользователи могут разрабатывать приложения с использованием предоставленных инструментов | Низкая: пользователи используют готовое приложение без возможности настройки |
| Примеры | Amazon EC2, Google Compute Engine, Microsoft Azure VMs | Google App Engine, Heroku, Microsoft Azure App Services | Google Workspace, Salesforce, Dropbox |

Сравнение IaaS, PaaS и SaaS показывает, что каждая модель облачных сервисов отвечает различным потребностям. IaaS предлагает максимальную

гибкость и контроль над инфраструктурой, что делает его идеальным для организаций с высокими требованиями к настройке и управлению вычислительными ресурсами, особенно для ИТ-отделов и разработчиков. С другой стороны, PaaS предлагает сбалансированный подход, позволяя разработчикам сосредоточиться на создании приложений без необходимости управления нижележащей инфраструктурой. Это делает PaaS привлекательным вариантом для компаний, которые хотят ускорить процесс разработки и тестирования. Наконец, SaaS является наиболее удобным для конечных пользователей, предоставляя готовые решения без необходимости в установке и обслуживании программного обеспечения. Эта модель идеально подходит для бизнеса, который стремится минимизировать затраты на ИТ и быстро внедрять новые инструменты.

Таким образом, выбор между IaaS, PaaS и SaaS зависит от конкретных требований бизнеса, уровня контроля, который необходим пользователям, и степени гибкости, которую они ищут.

Рост облачных технологий существенно повлиял на цифровую трансформацию, обеспечивая организациям гибкость, масштабируемость и доступность. Облачные решения позволяют компаниям быстро развивать проекты без крупных капиталовложений, внедрять инновации и адаптироваться к изменяющимся требованиям рынка. Они стали не только инструментом хранения данных, но и важной платформой для повышения эффективности бизнеса и адаптивных методов работы. Эволюция облачных технологий привнесла новый уровень производительности, играя ключевую роль в конкурентоспособности и готовности к вызовам цифровой эпохи.

**Угрозы информационной безопасности в облаке**

Облачные технологии играют ключевую роль в цифровой трансформации, предоставляя организациям гибкость и доступ к ресурсам. Однако переход на облачные решения создает новые вызовы в информационной безопасности, включая несанкционированный доступ из-за слабых паролей или утечек данных. Это позволяет злоумышленникам

получить доступ к конфиденциальной информации, что представляет серьезную угрозу.

Облачные хранилища также могут подвергаться атакам, направленным на кражу данных, как внешними злоумышленниками, так и из-за ошибок сотрудников. Риск возрастает, когда данные хранятся в географически распределенных дата-центрах. Кроме того, облачные платформы подвержены атакам с использованием вредоносного ПО и DDoS-атакам, что может привести к недоступности сервисов и потере данных. Кроме того, организации часто теряют контроль над данными при использовании облачных решений, что может вызвать юридические риски. Неправильная настройка облачных сервисов может создавать уязвимости, так как многие не имеют достаточного опыта для их конфигурации. Зависимость от поставщиков услуг также представляет проблему: сбои или проблемы безопасности у них могут негативно сказаться. Ещё одной угрозой является компрометация API, используемых облачными сервисами для взаимодействия с приложениями. Если злоумышленники получат доступ к этим интерфейсам, они смогут управлять ресурсами и получать данные [4, с. 39-40].

Несмотря на преимущества облачных технологий, организациям следует учитывать угрозы безопасности. Для минимизации рисков необходимо внедрять меры защиты, такие как многофакторная аутентификация, шифрование данных, регулярные аудиты безопасности и обучение сотрудников. Это обеспечит безопасность данных и эффективное использование облачных технологий.

**Инновационные подходы к обеспечению безопасности в облаке**

С увеличением числа организаций, переходящих на облачные технологии, вопросы информационной безопасности становятся критически важными. Облачные решения предлагают преимущества, но также открывают новые киберугрозы. Компании должны внедрять инновационные подходы к безопасности в облачных средах, включая адаптивные системы на основе ИИ и машинного обучения (ML). Эти технологии позволяют анализировать

поведение пользователей и выявлять аномалии в реальном времени, автоматически блокируя доступ при подозрительной активности [5, с. 597-601].

Модель «нулевого доверия» (Zero Trust) становится основным принципом защиты данных. Она включает проверку подлинности и авторизации для каждого взаимодействия, многофакторную аутентификацию (MFA) и принцип минимальных привилегий. Интеграция DevSecOps позволяет внедрять безопасность на всех этапах разработки, а автоматизированное тестирование уязвимостей помогает выявлять проблемы на ранних стадиях.

Прозрачность и отчетность также важны: системы SIEM централизуют сбор данных о безопасности, что упрощает отслеживание операций и расследование инцидентов. Обучение сотрудников по кибербезопасности и симуляции атак помогают предотвратить утечки данных.

Гибридные облачные архитектуры позволяют изолировать критически важные данные в частном облаке, сохраняя гибкость публичных сервисов и соответствуя требованиям законодательства. Таким образом, инновационные подходы к безопасности в облаке становятся ключевыми для цифровой трансформации организаций, защищая данные и укрепляя доверие клиентов.

**Заключение**

В современном информационном обществе, облачные технологии стали ключевым инструментом для повышения эффективности бизнес-процессов и ускорения инноваций. Однако увеличивающиеся угрозы информационной безопасности требуют внимательного обеспечения защиты данных. Инновационные методы, такие как искусственный интеллект, шифрование данных и блокчейн технологии, становятся важными в защите данных в облаке. Непрерывное совершенствование подходов к безопасности включает обучение сотрудников, мониторинг и использование современных методов аутентификации. Только комплексное применение инновационных подходов позволит компаниям эффективно защищать данные в облаке и обеспечивать информационную безопасность в цифровой трансформации.

**Список литературы**


1. Бирих Э. В. и др. РАЗВИТИЕ СТАНДАРТОВ И РУКОВОДСТВ В СФЕРЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 92-95. – URL: https://www.elibrary.ru/item.asp?edn=yrpzwj&ysclid=mckww01zcy563769356 (дата обращения 30.06.25)
2. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – №. 2. – С. 31-35. – URL: https://www.elibrary.ru/item.asp?id=46618712&ysclid=mckx1aln1550336258 4 (дата обращения 30.06.25)
3. Пестов И. Е. и др. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности //I-methods. – 2022. – Т. 14. – №. 1. – С. 4. – URL: https://cyberleninka.ru/article/n/metod-peredachi-metrik-zagruzhennosti-instansov-oblachnoy-infrastruktury-v-klaster-obrabotki-sredstvami-i-metodami-bolshih-dannyh?ysclid=mckx2k4kbz437392371 (дата обращения 01.07.25)
4. Гельфанд А. М. и др. Организация концептуальной модели критической информационной инфраструктуры //Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 39-40. – URL: https://www.elibrary.ru/item.asp?id=44017259&ysclid=mckx4dswof753269056 (дата обращения 29.06.25)
5. Ковцур М. М. и др. Обеспечение информационной безопасности web-приложений с использованием машинного обучения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 597-601. – URL:

https://www.elibrary.ru/item.asp?edn=avkacm&ysclid=mckx57ffcv796882101 (дата обращения 01.07.25)

6. Тонких А.С. Угрозы безопасности в облачных технологиях и их устранения. – 2017. – URL: https://cyberleninka.ru/article/n/ugrozy-bezopasnosti-v-oblachnyh-tehnologiyah-i-metody-ih-ustraneniya/viewer (дата обращения 01.07.25)