DOI: 10.58168/PPSPM2025_42-49
УДК 004.9

МЕТОДЫ ЗАЩИТЫ ОБЛАЧНЫХ ХРАНИЛИЩ: АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ

С.Н. Волкова

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

В работе рассматриваются угрозы безопасности облачных хранилищ (утечки, несанкционированный доступ) и сравниваются традиционные методы защиты (шифрование, аутентификация) с инновациями: блокчейн для децентрализации и ИИ для проактивного мониторинга. Подчеркивается необходимость интеграции подходов, организационных мер и экономических вложений для минимизации рисков.

Ключевые слова: облачное хранилище, защита данных, обеспечение безопасности, угрозы безопасности, шифрование, аутентификация, несанкционированный доступ.

ANALYSIS OF DATA FOR FORECASTING SALES BY THE MOVING AVERAGE METHOD

S.N. Volkova

Voronezh State University of Forestry and Technologies named after G.F. Morozov

The work examines threats to the security of cloud storage (leaks, unauthorized access) and compares traditional protection methods (encryption, authentication) with innovations: blockchain for decentralization and AI for proactive monitoring. The necessity of integrating approaches, organizational measures, and economic investments to minimize risks is emphasized.

Key words: cloud storage, data protection, security, security threats, encryption, authentication, and unauthorized access.

В современном мире, наполненном цифровыми данными, облачные хранилища становятся основными хранилищами информации, что делает их мишенью для различных угроз. Основные типы угроз для облачных хранилищ включают утечки данных и несанкционированный доступ. Эти аспекты

оказывают значительное влияние на безопасность и надежность данных, хранящихся в облачных системах.

Утечки данных, как правило, происходят из-за ошибок в конфигурации систем безопасности, что позволяет злоумышленникам получать доступ к конфиденциальной информации. Например, в 2021 году утечка данных из популярного облачного сервиса была вызвана неправильной настройкой доступа к файлам, что привело к компрометации личных данных миллионов пользователей. Такие утечки — тревожный сигнал: если не следить за тем, кто и что видит в облаке, рано или поздно данные окажутся не там, где нужно. Политика конфиденциальности и регулярная проверка прав доступа — это не бюрократия, а базовая гигиена информационной безопасности.

Особенно уязвимы системы, для входа в которые достаточно одного пароля. Исследование McAfee, проведенное в 2020 году, показало, что более 70% компаний защищали свои облачные сервисы только паролем. Для злоумышленников это все равно что оставить дверь нараспашку — особенно когда фишинговые атаки стали массовыми. Выход один: включать многофакторную аутентификацию (MFA) везде, где это возможно, и не забывать обновлять устаревшие протоколы, такие как TLS 1.0 или старые версии OAuth.

Но даже самая надёжная техническая защита рушится из-за человека. Сотрудник, использующий пароль «123456» для корпоративного облака, или коллега, отправивший ссылку на внутренний документ «для удобства», — вот настоящие слабые места. Поэтому обучение персонала — это не формальность, которую можно провести раз в году, а постоянная работа. Без неё любые инвестиции в безопасность могут пойти насмарку. Изучение реальных случаев показывает, что угрозы облачным хранилищам эволюционируют, и трудность их выявления часто связана с высокой степенью интеграции этих технологий в повседневную жизнь. На фоне растущей сложности кибертехнологий, адекватные меры предосторожности, такие как шифрование данных и мониторинг сети, приобретают особую актуальность.

Чтобы надёжно защитить информацию в условиях постоянно меняющихся киберугроз, недостаточно полагаться только на технические средства. Важно вкладывать средства в обучение пользователей и подготовку персонала. Только комплексный подход, сочетающий в себе технологии, грамотную организацию процессов и осведомлённость людей, позволяет создать устойчивую систему безопасности и снизить риски утечки данных или несанкционированного доступа.

