УДК – 004.056.53

Полшков Дмитрий Владимирович

Студент

Федеральное государственное бюджетное учреждение высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА), просп. Вернадского, д. 78, Москва, 119454, Россия, базовая кафедра №234 – управляющих ЭВМ

Polshkov Dmitriy Vladimirovich

Student

Federal State Budgetary Institution of Higher Education "MIREA – Russian Technological University" (RTU MIREA), ave. Vernadsky, 78, Moscow, 119454, Russia, Basic Department No. 234 – Control Computers

ОБЕСПЕЧЕНИЕ АВТОМАТИЗАЦИИ ДОСТУПА К ДАННЫМ ПРИ МОНИТОРИНГЕ ВЫБРОСОВ ПАРНИКОВЫХ ГАЗОВ НА ОСНОВЕ АРХИТЕКТУРЫ ZERO TRUST NETWORK ACCESS

Аннотация: Рассматривается подход к автоматизации защищённого доступа к данным мониторинга выбросов парниковых газов в гибридной инфраструктуре ФГБУ «ИГКЭ». Традиционные VPN-решения не обеспечивают требуемого уровня гранулярности и требуют ручных операций администрирования. Предложена эталонная архитектура Zero Trust Network Access, реализованная на базе свободно распространяемого программного обеспечения с открытым исходным кодом. Приведены модель взаимодействия компонентов PEP, PDP и PIP, конфигурационные решения на основе JWT-токенов и атрибутной модели управления доступом, а также результаты функционального тестирования. Показано, что внедрение архитектуры позволяет автоматизировать процессы аутентификации и авторизации, снизить риски горизонтального перемещения злоумышленника с высокого уровня до низкого и обеспечить тиражируемость решения в организациях аналогичного профиля без дополнительных лицензионных затрат.

Abstract: The paper considers an approach to automating secure access to greenhouse gas monitoring data in the hybrid infrastructure of the Federal State Budgetary Institution "Institute for Global Climate and Ecology". Traditional VPN solutions do not provide the required level of granularity and require manual administration. The paper proposes a reference architecture for Zero Trust Network Access based on freely available open-source software. The paper presents a model for the interaction between PEP, PDP, and PIP components, configuration solutions based on JWT tokens and an attribute-based access control model, and the results of functional testing. It has been shown that the implementation of the architecture allows for the automation of authentication and authorization processes, reduces the risks of an attacker's horizontal movement from a high level to a low level, and ensures the

scalability of the solution in organizations with similar profiles without additional licensing costs.

Ключевые слова: Zero Trust Network Access, автоматизация доступа, гибридная инфраструктура, мониторинг выбросов, парниковые газы, JWT, атрибутное управление доступом, контейнеризация, Docker.

Keywords: Zero Trust Network Access, access automation, hybrid infrastructure, emissions monitoring, greenhouse gases, JWT, attribute-based access control, containerization, Docker.

Введение

Мониторинг выбросов парниковых газов является одной из приоритетных задач государственной экологической политики Российской Федерации. Федеральное государственное бюджетное учреждение «Институт глобального климата и экологии имени академика Ю.А. Израэля» выполняет расчёты национального кадастра антропогенных выбросов из источников и абсорбции поглотителями парниковых газов. Все расчеты и данные размещены в локальном центре обработке данных, к которому необходимо предоставлять удаленный доступ.

Доступ к этим данным должен предоставляться как штатным сотрудникам, так и внешним научным партнёрам. При этом сотрудникам разрешено использование личных устройств (концепция BYOD), что расширяет увеличивает количество конечных точек и делает актуальной задачу автоматизации и защиты доступа. Предоставление доступа к указанным информационным ресурсам регламентируется требованиями федеральных законов и постановлениями правительства РФ.

