Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/55-229**
Ссылка для цитирования этой статьи:
Гавкина М.С., Садыхов М.Р., Тупиков К.А. Интеллектуальная система управления сетевым доступом и кибербезопасностью // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2026. №1

УДК 004.056.3 DOI:10.24412/2541-9269-2026-1-26-30

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ СЕТЕВЫМ ДОСТУПОМ И КИБЕРБЕЗОПАСНОСТЬЮ

М.С. Гавкина[1], М.Р. Садыхов[1], К.А. Тупиков[1],
[1]Саратовский государственный технический университет имени Гагарина Ю.А.,
Россия, Саратов, April-18@inbox.ru

INTELLECTUAL SYSTEM ACCESS AND CYBERSECURITY MANAGEMENT SYSTEM

M.S. Gavkina[1], M.R. Sadykhov[1], K.A. Tupikov[1]
[1]Yuri Gagarin State Technical University of Saratov,
Russia, Saratov, April-18@inbox.ru

Аннотация. В условиях стремительной цифровизации и роста числа киберугроз вопросы управления сетевым доступом и защиты корпоративной инфраструктуры становятся критически важными для организаций любого масштаба. В статье представлена автоматизированная система доступа АСД (AccessSfera**)** — отечественная платформа класса Network Access Control (NAC), предназначенная для централизованного контроля подключений, анализа сетевого трафика и автоматического реагирования на инциденты безопасности. Рассматриваются архитектура системы, ключевые функциональные возможности, практическая ценность для бизнеса и конкурентные преимущества AccessSfera на рынке решений кибербезопасности.

Ключевые слова: автоматизированная система доступа, кибербезопасность, киберинцидент, файрволы.

Abstract. In the context of rapid digitalization and an increasing number of cyber threats, managing network access and protecting corporate infrastructure has become critical for organizations of all sizes. This article introduces the Automated Access System (AccessSfera), a domestic Network Access Control (NAC) platform designed for centralized connection control, network traffic analysis, and automated response to security incidents. It explores the system's architecture, key features, business value, and competitive advantages in the cybersecurity solution market.

Keywords: automated access system, cybersecurity, cyber incident, firewalls.

Современные корпоративные сети больше не ограничиваются офисными компьютерами и локальными серверами. Сегодня в инфраструктуре компаний присутствуют удалённые сотрудники, мобильные устройства, IoT-оборудование, виртуальные среды и облачные сервисы. Такое разнообразие точек доступа значительно усложняет контроль безопасности.

При этом статистика показывает устойчивый рост числа киберинцидентов: утечки данных, внутренние угрозы, несанкционированный доступ, атаки через уязвимые устройства. Во многих организациях контроль сетевого доступа до сих пор осуществляется вручную или с помощью разрозненных инструментов, что повышает вероятность ошибок и замедляет реакцию на угрозы.

В этих условиях особенно востребованы решения, способные обеспечить **единый, автоматизированный и интеллектуальный контроль доступа** к сетевым ресурсам [1].

Цифровая трансформация бизнеса сопровождается не только ростом эффективности, но и увеличением уязвимостей. Использование облачных сервисов, удалённых рабочих мест, мобильных устройств и IoT-систем приводит к тому, что классические периметры безопасности теряют актуальность. Компании больше не могут полагаться исключительно на файрволы и антивирусы.

Особую опасность представляют внутренние угрозы — ошибки сотрудников, использование несанкционированных устройств, компрометация учётных записей. В таких условиях критически важно иметь инструмент, который позволяет **не просто контролировать доступ, а понимать контекст каждого подключения** [2].

Что такое АСД (AccessSfera)

АСД (AccessSfera) — это автоматизированная система управления сетевым доступом и кибербезопасностью, объединяющая в одной платформе функции контроля подключений, анализа трафика, мониторинга угроз и реагирования на инциденты.

Система относится к классу NAC (Network Access Control), но при этом выходит за рамки классических решений, дополняя их поведенческим анализом, AI-модулями и расширенной аналитикой. AccessSfera позволяет администратору не только контролировать, кто подключается к сети, но и понимать, как именно ведёт себя каждое устройство и пользователь [3].

Архитектура и принцип работы

Архитектура AccessSfera построена по модульному принципу, что обеспечивает гибкость, масштабируемость и возможность адаптации под инфраструктуру конкретной организации.

