Научная статья
УДК 004.056.53

ЗАЩИТА ОБЛАЧНЫХ ДАННЫХ: СОВРЕМЕННЫЕ УГРОЗЫ, МЕТОДЫ И РЕКОМЕНДАЦИИ

Исроил Бекович Исмоилов[1], Евгений Николаевич Щепеткин[2]
[1, 2] Уральский государственный лесотехнический университет, Екатеринбург, Россия
[1, 2] evg0606@mail.ru

Аннотация. В данной статье рассматриваются актуальные вопросы защиты данных в облачных инфраструктурах. Анализируются современные угрозы безопасности облачных сервисов (вычисления злоумышленников, программные уязвимости, неправильные конфигурации), методы защиты.

Ключевые слова: облачные вычисления, безопасность данных, резервное копирование, контроль доступа, искусственный интеллект

Для цитирования: Исмоилов И. Б., Щепеткин Е. Н. Защита облачных данных: современные угрозы, методы и рекомендации // Научное творчество молодежи – лесному комплексу России = Scientific creativity of youth to the forest complex of Russia : материалы XXII Всероссийской (национальной) научно-технической конференции студентов и аспирантов. Екатеринбург : УГЛТУ, 2026. С. 1154−1159.

Original article

CLOUD DATA PROTECTION: MODERN THREATS, METHODS, AND RECOMMENDATIONS

Isroil B. Ismoilov[1], Evgeny N. Shchepetkin[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1, 2] evg0606@mail.ru

Abstract. This article discusses current issues of data protection in cloud infrastructures. Modern threats to the security of cloud services (malicious calculations, software vulnerabilities, misconfigurations), and protection methods are analyzed.

Keywords: cloud computing, data security, encryption, backup, access control, artificial intelligence

For citation: Ismoilov I. B., Shchepetkin E. N. (2026) Zashhita oblachny`x danny`x: sovremenny`e ugrozy`, metody` i rekomendacii [Cloud data protection: modern threats, methods and recommendations]. Nauchnoe tvorchestvo molodezhi – lesnomu kompleksu Rossii [Scientific creativity of youth to the forest complex of Russia] : materials of the XXII All-Russian (national) Scientific and Technical Conference of undergraduate and postgraduate students. Ekaterinburg : USFEU, 2026. P. 1154–1159. (In Russ).

Облачные технологии стали неотъемлемой частью IT-инфраструктур современных организаций, обеспечивая гибкость и масштабируемость бизнеса. Вместе с тем рост доли данных в облаке сопровождается увеличением киберугроз. Так, по данным отраслевых отчетов, в 2024 г. 52 % компаний во всем мире фиксировали атаки на свои облачные среды (в России доля подобных инцидентов близка к глобальной). При этом методы атак постоянно эволюционируют: чаще всего злоумышленники стремятся получить несанкционированный доступ к облачным ресурсам (например, с помощью вредоносного ПО, эксплуатирующего уязвимости), а также используют сложные комбинированные приемы (например, атаки программ-вымогателей, фишинг для кражи учетных данных). Статья посвящена анализу этих угроз, описанию современных средств защиты (шифрования, бэкапов, контроля доступа), роли ИИ в обеспечении безопасности облака, а также практическим рекомендациям на основе инцидентов 2024–2025 гг. [1].

Облачные платформы подвержены множеству угроз, характерных как для традиционных ИТ-систем, так и специфичных для виртуальной среды. Наиболее распространенные из них:

– **неправильная конфигурация и отсутствие защиты.** Неправильные настройки облачных ресурсов (например, публично открытые хранилища данных S3) по-прежнему остаются серьезной уязвимостью. По оценкам Qualys, около 31 % хранилищ AWS S3 имеют публичный доступ, что ставит под угрозу данные пользователей. Плохо настроенные политики доступа позволяют злоумышленникам обнаруживать и эксплуатировать ресурсы через общедоступные сервисы (микросервисы, API, контейнеры и т. д.);

– **компрометация учетных данных.** Частой причиной атак является кража логинов и паролей от облачных аккаунтов. Если многофакторная аутентификация (MFA) не включена, злоумышленнику достаточно похищенного пароля для доступа к облачным ресурсам. Примером может служить масштабная атака на платформу Snowflake (облачное хранилище данных): злоумышленники использовали ранее украденные учетные данные без MFA, что позволило скомпрометировать более 160 клиентских инстансов Snowflake и похитить конфиденциальную информацию;