Традиционные решения предоставления доступа, используемые ранее в организации, работали на базе открытого VPN протокола. Такие решения обладают следующими недостатками: они предоставляют избыточный сетевой доступ ко всей подсети ЦОД, а не к конкретным приложениям; не обеспечивают непрерывной верификации контекста запроса; не имеют встроенных механизмов оценки состояния конечных устройств; требуют ручного управления сертификатами для временных учётных записей внешних партнёров (Sarkar et al.,

2022). В условиях размытия сетевого периметра это приводит к высоким рискам горизонтального перемещения злоумышленника (lateral movement) и утечки критичных данных.

Данная статья описывает разработанный подход к автоматизации защищённого доступа к данным мониторинга выбросов парниковых газов на основе архитектуры Zero Trust Network Access (ZTNA), формализованной в стандарте NIST SP 800-207 (Rose et al., 2020) и обеспечивающей гранулярный контроль доступа при минимизации ручных операций администрирования.

Цель исследования

Разработка подхода к автоматизации защищённого доступа к данным мониторинга выбросов парниковых газов в гибридной инфраструктуре научного учреждения. Методы: анализ угроз гибридной инфраструктуры, проектирование эталонной архитектуры ZTNA на основе стандарта NIST SP 800-207, сравнительный анализ методов предоставления удаленного доступа, реализация программного комплекса на базе открытого ПО с использованием контейнеризации, функциональное тестирование и качественная оценка снижения рисков.

Методы и материалы

Разработка архитектуры автоматизированного доступа базируется на стандарте NIST SP 800-207 «Zero Trust Architecture», который определяет три ключевых логических компонента: Policy Enforcement Point (PEP) — компонент обеспечения политик, перехватывающий запросы к защищаемым ресурсам; Policy Decision Point (PDP) — компонент принятия политик, анализирующий запрос на основе динамических сигналов; Policy Information Point (PIP) — источник атрибутивной информации (идентичность, состояние устройства, контекст сессии).

В качестве технологической платформы использована система контейнеризации Docker с оркестратором Docker Compose, что обеспечивает

изоляцию компонентов и воспроизводимость развёртывания. Все программные средства выбраны из категории свободно распространяемого программного обеспечения с открытым исходным кодом. Веб-сервер Caddy с плагином caddy-security выполняет функции PEP. Сервер аутентификации Authelia реализует логику PDP. Хранилище данных Redis используется в качестве PIP для хранения состояния сессий; веб-интерфейс FileBrowser обеспечивает безагентский доступ к файловым хранилищам ЦОД.

Аутентификация и авторизация реализованы на основе протокола OAuth 2.0 и расширения OpenID Connect с использованием JSON Web Token в формате JWT (Indran, Alwi, 2024). Управление доступом построено на атрибутной модели ABAC (Attribute-Based Access Control), где решение о предоставлении доступа принимается на основе утверждений (claims), содержащихся в JWT-токене, в частности — групповой принадлежности пользователя.

Результаты

Разработанная эталонная архитектура ZTNA включает три функциональных слоя. Слой доступа (Access Plane) представлен обратным прокси-сервером Caddy, который является единственной точкой входа из внешней сети, терминирует TLS-соединения с использованием автоматически получаемых сертификатов по протоколу ACME и осуществляет первичную валидацию JWT-токенов. Слой управления (Control Plane) содержит сервер Authelia и хранилище Redis, не имеющие прямого доступа из интернета. Слой защищаемых ресурсов (Data Plane) включает веб-интерфейсы научных сервисов, в том числе портал доступа к данным кадастра выбросов парниковых газов, которые также полностью скрыты от внешней сети.

