УДК 004.771

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ УДАЛЁННОГО ДОСТУПА: VPN VS ZTNA И РОЛЬ SASE; ПРИМЕНЕНИЕ TOGAF В ПРОЕКТИРОВАНИИ ZERO TRUST

Наталья Викторовна Картечина
кандидат сельскохозяйственных наук, доцент
kartechnatali@mail.ru
Никита Алексеевич Улыбышев
студент
avtocad68@yandex.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. Рост удалённой работы, гибридной ИТ-инфраструктуры (on-prem + IaaS + SaaS) и атак на идентичность снижает эффективность классического подхода к удалённому доступу, основанного на модели «туннель в сеть» (VPN), как универсального механизма безопасного доступа к корпоративным ресурсам. В статье выполняется сравнительный анализ VPN и ZTNA (Zero Trust Network Access) по архитектурной «единице доступа», поверхности атаки и рискам латерального перемещения, учёту контекста и возможностям аудита. Отдельно показано, как методология TOGAF (ADM) помогает формализовать требования, описать целевую архитектуру и спланировать миграцию к Zero Trust, а также обеспечить управляемость внедрения через трассируемость требований и архитектурное управление.

Ключевые слова: удалённый доступ, VPN, ZTNA, SASE, Zero Trust, TOGAF ADM, контекстный доступ, сегментация, аудит.

Традиционная логика удалённого доступа долгое время строилась вокруг расширения корпоративной сети до пользователя: «создать защищённый туннель (VPN) – и пользователь оказывается «внутри»». При этом безопасность нередко опиралась на допущение, что внутренний сегмент сети более доверенный, чем внешняя среда.

Современные условия меняют исходные допущения:

1) Периметр стал «размытым»: приложения и данные распределены между on-prem, IaaS и Saas;

2) Идентичность стала основной целью атак: фишинг, перехват токенов, атаки на MFA, компрометация конечных устройств;

3) Сетевой контроль и сегментация часто недостаточны: компрометация одной учётной записи/устройства может дать возможность перемещения внутри сети;

4) Аудит и трассируемость стали обязательными: необходимо доказуемо отвечать на вопросы «кто», «к чему», «почему разрешено», «на основании какой политики», «с какого устройства», «в какой сессии».

Следовательно, требуется модель, где доступ выдаётся не «в сеть», а «к конкретному приложению/сервису», с учётом контекста и постоянной проверкой доверия по событиям и сигналам риска, что соответствует подходу Zero Trust и реализуется, в частности, через ZTNA.

VPN (Virtual Private Network) – защищённый туннель, предоставляющий сетевую связность (обычно L3/L4) между пользователем и корпоративной сетью/подсетями. В зависимости от реализации VPN может ограничиваться ACL/сегментацией/бастионами, однако базовая логика часто начинается с предоставления сетевой достижимости и переноса контроля внутрь периметра.

Zero Trust – модель, основанная на принципах:

– never trust, always verify (не доверять по умолчанию),

– least privilege (минимально необходимые привилегии),

– assume breach (предположение компрометации).

ZTNA (Zero Trust Network Access) – модель доступа к конкретным приложениям/сервисам на основе политики, идентичности и контекста (роль, состояние устройства, риск, география и др.), как правило без предоставления пользователю L3-достижимости и «видимости» адресного пространства корпоративной сети. Доступ обычно устанавливает брокеры на уровне приложения/сессии.

SASE (Secure Access Service Edge) – архитектурная модель облачной доставки сетевых и защитных функций (например, ZTNA, SWG, CASB, FWaaS), приближающая контроль к пользователю через распределённые точки присутствия (PoP). Важно различать: ZTNA – механизм доступа, а SASE – способ архитектурной доставки набора функций, в который ZTNA может входить как компонент.

Архитектурное сравнение: VPN против ZTNA (и роль SASE как модели доставки)

1. Различие «единицы доступа».

– VPN: пользователь получает доступ к сети/подсетям, а уже поверх этого ограничивается доступ к приложениям (ACL, сегментация, дополнительные шлюзы);

– ZTNA: доступ выдаётся непосредственно к приложению/сервису, согласно политикам (identity + context), без необходимости «вводить» пользователя в сеть.

