ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ СЕРВИСАХ

А.Д. Яковишин, *магистр*
Камчатский государственный технический университет
(Россия, г. Петропавловск-Камчатский)

DOI:10.24412/2500-1000-2024-1-2-245-249

Аннотация. *В статье исследуется применение криптографических технологий в облачных сервисах. Описывается важность облачных технологий, их быстрый рост и необходимость защиты информации. Основное внимание уделяется уязвимостям облачных сервисов и методам их защиты, включая шифрование данных, хэширование, аутентификацию, использование VPN и многофакторную аутентификацию. В статья также уделяется внимание роли и важность криптографии в современной защите данных и информации.*

Ключевые слова: *облачные сервисы, криптографические технологии, защита данных, шифрование, аутентификация, кибербезопасность.*

В настоящее время происходит стремительное развитие технологий, в связи с чем качественно изменился подход к хранению информации.

Одним из способов хранения являются облачные сервисы, которые обладают рядом важных достоинств (высокотехнологичная защита, возможность удаленного доступа к данным через Интернет, доступность и гибкость в использовании информационных ресурсов). Эти достоинства позволяют сервисам эффективно и безопасно организовывать защиту и обработку данных, дают облачным технологиям значительный приоритет среди других современных технических инструментов, которые занимаются сбором и хранением информации [1].

Согласно исследованиям компаний International Data Corporation (Нидхэм, США), Gartner (Стэмфорд, США) и Synergy Research Group (Алматы, Казахстан), специализирующихся на изучении мирового рынка информационных технологий и телекоммуникаций, с 2017 по 2022 гг. произошел значительный рост рынка публичных облачных сервисов. В 2017 году аналитики IDC опубликовали данные об увеличении объема глобального рынка облачных сервисов на 29%, который в денежном выражении составил около $117 млрд. В 2023 году Gartner оценивал мировой рынок облачных технологий (рис. 1) уже в $563,59 млрд.

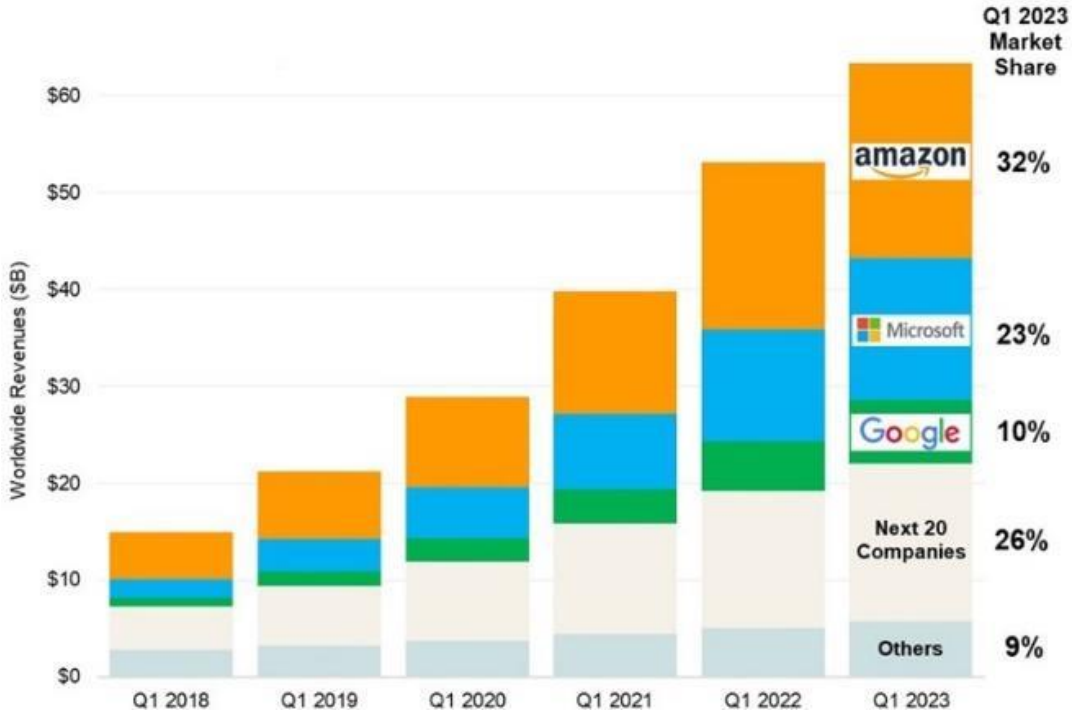

Рис. Исследование Synergy Research Group, рост объема глобального рынка публичных облачных сервисов [2]

Такой масштабный рост числа компаний и частных лиц, которые переходят на облачные решения для хранения и обработки данных, а также используют облачные сервисы для разработки и развертывания приложений, объясняется свойствами их высокой масштабируемости и гибкости [3]. Это особенно полезно для бизнеса, поскольку позволяет ему быстро адаптироваться к изменяющимся рыночным условиям. Немаловажным преимуществом облачных сервисов является возможность хранения большого объема данных. По данным исследования американской компании Cisco, в 2020 году на облачных сервисах хранилось более 100 зеттабайт (10^{21} байт) данных, что на 26% больше, чем в 2019 году.