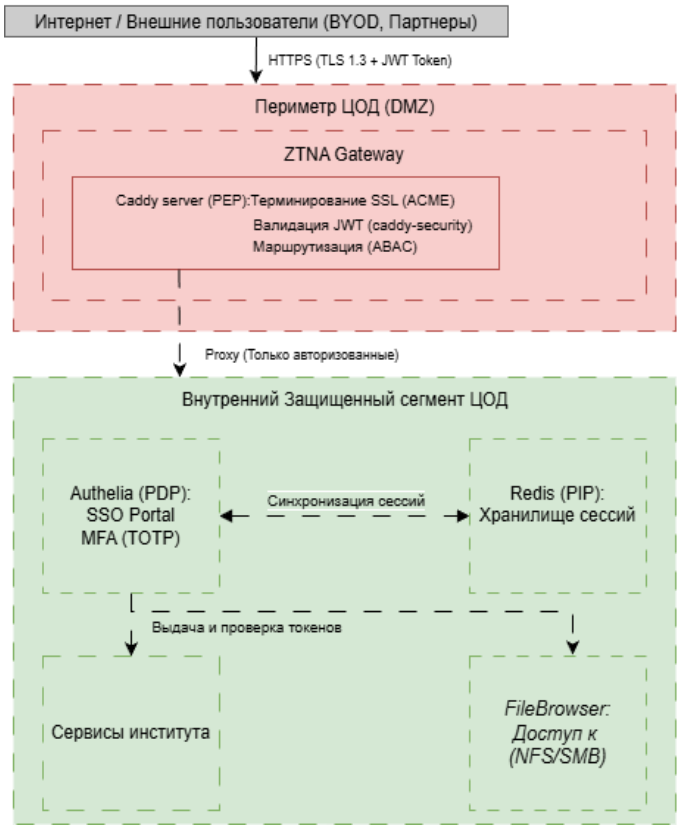

Рисунок 1. Структурная схема эталонной архитектуры ZTNA

Источник: анализ автора

Модель автоматизированного управления доступом реализует полный цикл OAuth 2.0 Authorization Code Flow. При попытке доступа к защищённому ресурсу PEP (Caddy) проверяет наличие валидного JWT-токена. Если токен отсутствует, пользователь перенаправляется на портал PDP (Authelia), где проходит двухфакторную аутентификацию (пароль + TOTP). После успешной проверки PDP генерирует подписанный токен, сохраняет сессию в Redis и возвращает пользователя обратно на исходный URL. PEP верифицирует токен, извлекает из его полезной нагрузки атрибуты, включая групповую принадлежность, и принимает решение о предоставлении или отказе в доступе на основе политик ABAC, заданных декларативно в файлах Caddyfile и configuration.yml.