Основные компоненты системы:

— модуль управления доступом и VLAN;
— подсистема аутентификации и авторизации;
— модуль мониторинга сетевого трафика;

— IDS/IPS-компонент;
— AI-модуль поведенческого анализа;
— система логирования и аудита;
— интерфейс администратора и аналитическая панель

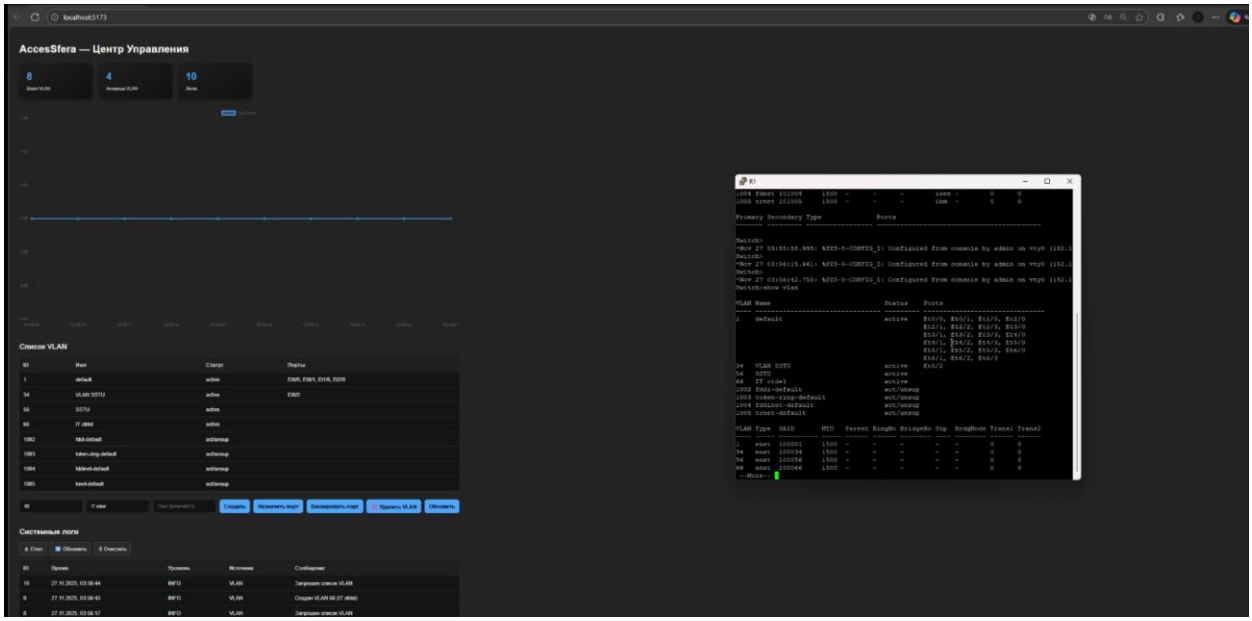

Рисунок 1 – Начальный интерфейс AccessSfera

Все компоненты работают в едином пространстве управления, что исключает необходимость использования нескольких несвязанных продуктов.

Ключевые функциональные возможности

Централизованное управление доступом

АСД обеспечивает полный контроль над сетевыми подключениями. Администратор может в реальном времени назначать роли, управлять VLAN, ограничивать доступ к ресурсам и создавать политики безопасности для различных групп пользователей и устройств [4].

Многофакторная аутентификация

Поддержка MFA значительно повышает уровень защиты и снижает риск компрометации учетных данных, особенно в распределённых и гибридных сетях [5].

Мониторинг и анализ сетевого трафика

Встроенные механизмы IDS/IPS анализируют трафик в реальном времени, выявляя подозрительные активности, попытки вторжений и аномалии в поведении сети [6].

Поведенческий анализ на основе ИИ

Одной из ключевых особенностей AccessSfera является использование алгоритмов машинного обучения. Система формирует поведенческие профили пользователей и устройств, выявляет отклонения от нормы и прогнозирует потенциальные угрозы ещё до того, как они приведут к инциденту [7].

Автоматическое реагирование на угрозы

При обнаружении подозрительной активности AccessSfera способна автоматически изолировать устройство, ограничить его доступ или перевести в безопасный сегмент сети, минимизируя последствия атаки [8].

