УДК 004.056

Артыков Ильнур Кимсанович, студент, Уфимский Университет Науки и Технологий, РФ, г. Нефтекамск

Аюпова Айгуль Рафисовна, доцент, кандидат физико-математических наук, Уфимский Университет Науки и Технологий, РФ, г. Нефтекамск

ТЕХНОЛОГИИ ZERO TRUST В ОБЛАЧНЫХ СРЕДАХ: ОЦЕНКА ЭФФЕКТИВНОСТИ НА ПРИМЕРЕ SAAS-РЕШЕНИЙ

Аннотация

В условиях стремительной цифровизации и активного перехода организаций к облачным вычислениям особую актуальность приобретает обеспечение информационной безопасности в средах SaaS. Традиционные периметровые модели защиты демонстрируют ограниченную эффективность в распределённых инфраструктурах, что обусловило развитие концепции Zero Trust. В статье проводится анализ принципов Zero Trust, рассматриваются архитектурные особенности их внедрения в облачных средах, а также оценивается эффективность данных технологий на примере SaaS-решений. Особое внимание уделяется механизмам аутентификации, авторизации, микросегментации и непрерывного мониторинга. Представлены критерии оценки эффективности, включая снижение рисков компрометации, повышение прозрачности доступа и адаптивность к современным угрозам.

Annotation

In the context of rapid digital transformation and widespread adoption of cloud computing, ensuring information security in SaaS environments becomes critically important. Traditional perimeter-based security models show limited effectiveness in distributed infrastructures, leading to the emergence of the Zero Trust concept. This article analyzes the principles of Zero Trust, examines architectural features of its implementation in cloud environments, and evaluates its effectiveness using

SaaS solutions as an example. Special attention is given to authentication, authorization, micro-segmentation, and continuous monitoring mechanisms. Evaluation criteria are presented, including risk reduction, improved access visibility, and adaptability to modern threats.

Ключевые слова: Zero Trust, облачные вычисления, SaaS, информационная безопасность, контроль доступа, микросегментация

Keywords: Zero Trust, cloud computing, SaaS, information security, access control, micro-segmentation

В условиях интенсивной цифровой трансформации экономики и широкого внедрения облачных вычислений наблюдается кардинальное изменение архитектуры информационных систем. Особое распространение получила модель предоставления программного обеспечения по подписке — SaaS, предполагающая удалённый доступ к функционалу приложений через сетевую инфраструктуру. Однако подобная трансформация сопровождается усложнением ландшафта угроз и увеличением числа потенциальных векторов атак.

Классическая парадигма защиты, основанная на разграничении внутренней и внешней сетевых зон, в современных условиях демонстрирует ограниченную применимость. Размывание сетевого периметра, вызванное использованием мобильных устройств, удалённого доступа и облачных сервисов, делает невозможным однозначное определение «доверенной» среды. В этой связи актуализируется необходимость перехода к принципиально иной модели обеспечения безопасности, ориентированной на непрерывную проверку всех субъектов взаимодействия.

Одной из таких моделей является концепция Zero Trust, предполагающая отказ от априорного доверия к любому элементу системы. В рамках данного подхода каждый запрос на доступ рассматривается как потенциально небезопасный и подлежит обязательной проверке с использованием совокупности аутентификационных и контекстных механизмов. Таким образом, формируется динамическая модель контроля доступа, не зависящая от сетевого расположения субъекта.

К числу базовых положений Zero Trust относятся:
– обязательная многофакторная аутентификация с учётом различных факторов риска;
– строгое ограничение прав доступа в соответствии с функциональной необходимостью;
– декомпозиция инфраструктуры на изолированные сегменты;
– постоянный сбор и корреляция событий безопасности;

– адаптивное управление политиками доступа на основе анализа контекста.

Применительно к SaaS-решениям реализация указанных принципов приобретает специфический характер. Это обусловлено тем, что значительная часть инфраструктурных компонентов находится вне зоны прямого контроля организации-потребителя. В связи с этим особое значение приобретают системы централизованного управления идентификацией (IAM), обеспечивающие унифицированный механизм аутентификации и авторизации пользователей в распределённой среде.

Дополнительный уровень защиты формируется за счёт внедрения многофакторной аутентификации, включающей сочетание различных категорий факторов: знание (пароль), владение (токен или устройство) и биометрические характеристики. В ряде случаев используются адаптивные схемы, при которых требования к аутентификации варьируются в зависимости от уровня риска конкретной сессии.