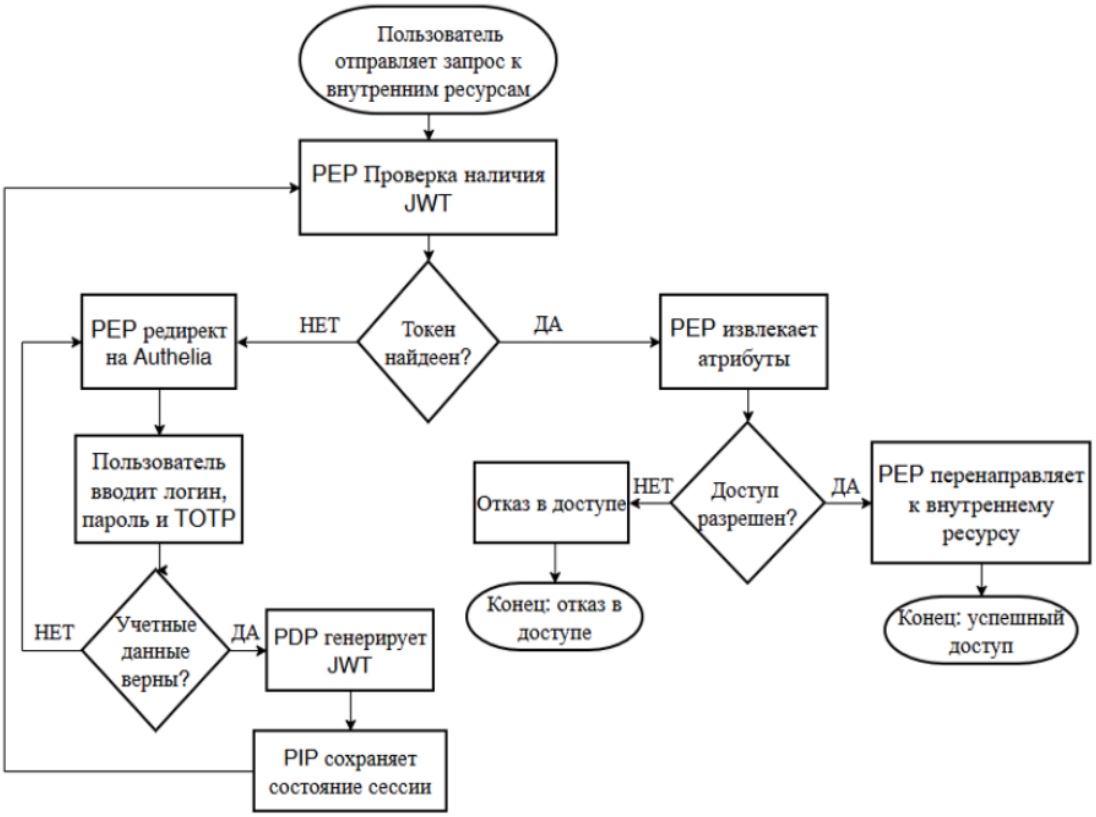

Рисунок 2. Блок-схема алгоритма взаимодействия компонентов ZTNA

Источник: анализ автора

Система удалённого доступа на базе OpenVPN функционирует на сетевом уровне (L3), предоставляя пользователю после успешной аутентификации доступ ко всей подсети ЦОД. Разработанное решение на основе ZTNA, напротив, работает на прикладном уровне (L7) и реализует доступ исключительно к конкретным приложениям и сервисам. Принципиальные различия между двумя подходами систематизированы в Таблице 1.

Таблица 1. Сравнение разработанного решения на основе ZTNA и VPN-решения для удалённого доступа

Критерий	**Текущее решение (OpenVPN)**	**Разработанное решение (ZTNA)**
Уровень модели OSI	Сетевой (L3)	Прикладной (L7)
Объект доступа	Подсеть ЦОД	Конкретное приложение (URL)

Видимость ресурсов	Все сервисы видны при сканировании	Ресурсы скрыты (Darknet)
Модель доступа	Имплицитное доверие (доступ после однократной аутентификации)	Эксплицитная верификация каждого запроса
Аутентификация	Однофакторная (логин/пароль)	Многофакторная (логин/пароль + TOTP)
Управление политиками	Статическое (IP-адреса, порты)	Динамическое, атрибутное (ABAC на основе JWT-claims)
Непрерывная верификация	Отсутствует	Реализована (проверка JWT при каждом запросе)
Оценка состояния устройства	Отсутствует	Частично (перспектива интеграции с EDR)
Установка клиентского ПО	Требуется VPN-клиент	Не требуется (agentless, доступ через браузер)
Поддержка внешних партнёров	Ручное управление сертификатами	Автоматическая авторизация по группам в JWT
Защита от lateral movement	Отсутствует (доступна вся подсеть)	Обеспечена (микросегментация L7)
Зависимость от вендора	Отсутствует (open source)	Отсутствует (open source)
Соответствие ГОСТ Р ИСО/МЭК 27001-2021	Частичное	Полное (MFA, аудит, управление сессиями)

Источник: анализ автора

Для автоматизации развёртывания разработан сценарий `deploy.sh`, который выполняет проверку наличия Docker, создание структуры каталогов, генерацию криптографических ключей длиной 64 байта для JWT и сессионных cookie, и запуск четырёх контейнеризированных сервисов одной командой. Время приведения системы в рабочее состояние на новом узле не превышает пяти минут, что полностью исключает ручное конфигурирование и снижает вероятность ошибок администрирования.