Основу защиты по-прежнему составляют проверенные методы: шифрование, аутентификация и контроль доступа. Шифрование преобразует данные в нечитаемый вид, делая их бесполезными без соответствующего ключа. Аутентификация подтверждает личность пользователя или системы, гарантируя, что доступ получит только тот, кто действительно имеет на это право. Контроль доступа, в свою очередь, определяет, какие именно действия разрешены каждому пользователю в зависимости от его роли.

Несмотря на свою эффективность, эти методы имеют слабые места. Например, даже самое надёжное шифрование становится бесполезным, если злоумышленник получает доступ к ключам. Кроме того, шифрование и расшифровка требуют дополнительных вычислительных ресурсов, что может замедлять работу систем.

Многофакторная аутентификация значительно повышает уровень защиты, но и она не гарантирует полной безопасности. Фишинг и другие методы социальной инженерии часто позволяют обойти даже сложные схемы проверки подлинности, особенно если пользователь не умеет распознавать угрозы.

Контроль доступа тоже не лишён недостатков. Настройка политик безопасности — непростая и трудоёмкая задача. Ошибки в конфигурации легко могут привести к тому, что пользователи получат больше прав, чем им действительно нужно. Такие избыточные привилегии становятся лазейками для злоумышленников, которые используют их для продвижения внутри системы.

Особенно остро эти проблемы проявляются при столкновении с такими угрозами, как APT (продвинутые постоянные угрозы). Такие атаки проводятся скрытно, методично и могут длиться месяцами. Они часто обходят даже самые строгие технические барьеры, используя человеческий фактор и недочёты в настройке систем.

Поэтому сегодня недостаточно просто поддерживать существующие механизмы — их нужно дополнять новыми решениями. Среди перспективных технологий особого внимания заслуживают блокчейн и искусственный интеллект.

Блокчейн — это децентрализованная структура, в которой данные записываются в связанные между собой блоки. Изменить такую запись практически невозможно без согласия большинства участников сети. Благодаря криптографической защите и прозрачности блокчейн может стать надёжной основой для хранения критически важной информации. Например, в банковской сфере он может повысить доверие к транзакциям и снизить риск мошенничества.

Искусственный интеллект, в свою очередь, помогает выявлять аномалии и подозрительную активность в режиме реального времени. Системы на основе машинного обучения анализируют поведение пользователей и сетевой трафик, выявляя отклонения, которые человек может упустить. Это позволяет обнаруживать угрозы на ранних стадиях — ещё до того, как они нанесут ущерб.

Таким образом, будущее кибербезопасности — за сочетанием традиционных методов, новых технологий и постоянного повышения квалификации людей, работающих с информацией. Только такой подход способен противостоять современным и будущим вызовам.

Если сравнивать блокчейн и ИИ с привычными инструментами вроде антивирусов или брандмауэров, разница бросается в глаза. Старые решения работают по чёткому принципу: «увидел угрозу — заблокировал». Они отлично справляются с известными вирусами или атаками, но беспомощны перед всем новым. Блокчейн и искусственный интеллект устроены иначе: они не ждут, пока что-то сломается, а пытаются предугадать проблему до того, как она возникнет.

Но не всё так гладко. Блокчейн, например, требует огромных вычислительных мощностей. Запись каждого обращения к файлу в распределённый реестр — звучит надёжно, но на практике это может в разы увеличить нагрузку на систему и счёт за облачные ресурсы. А ИИ, несмотря на всю свою «умность», легко ввести в заблуждение недостоверными данными. Если модель обучалась на искажённой или неполной информации, она начнёт видеть угрозы там, где их нет, или, наоборот, пропустит настоящую атаку. Так что и здесь без критического подхода не обойтись.