Существенным элементом рассматриваемой модели выступает микросегментация, позволяющая реализовать изоляцию ресурсов на более детальном уровне по сравнению с традиционным сетевым разделением. В контексте SaaS это выражается в разграничении доступа к отдельным сервисам, модулям или данным с применением политик, ориентированных на конкретные роли и сценарии использования. Подобный подход существенно ограничивает возможности латерального перемещения злоумышленника внутри системы.

Неотъемлемой составляющей Zero Trust является организация непрерывного мониторинга и интеллектуального анализа событий. Для этих целей применяются системы классов SIEM и UEBA, обеспечивающие агрегацию данных о действиях пользователей и автоматическое выявление аномалий. Использование методов машинного обучения позволяет повысить точность детектирования отклонений и снизить количество ложных срабатываний.

Оценка результативности внедрения Zero Trust в SaaS-средах должна

носить комплексный характер и учитывать как технические, так и организационные показатели. В качестве ключевых критериев целесообразно выделить:

1. **Снижение вероятности реализации атак.** Многоуровневая проверка доступа и контекстный анализ существенно усложняют эксплуатацию уязвимостей, связанных с компрометацией учетных данных.
2. **Локализация последствий инцидентов.** Использование микросегментации препятствует распространению атаки за пределы скомпрометированного сегмента.
3. **Повышение наблюдаемости процессов доступа.** Наличие детализированных журналов и механизмов анализа позволяет формировать полное представление о действиях пользователей.
4. **Сокращение времени реагирования.** Автоматизация процессов обнаружения и обработки инцидентов способствует ускорению реакции на угрозы.
5. **Соответствие требованиям регуляторов.** Принципы Zero Trust коррелируют с международными стандартами в области информационной безопасности.

Несмотря на значительный потенциал, внедрение Zero Trust сопровождается рядом сложностей. К ним относятся необходимость глубокой ревизии существующей ИТ-инфраструктуры, интеграция разнородных систем, а также повышение требований к квалификации персонала. Кроме того, на начальном этапе возможно увеличение нагрузки на систему и снижение удобства для конечных пользователей.

Сравнение традиционной периметровой модели с подходом Zero Trust показывает, что последняя обеспечивает более высокий уровень устойчивости к современным киберугрозам. Это достигается за счёт отказа от статических границ безопасности и перехода к динамическому контролю каждого запроса на доступ.

Анализ практических кейсов внедрения Zero Trust в SaaS-решениях свидетельствует о том, что максимальный эффект достигается при комплексной реализации всех компонентов данной модели. Частичное внедрение не позволяет в полной мере раскрыть её потенциал и может приводить к формированию уязвимых участков в системе защиты.

Таким образом, концепция Zero Trust представляет собой логичный этап эволюции подходов к обеспечению информационной безопасности в условиях облачных вычислений. Её применение в SaaS-средах способствует не только снижению рисков, но и формированию более гибкой и адаптивной системы защиты. Перспективы дальнейшего развития связаны с внедрением интеллектуальных механизмов анализа, автоматизацией управления политиками безопасности и унификацией стандартов реализации данной концепции.

Список литературы

1. Rose S., Borchert O., Mitchell S., Connelly S. Архитектура Zero Trust. NIST Special Publication 800-207. 2020. URL: https://doi.org/10.6028/NIST.SP.800-207
2. Chandramouli R., Butcher Z. Модель архитектуры Zero Trust для облачных сред. NIST SP 800-207A. 2023. URL: https://doi.org/10.6028/NIST.SP.800-207A
3. Kovacevic I., Stojkov M., Simic M. Аутентификация и управление идентификацией на основе модели Zero Trust. arXiv. 2024. URL: https://arxiv.org/abs/2410.21870
4. Chen X., Feng W., Ge N., Zhang Y. Архитектура Zero Trust для безопасности сетей нового поколения. arXiv. 2022. URL: https://arxiv.org/abs/2203.07716
5. Cloud Security Alliance. Руководство по обеспечению безопасности облачных вычислений. URL: https://cloudsecurityalliance.org

References

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. URL: https://doi.org/10.6028/NIST.SP.800-207
2. Chandramouli R., Butcher Z. Zero Trust Architecture Model for Cloud Environments. NIST SP 800-207A. 2023. URL: https://doi.org/10.6028/NIST.SP.800-207A
3. Kovacevic I., Stojkov M., Simic M. Authentication and Identity Management Based on Zero Trust Security Model. arXiv. 2024. URL: https://arxiv.org/abs/2410.21870
4. Chen X., Feng W., Ge N., Zhang Y. Zero Trust Architecture for 6G Security. arXiv. 2022. URL: https://arxiv.org/abs/2203.07716

5. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. URL: https://cloudsecurityalliance.org