Были разработаны сценарии использования для функционального тестирования на тестовом стенде, включавшем две виртуальные машины под

управлением Ubuntu Server 24.04 LTS. Данное тестирование подтвердило работоспособность предложенного решения по пяти сценариям (таблица 2).

Таблица 2. Результаты функционального тестирования

Сценарий	Ожидаемый результат	Фактический результат
Запрос без аутентификации к защищённому ресурсу	Перенаправление на портал входа (HTTP 302)	Соответствует
Вход с валидными учётными данными и TOTP-кодом	Доступ к ресурсу разрешён	Соответствует
Запрос пользователя без требуемой роли	Отказ в доступе (HTTP 403)	Соответствует
Запрос с истекшим JWT-токеном	Блокировка, перенаправление на повторный вход	Соответствует
Сканирование портов ЦОД утилитой nmap	Открыты только порты 80 и 443	Соответствует

Источник: анализ автора

Качественная оценка эффективности на основе матрицы угроз, построенной по результатам предпроектного обследования инфраструктуры ФГБУ «ИГКЭ», продемонстрировала существенное снижение рисков (таблица 3).

Таблица 3. Оценка снижения рисков при переходе к ZTNA

Угроза	Уровень риска (As-Is, OpenVPN)	Уровень риска (To-Be, ZTNA)	Обоснование снижения
Компрометация учётных данных и Lateral Movement	Высокий	Низкий	Микросегментация на уровне L7, сокрытие ресурсов (Darknet), отсутствие сетевого маршрута к подсети ЦОД
Доступ с недоверенных устройств (BYOD)	Высокий	Средний	Agentless-доступ, многофакторная аутентификация, отсутствие необходимости установки VPN-клиента

Отсутствие гранулярного контроля для внешних партнёров	Высокий	Низкий	ABAC-политики на основе JWT-claims, доступ к конкретным URL, а не к подсети

Источник: анализ автора

Выводы

В статье проведён анализ подходов к организации удалённого доступа в гибридных инфраструктурах государственных научных учреждений. Научная новизна заключается в разработке эталонной архитектуры ZTNA, адаптированной к специфике учреждения, выполняющего мониторинг выбросов парниковых газов, и реализованной исключительно на базе открытого программного обеспечения. Установлено, что традиционные VPN-решения и коммерческие ZTNA-продукты не удовлетворяют одновременно требованиям гранулярного контроля, независимости от вендоров и соответствия российским нормативным документам. Разработанное решение обеспечивает полную автоматизацию процессов аутентификации, авторизации и управления доступом, а функциональное тестирование подтвердило его работоспособность. Практическая значимость заключается в возможности тиражирования архитектуры в других научных учреждениях без дополнительных лицензионных затрат.

Список источников и литературы:

1. Sarkar S., Choudhary G., Shandilya S.K., Hussain A., Kim H. 2022. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. – Sustainability, vol. 14, No. 17, Article 10756.

2. Rose S., Borchert O., Mitchell S., Connelly S. 2020. NIST SP 800-207. Zero Trust Architecture. – Gaithersburg, MD, National Institute of Standards and Technology, 59 p.

3. Indran S., Alwi N.H.M. 2024. Systematic Literature Review on Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA)

Implementation to Ensure Secure Access. – Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 56, No. 4, p. 76-89.

4. ГОСТ Р ИСО/МЭК 27001-2021. 2024. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М., Российский институт стандартизации, 23 с.

5. Caddy Security: Plugin for Caddy v2. 2024–2026. – Электронный ресурс. URL: https://github.com/greenpau/caddy-security (дата обращения: 10.04.2026).

6. RFC 7519. 2015. JSON Web Token (JWT). – Internet Engineering Task Force (IETF), 30 p.

7. RFC 8446. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. – Internet Engineering Task Force (IETF), 160 p.