– **программы-вымогатели (Ransomware).** В 2024 г. частота атак с шифрованием корпоративных данных возросла. Так, в ноябре 2024 г. компания Schneider Electric подверглась атаке шифровальщика, выведшему из строя ее IT-системы и заблокировавшему доступ к данным. Аналогично промышленные предприятия сообщали о множественных атаках на инфраструктуру, связанных с отказом и похищением данных ради выкупа;

– **сетевая экспансия и IoT.** Многие промышленные объекты и предприятия расширяют свои сети, подключая к ним устройства Интернета вещей и системы OT. Это повышает поверхность атаки: при успешном проникновении в сеть через IoT-устройство злоумышленник может получить доступ к облачным сервисам предприятия;

– **человеческий фактор**. Социальная инженерия (фишинг, инсайдерские утечки) остается одной из главных причин компрометации данных. По исследованию SearchInform, в 2024 г. утечки данных происходили в 48 % опрошенных российских компаний (причем во многих случаях причиной были ошибки сотрудников). В облачных условиях это может проявляться через небезопасное хранение учетных данных или использование учетных записей с избыточными правами [2].

Анализ инцидентов показывает резкий рост кибератак на облачные окружения. Например, отчет CrowdStrike за 2024 г. фиксировал 75 %-е увеличение атак на облачные инфраструктуры и 110 %-й рост случаев использования именно облачных уязвимостей для проникновения в системы. Это подчеркивает актуальность постоянного мониторинга и защиты облака.

Эффективная защита данных в облаке базируется на многоуровневом подходе, включающем криптографические методы, надежное резервное копирование и жесткие политики доступа.

Выделяют несколько методов защиты информации:

– **шифрование данных**. Шифрование обеспечивает конфиденциальность информации как при передаче, так и при хранении. «Шифрование облачных данных – это процесс преобразования информации в нечитаемый формат, доступный только при наличии ключей дешифрования». Используются симметричные алгоритмы (например, AES) и асимметричные (RSA, ECC): первый обеспечивает быстрое шифрование больших объемов данных, второй – усиленную защиту при обмене ключами. Облачные провайдеры по умолчанию шифруют данные «на покое» (AES-256) и «в пути» (TLS). Для управления ключами применяются специализированные службы (KMS) и аппаратные модули HSM. Организации могут выбирать между ключами, управляемыми провайдером (упрощенный подход), и собственными ключами (CMK), что дает полный контроль над безопасностью;

– **резервное копирование**. Регулярное сохранение резервных копий критически важно для восстановления после потери данных (например, из-за ошибки, сбоя или ransomware). По экспертным оценкам, системы бэкапа «обеспечивают защиту информации от потери» и спрос на такие решения продолжает расти. Для облачных сред рекомендуется хранить резервные копии в отдельном сервисе или географически удаленно, использовать версионность и неизменяемые хранилища (immutable storage). Также важна автоматизация процесса и периодическое тестирование восстановления, чтобы гарантировать надежность резервных данных;

– **контроль доступа и управление привилегиями**. Не менее важно ограничивать доступ к облачным ресурсам (RBAC, least privilege) и использовать корпоративные системы управления идентификацией (IAM). Внедрение многофакторной аутентификации (MFA) и единого входа (SSO) позволяет существенно снизить риск компрометации аккаунтов. Как отмечают специалисты, «инструменты, такие как поддержка SSO и MFA, а также аудит-логи, позволяющие контролировать доступ к корпоративным данным и отслеживать действия сотрудников, повышают уровень защиты». Аудит и логирование операций в облаке (например, сервисов CloudTrail, CloudWatch) позволяют оперативно выявлять подозрительную активность и быстро реагировать на инциденты [3].

Искусственный интеллект (ИИ) и машинное обучение (МО) все активнее применяются в задачах кибербезопасности облака. Интеллектуальные системы анализируют большие объемы данных из облачных журналов и трафика, выявляя аномалии и инциденты быстрее человека. Например, современные платформы безопасности используют МО-модели, обученные на обширных наборах нормального поведения, чтобы автоматически обнаруживать нештатные события: «если ключ API используется из неожиданного региона или резко возрастает число вызовов API, такие системы обнаруживают и сигнализируют об этом администратору». Подходы AI-Driven Threat Detection (или AI-XDR) позволяют автоматически коррелировать данные из различных источников (логов, сетевого трафика, инцидентов) и выявлять скрытые признаки атаки, минимизируя время реакции.