Уязвимость облачных сервисов и основные методы их защиты от несанкционированного доступа. Защита облачных сервисов является важной задачей, так как эти сервисы используются для хранения и обработки конфиденциальной информации, такой как личные данные пользователей, финансовые сведения, коммерческие секреты и т.д. Утечка или несанкционированный доступ таким данным может привести к финансовым потерям, утрате репутации компании, нарушению законодательства и другим серьезным последствиям.

Для определения уровня защищенности информации в облачном сервисе используются различные методы (напр., сканирование уязвимостей, анализ сетевого трафика, тестирование на проникновение), которые позволяют выявлять недостатки в системе защиты и принимать меры по их устранению.

Производством технологий безопасности для облачных приложений занимаются специализированные организации (напр., Cloud Security Alliance и Open Web Application Security Project). Их проекты включают в себя разработку стандартов и рекомендаций по защите инфраструктуры облачного сервиса от сетевых атак, усовершенствование системы контроля и управления доступом, проведение аудита по обнаружению ошибок и уязвимостей в системе защиты провайдера облачных услуг. Неустойчивость облачной сервисной инфраструктуры к киберугрозам может быть связана с различными факторами, в список которых входят ошибки в программном обеспечении, недостаточный

контроль доступа, уязвимость системы к DDoS-атакам и др. Проектирование эффективной системы безопасности облачного сервиса, включает в себя обязательное использование многоуровневого подхода к защите информации, который обеспечивает конфиденциальность, целостность и аутентичность данных. Это решение реализуется через использование различных криптографических технологий, что позволяет устранить критические уязвимости в сервисной системе защиты. Некоторые из основных видов криптографических технологий используют следующие инструменты:

1. Шифрование данных. Используется для защиты конфиденциальной информации, которая хранится в облачных сервисах. Может быть симметричным или асимметричным. В первом случае используется один ключ , в то время как в асимметричном шифровании используется два ключа – открытый и закрытый.

2. Хэширование. При хэшировании данные преобразуются в уникальную строку символов фиксированной длины, которая служит цифровой подписью. Если данные меняются, хэш также изменяется, что позволяет обнаруживать любые внесенные изменения.

3. Аутентификация. Используется для проверки подлинности документов пользователей облачных сервисов. Такой эффект достигается за счет различных методов: введение паролей, биометрических данных, одноразовых кодов и т.д.

4. Virtual Private Network, VPN. Применяется для обеспечения безопасного соединения между удаленными пользователями и облачными серверами. VPN шифрует данные, передаваемые между пользователем и сервером, что обеспечивает конфиденциальность и защиту от несанкционированного доступа.

5. Многофакторная аутентификация. Используется для обеспечения дополнительной защиты облачных сервисов. В отличие от однофакторной аутентификации, где для проверки подлинности используется только один фактор (например, пароль), в многофакторной аутентификации задействовано несколько таких факторов (например, пароль и голосовое распознавание).

Высокая скорость роста глобального рынка облачных сервисов увеличивает спрос на усовершенствование инструментов криптографии. Согласно отчету [4] американской исследовательской компании Dell'Oro Group в области информационных технологий, прибыль в отрасли защиты облачных приложений (SSE) в 2022 году увеличилась приблизительно на $1 млрд, или на 38%, по сравнению с 2021 годом.

Такое сильное расширение отрасли связано со стремительным развитием спроса на облачные приложения в период пандемии COVID-19, а также развитием удаленной работы и дистанционного обучения [5]. Масштабное увеличение числа пользователей облачных серверов значительно повышает количество потенциальных целей для киберпреступников. Это провоцирует стремительное распространение киберугроз, из-за чего традиционные методы и технологии защиты могут оказаться недостаточными для эффективной борьбы с ними. В связи с этим, компании и организации активно внедряют в систему безопасности своих облачных приложений решения Secure Socket Layer (SSL), Transport Layer Security (TLS) и Secure Access Service Edge (SASE).