Журналирование и аудит

Все действия пользователей и администраторов фиксируются в защищённых журналах. Это важно как для расследования инцидентов, так и для соблюдения требований регуляторов [9].

Интеграция и внедрение

AccessSfera разрабатывается с учётом необходимости быстрого и бесшовного внедрения. Система интегрируется с:

— Active Directory;
— SIEM и SOC-платформами;
— сетевым оборудованием;
— системами логирования и мониторинга.

Это позволяет использовать AccessSfera в существующей инфраструктуре без масштабных изменений и длительного обучения персонала [10].

Тарифная модель

Платформа распространяется по подписочной модели и включает несколько тарифных планов:

— **Контроль Lite** — базовый функционал управления доступом;
— **Контроль+** — расширенная безопасность и мониторинг;
— **Intellect PRO** — максимальный пакет с AI-аналитикой и поддержкой 24/7.

Такая модель делает систему доступной как для малого и среднего бизнеса, так и для крупных организаций.

Важным аспектом системы является ведение защищённых журналов событий и аудит действий пользователей и администраторов. Все операции фиксируются в зашифрованном виде, что позволяет проводить расследование инцидентов, confirms соответствие требованиям регуляторов и формировать отчётность для руководства. Это особенно актуально для организаций, работающих в регулируемых отраслях, где вопросы информационной безопасности напрямую связаны с юридической ответственностью [11].

С точки зрения внедрения AccessSfera ориентирована на минимальное вмешательство в существующую инфраструктуру. Система поддерживает интеграцию с распространёнными корпоративными сервисами, такими как Active Directory и системы управления событиями безопасности, что позволяет использовать уже имеющиеся ресурсы без необходимости полной перестройки сети. Такой подход делает внедрение более быстрым и экономически оправданным [12].

Экономическая эффективность выражается не только в снижении рисков киберинцидентов, но и в оптимизации затрат на безопасность. Использование единой платформы позволяет отказаться от нескольких разрозненных решений,

сократить расходы на лицензирование и обслуживание, а также снизить потери, связанные с простоями и восстановлением после атак. Для бизнеса это означает более предсказуемые затраты и повышение устойчивости к внешним и внутренним угрозам.

Перспективы развития связаны с дальнейшим расширением интеллектуальных функций системы, внедрением принципов Zero Trust и углублением аналитики. По мере роста объёмов данных система будет становиться более точной и автономной, превращаясь в активного участника процессов обеспечения безопасности, а не просто инструмент мониторинга [13].

Таким образом, автоматизированная система доступа AccessSfera является фундаментальным элементом современной цифровой инфраструктуры, позволяющим организациям эффективно управлять сетевым доступом, повышать уровень кибербезопасности и обеспечивать стабильность бизнес-процессов в условиях постоянно меняющихся угроз

Литература

1. Иванов, А. Н. Управление сетевым доступом (NAC): принципы и практики. Журнал кибербезопасности, 2021.
2. Петрова, Е. В., Смирнов, Д. Р. Архитектура Zero Trust: концепции и внедрение. Вестник информационной безопасности, 2022.
3. Кузнецова, Л. Поведенческий анализ в кибербезопасности: ML-подходы и приложения. Обзор ACM, 2020 (русский перевод/аналоги).
4. ФСТЭК России: рекомендации по безопасной интеграции сетевых решений в hybrid-сетях, 2020–2023.
5. CERT-Russia: практики противодействия киберугрозам в корпоративных сетях, 2021.
6. Smith J. Network Access Control (NAC): Principles and Practices. Journal of Cybersecurity, 2022.
7. Kumar A., et al. Zero Trust Architecture: Concepts, Implementation and Challenges. IEEE Communications Surveys & Tutorials, 2023.
8. North R. Behavioral Analytics for Cybersecurity: ML Approaches and Applications. ACM Computing Surveys, 2021.
9. Gartner. Market Guide for NAC Solutions. Gartner Research, 2023.
10. ENISA. Threat Landscape and Mitigation in Hybrid Networks. European Union Agency for Cybersecurity, 2020.
11. Secure Access Service Edge (SASE) Overview. Forrester Report, 2021.
12. ISO/IEC 27001 standard. Information security management systems, latest edition.
13. Kravchenko L. Integrating SIEM/SOC with NAC: Best Practices. InfoSec Journal, 2022.