Несмотря на недостатки, блокчейн и искусственный интеллект уже сегодня приносят реальную пользу. Они не просто добавляют ещё один уровень защиты — они меняют сам подход: вместо того чтобы латать дыры после атак, мы начинаем создавать системы, которые умеют «чувствовать» угрозу заранее. И хотя ни одна технология не даёт стопроцентной гарантии, вместе они открывают новые возможности для защиты данных — особенно в условиях, когда угрозы становятся всё более изощрёнными.

Но полагаться только на новинки — опасная иллюзия. Настоящая безопасность рождается там, где проверенные решения работают в паре с инновациями. Например, шифрование данных — технология не новая, но в сочетании с ИИ, который отслеживает подозрительные попытки доступа, она становится гораздо эффективнее. То же касается многофакторной аутентификации: сама по себе она надёжна, но если добавить к ней

поведенческий анализ (когда система замечает, что пользователь вдруг начал скачивать файлы в 3 часа ночи с нового устройства), шансы пропустить злоумышленника резко снижаются.

Внедрение таких гибридных решений — непростая задача. Тот же блокчейн для регистрации событий безопасности звучит круто, но на практике требует чёткого понимания, какие именно события нужно записывать, как хранить цепочку и кто будет всё это отслеживать. А главное — нужны люди, которые в этом разбираются. Без команды, способной быстро реагировать на аномалии и принимать решения в стрессовой ситуации, даже самая умная система окажется бесполезной.

Важным шагом на пути к повышению безопасности является интеграция инноваций в существующие ИТ-архитектуры с минимальными затратами. Разработка гибридных решений, находящих баланс между защитой и производительностью, позволит организациям не только защитить данные, но и оптимально использовать ресурсы. Следовательно, реализация мер по защите данных должна учитывать экономические аспекты, чтобы не перегрузить бюджет компании. Экономические соображения играют ключевую роль в принятии решений относительно безопасности, особенно в контексте облачных технологий. С одной стороны, внедрение новых технологий требует значительных капиталовложений, в то время как с другой стороны, предотвратив потенциальные утечки данных, можно избежать значительных убытков. К примеру, внедрение многофакторной аутентификации может снизить риск утечки данных, но требует инвестиций в программное обеспечение и обучение сотрудников.

Сравнительный анализ затрат на различные технологии позволяет более осознанно подходить к выбору стратегии защиты. На практике это может включать использование облачных решений с внедренными сервисами безопасности, которые обычно предлагают относительно низкую стоимость по сравнению с самостоятельными разработками и внедрениями. Тем не менее, для точной оценки требуется учитывать весь жизненный цикл технологий, включая эксплуатационные расходы и возможные риски.

Некоторые компании прибегают к страхованию киберрисков как дополнительной мере, что снижает потенциальные финансовые последствия и создает дополнительный экономический стимул для вложений в безопасность. Тем не менее, необходимо помнить, что страхование не заменяет активные меры снижения рисков, а лишь служит их дополнением. Для эффективного

управления безопасностью необходимо интегрировать экономические соображения в управленческие решения.

Современные управленческие стратегии играют ключевую роль в обеспечении безопасности данных, особенно в контексте облачных технологий. Эти стратегии направлены на выработку комплексного подхода к защите информации, что включает в себя не только технические, но и организационные меры. Управление информационной безопасностью требует рассмотрения множества аспектов, начиная от человеческого фактора и заканчивая интеграцией сложных технологических решений. Хорошая стратегия обеспечения безопасности начинается не с покупки дорогих систем, а с понимания того, что именно может пойти не так и что делать, если это случится. Недостаточно просто поставить «щит»; нужно заранее продумать действия на случай, если его пробьют.

Технологии сами по себе не спасут, если в компании нет чётких правил: кто к чему имеет доступ, как реагировать на подозрительный вход в систему, куда сообщать о странной ссылке в письме. Эти правила должны быть простыми, понятными и — главное — работать на практике. Регулярные тренинги (не раз в год, а по мере появления новых угроз) и реальные проверки — например, имитация фишинга — помогают держать персонал в тонусе. Особенно важно не просто назначить «ответственного за безопасность», а создать рабочую группу, которая сможет ночью поднять тревогу, отключить угрозу и запустить восстановление. В 2023 году компании, у которых такая команда была готова к действиям, в среднем сократили ущерб от атак почти на 40 % (по данным IBM).