SSL и TLS – это криптографические протоколы, которые обеспечивают безопасность соединения между клиентом и сервером во время передачи данных в Интернете. Они используются для защиты конфиденциальности, целостности и подлинности данных, передаваемых между веб-браузером пользователя и веб-сервером. Решения SSL и TLS предоставляют ряд важных преимуществ и гарантий для обеспечения безопасности облачных сервисов. SSL и TLS обеспечивают защиту от различных видов атак и безопасное соединение, защищая данные от несанкционированного доступа или изменений. Возможности этих протоколов позволяют проверить подлинность веб-сервера, с которым устанавливается соединение, при этом сервер должен предоставить действительный сертификат, который подтвер-

ждает его идентификацию. Это помогает предотвратить атаки типа Man-in-the-Middle (тип атаки, при которой злоумышленник встраивается между двумя узлами связи и перехватывает или изменяет передаваемые данные, не позволяя пользователям общаться напрямую).

SSL и TLS являются стандартными протоколами, поддерживаемыми всеми современными веб-браузерами и серверами, поэтому они совместимы с большинством платформ и приложений, что облегчает их использование и обеспечивает безопасность для широкого круга пользователей.

Стратегия безопасности SASE стремится к эффективному объединению возможностей криптографических технологий для защиты информации на облачных сервисах. Она включает функции шифрования, контроля доступа, сегментации трафика, защиты от DDoS и обнаружения угроз. Главным преимуществом SASE, относительно традиционных моделей, является размещение механизмов управления безопасностью сети в распределенной среде. Это исключает необходимость в индивидуальной конфигурации в управлении системой безопасности и позволяет создать надёжную сетевую инфраструктуру, предоставляя стандартизированный набор сетевых сервисов. SASE позволяет организациям создавать политики безопасности, основанные на приложениях, благодаря чему обеспечивает безопасность на периферии сети и защиту от угроз.

Все эти факторы делают SASE эффективным подходом для защиты облачных сервисов. Стратегия обеспечивает стандартизацию, гибкость, улучшение производительности, защиту от угроз и упрощение управления, что позволяет организациям эффективно защитить свои приложения и данные от различных видов угроз.

Вывод

Криптографические технологии играют важную роль в обеспечении безопасности информации на облачных сервисах. На сегодняшний день их решения являются основой для защиты конфиденциальности, целостности и подлинности данных, гарантируют безопасность в проведении коммуникаций и транзакций. Без криптографической защиты такие современных технологии, как блокчейн или цифровая подпись не смогут обеспечить компаниям и частным пользователям должный уровень безопасности.

Необходимость в криптографии усиливается с появлением новых технологий и угроз, таких как искусственный интеллект, облачные вычисления и киберпреступность, которые создают новый тип эффективных уязвимостей для системы защиты облачных сервисов.

Можно заключить, что применение криптографических технологий является необходимым для обеспечения безопасности данных и информации в современном цифровом мире. Их использование и совершенствование позволяет защитить данные от несанкционированного доступа, обеспечить конфиденциальность переписки, сохранить целостность информации и обеспечить подлинность транзакций. Криптография является неотъемлемой частью многих современных технологий и играет ключевую роль в обеспечении безопасности в эпоху цифровизации.

Библиографический список

1. Кенджаев Д.А. Трансформация искусства и музейного пространства с помощью AR-технологий // Современные научные исследования и инновации. – 2023. – № 12.

2. Staal, T.J. (2022) The impact of the Internet of Things on the demand of cloud resources (Bachelor's thesis, University of Twente).

3. Тюменцев, Д.В. Devops в эпоху облачных технологий: современные практики и перспективы развития / Д.В. Тюменцев // Вестник науки. – 2023. – Т. 2, № 8(65). – С. 190-195. – EDN AGNLBG.

4. Israfilov A. Covid-19 and its cybersecurity implications: from threat escalation to strategic response // Вестник науки. – 2023. – №12 (69) Том 4. – С. 1087-1093. ISSN 2712-8849.

5. Tahenni A, Merazka F. SD-WAN over MPLS: A Comprehensive Performance Analysis and Security with Insights into the Future of SD-WAN. (preprint): 2401.01344. 2023 Oct 23.

APPLICATION OF CRYPTOGRAPHIC TECHNOLOGIES FOR INFORMATION PROTECTION IN CLOUD SERVICES

A.D. Yakovishin, *Master's degree*
Kamchatka State Technical University
(Russia, Petropavlovsk-Kamchatsky)

Abstract. *The paper investigates the application of cryptographic technologies in cloud services. It describes the importance of cloud technologies, their rapid growth and the need to protect information. The main focus is on the vulnerabilities of cloud services and methods of their protection, including data encryption, hashing, authentication, use of VPN and multi-factor authentication. The article also focuses on the role and importance of cryptography in modern data and information security.*

Keywords: *cloud services, cryptographic technologies, data protection, encryption, authentication, cybersecurity.*