Кроме того, ИИ используется для предиктивного анализа уязвимостей и формирования рекомендаций. Аналитики Gartner прогнозируют, что в ближайшие годы облачные стратегии будут в значительной степени основаны на ИИ (например, для оптимального распределения ресурсов и защиты данных). Многие провайдеры облаков внедряют встроенные ИИ-сервисы безопасности (IDS/IPS с ML, Cloud Intrusion Detection, автоматический анализ настроек – Cloud Security Posture Management и т. д.). В совокупности эти решения позволяют проводить «мониторинг в реальном времени» и быстрее обнаруживать угрозы, что особенно важно для облака из-за его динамичности [2].

Наиболее крупные инциденты последних лет демонстрируют типичные уязвимости в облачной безопасности:

– **массовые утечки через уязвимые сервисы.** В 2024 г. стало известно о масштабном инциденте со службой Snowflake: злоумышленники (группа UNC5537) получили доступ к множеству клиентских баз данных, воспользовавшись ранее похищенными логинами без MFA. В результате пострадали крупные компании (AT&T, Ticketmaster и др.), было похищено более 50 млрд телефонных записей и другой конфиденциальной информации. Основными причинами взлома стали отсутствие включенного MFA на учетных записях и неготовность к ограничению доступа (отсутствие сетевых «белых списков»);

– **атаки шифровальщиков на облачную инфраструктуру.** В мае 2024 г. немецкий производитель сельскохозяйственной техники Lemken столкнулся с кибератакой, из-за которой были приостановлены производственные процессы и заторможена обработка заказов. Аналогично, в ноябре 2024 г. атака программы-вымогателя парализовала IT-системы компании Schneider Electric и угрожала публикацией конфиденциальных данных при отказе от выкупа. Эти инциденты подчеркивают, что облачные сервисы не защищены от распространения шифровальщиков, особенно если отсутствуют офлайн-резервные копии и своевременное обнаружение атак;

– **неправильная конфигурация облачных ресурсов.** Часто причиной утечки данных становятся неустановленные обновления или ошибки настройки. Например, по данным Qualys, около 31 % бакетов AWS S3 остаются открытыми для публичного доступа, что может привести к экспонированию конфиденциальных файлов. Любые данные (ключи, резервные копии, данные пользователей), хранящиеся в таких открытых хранилищах, доступны злоумышленникам, что неоднократно приводило к инцидентам утечки персональной информации и коммерческой тайны;

– **компрометация учетных данных через социальную инженерию.** Фишинговые кампании и внутренние утечки (например, когда сотрудники передают учетные данные) остаются одной из ключевых причин взломов. Как показывает исследование SearchInform, почти половина компаний сталкивалась с утечками конфиденциальной информации за счет действий сотрудников. В облачном контексте это приводит к тому, что аккаунты с высокими правами могут быть скомпрометированы и злоумышленники получают доступ к облачным базам данных или администрированию сервисов [4].

Все эти примеры указывают на разнообразие и серьезность рисков: от технических ошибок до целевых атак. Статистика говорит об экспоненциальном росте подобных инцидентов: согласно аналитикам CrowdStrike, атаки, нацеленные именно на облачные инфраструктуры, выросли на 75 % в 2024 г.

Список источников

1. Бурсак А. Киберзащита на высоте // Ведомости : [сайт]. 2025. URL: https://clck.ru/3RXvDE (дата обращения: 22.10.2025).

2. Киреева О. Обзор рынка систем резервного копирования и восстановления данных // Anti-Malware : [сайт]. 2024. URL: https://clck.ru/3RXvPH (дата обращения: 22.10.2025).

3. UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion // Google Cloud : [website]. 2024. URL: https://clck.ru/3RXvbc (date of accessed: 22.10.2025).

4. Fortinet. What Is Cloud Encryption? How It Works & Use Cases // Fortinet : [website]. URL: https://clck.ru/3RXvtM (date of accessed: 22.10.2025).