Но самое главное — это культура. Когда сотрудники не боятся сообщить, что «нажали на ссылку», а считают защиту данных частью своей работы, половина дела уже сделана. Безопасность — это не функция ИТ-отдела. Это привычка всей организации. Дополнительно, проведение аудитов и оценка рисков помогают своевременно выявлять слабые места в системе безопасности. Расширение знаний в области кибербезопасности позволяет поддерживать высокий уровень защиты данных и уменьшает вероятность ошибок, вызванных человеческим фактором.

В ходе исследования выявлены основные угрозы, с которыми могут столкнуться пользователи облачных хранилищ. Среди них были выделены атаки типа man-in-the-middle, проникновение злоумышленников в систему, а также нарушение конфиденциальности данных. Проведенный анализ показал, что комбинированное использование различных методов защиты, таких как

шифрование данных и многофакторная аутентификация, позволяет значительно повысить уровень безопасности. Кроме того, особое внимание уделено вопросу управления доступом. К примеру, внедрение ролевой модели управления, где каждый пользователь имеет четко определенные права доступа, значительно снижает риск несанкционированного доступа. Этот подход позволяет создавать более контролируемую среду, в которой безопасность данных становится приоритетом.

Подчеркивается важность постоянного развития в сфере кибербезопасности и адаптации существующих методов к новым вызовам. Всесторонний подход, основанный на комбинировании технологий и стратегий, способен успешно противостоять изменяющимся угрозам. Модернизация программного обеспечения и обучение пользователей являются обязательными мерами для поддержания высокого уровня защиты.

Следовательно, важно не только разработать эффективные технологии, но и обеспечить их устойчивое внедрение в повседневную практику. Развитие программ повышения осведомленности пользователей о киберугрозах и инструментах защиты необходимо интегрировать в стратегию безопасности.

Список литературы

1. Тимофеев А. Н. Основы защиты информации. — М.: Изд-во МГУ, 2019. — 456 с.

2. Петров Б. Ю. Информационная безопасность в облаке: вызовы и решения. — СПб.: Наука, 2020. — 379 с.

3. Сидоров В. Л. Облачные технологии и их защита. — Екатеринбург: Урал, 2021. — 312 с.

4. Иванов Д. И. Эволюция технологий шифрования // Журнал кибербезопасности. — 2022. — Т. 15, № 4. — С. 12-23.

5. Сергеев К. А. Роль искусственного интеллекта в безопасности данных // Информационные технологии. — 2021. — Т. 12, № 2. — С. 34-47.

6. Николаев С. П. Блокчейн как технология защиты информации // Международный журнал информационной безопасности. — 2020. — Т. 18, № 7. — С. 56-68.

References

1. Timofeev A. N. Fundamentals of Information Security. — Moscow: Moscow State University Press, 2019. — 456 p.

2. Petrov B. Yu. Information Security in the Cloud: Challenges and Solutions. — St. Petersburg: Nauka, 2020. — 379 p.

3. Sidorov V. L. Cloud Technologies and Their Protection. — Yekaterinburg: Ural, 2021. — 312 p.

4. Ivanov D. I. Evolution of Encryption Technologies // Journal of Cybersecurity. — 2022. — Vol. 15, No. 4. — P. 12-23.

5. Sergeev K. A. The Role of Artificial Intelligence in Data Security // Information Technologies. — 2021. — Vol. 12, No. 2. — P. 34-47.

6. Nikolaev S. P. Blockchain as a Technology for Protecting Information // International Journal of Information Security. — 2020. — Vol. 18, No. 7. — P. 56-68.