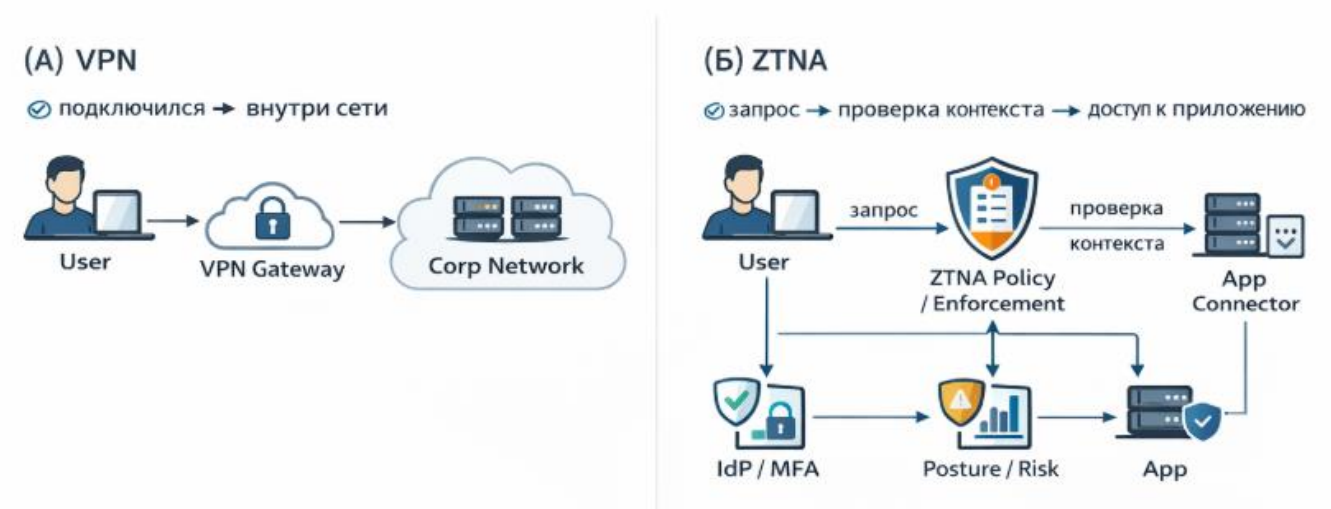

Рисунок 1 – Упрощённая логика доступа VPN vs ZTNA (ASCII-схема).

2. Поверхность атаки и латеральное перемещение.

В VPN-модели после успешной аутентификации и установления туннеля часто возникают риски:

– сканирования внутренних адресов;

– обращения к сервисам «по пути»;

– lateral movement при компрометации учётной записи/устройства.

ZTNA снижает эти риски, поскольку:

– обычно не раскрывает адресное пространство и не предоставляет L3-достижимость;

– изолирует доступ на уровне приложения;

– упрощает реализацию принципа «минимально необходимого».

3. Контекст и динамика доверия.

VPN чаще всего принимает решение «один раз» (при подключении). Дополнительные проверки возможны (например, re-authentication, NAC, EDR сигналы), но нередко они реализованы вне единого policy-контура либо не являются обязательными.

ZTNA строится вокруг контекстной и событийной переоценки доступа на основе:

– идентичности (IdP, роли);

– состояния устройства (MDM/UEM, EDR);

– контекста (география, репутация IP, время);

– риск-сигналов (аномалии, подозрительная активность, политики Conditional Access).

Результат – доступ становится условным: при изменении контекста политика может потребовать усиления (step-up MFA), ограничить доступ или завершить сессию.

4. Практические сценарии применения

Сценарий A (типичный офисный пользователь): доступ к Saas и 1-2 внутренним web-приложениям.

ZTNA (часто в рамках SASE) даёт лучший баланс безопасности и управляемости: точечный доступ, единый контур политик, хорошие возможности аудита.

Сценарий B (администратор/инженер): доступ к множеству систем, включая legacy протоколы/инфраструктурные компоненты.

На практике часто требуется комбинация: ZTNA для прикладных сервисов + bastion/jump host/PAW для привилегированного доступа. VPN может сохраниться как транспорт в отдельных случаях, но должен быть «обёрнут» политиками, сегментацией и усиленным контролем привилегий.

Таблица 1

Сравнение VPN и ZTNA/SASE.

Критерий	VPN	ZTNA/SASE
Единица доступа	Сеть/подсеть	Приложение/сервис
Модель доверия	Часто «внутри=доверено»	«Никому не доверять по умолчанию»
Контекст (device posture, риск)	Иногда/частично	Обычно встроено и обязательно
Латеральное перемещение	Выше	Ниже (доступ точечный)
Масштабирование	Узкие места на шлюзах	Эластичность (edge/PoP)

Видимость/аудит	Нередко сетевой уровень	Гранулярность до приложения/сессии
Типовые сложности	Сегментация, «слишком широкий» доступ	Интеграции (IdP/EDR), дизайн политик

Как TOGAF помогает «приземлить» Zero Trust (ADM-логика)

Технологический выбор (VPN/ZTNA/SASE) превращается в управляемую архитектуру, если:

– фиксируются драйверы и архитектурные принципы;

– формализуются требования (security + compliance + UX);

– описывается целевое состояние и границы применимости технологий;

– планируется миграция и контроль внедрения;

– обеспечивает контроль соответствия (governance) и измеримость результатов (KPI/KRI).

1. Привязка к фазам TOGAF ADM.

– Architecture Vision: цели (контекстный доступ, снижение поверхности атаки), KPI (доля приложений, переведённых на ZTNA; снижение числа инцидентов/нарушений политик);

– Business Architecture: роли и сценарии удалённого доступа (пользователь, подрядчик, администратор), требования к разделению обязанностей;

– Application Architecture: классификация приложений (web/клиент сервер/legacy), критичность, зависимости, готовность к SSO, требования к журналированию;

– Technology Architecture: выбор компонентов (IdP/SSO, MFA, posture проверки, ZTNA enforcement/коннекторы, logging/telemetry, интеграция с SIEM);

– Opportunities&Solutions/Migration Planning: этапность перехода (пилот → расширение → перевод критичных приложений → ограничение роли VPN до исключений);

– Implementation Governance: контроль соответствия реализаций требованиям и целевой архитектуре, включая проверяемые метрики и аудит.

2. Пример артефакта TOGAF: каталог требований безопасности.

Таблица 2

Пример Security Requirements Catalog.

ID	Требование	Приоритет	Метрика проверки
SR-01	MFA для удалённого доступа	Высокий	100% интерактивных входов с MFA
SR-02	Доступ к критичным приложениям только с управляемых устройств	Высокий	Доля доступов с compliant device
SR-03	Least privilege на уровне приложений	Высокий	Нет доступов «по подсети» без необходимости
SR-04	Полный аудит «кто/куда/почему»	Высокий	Логи содержат user, device, app, policy, result
SR-05	Реакция на риск (step-up/terminate)	Средний	Политика меняется при risk-score↑

3. Матрица трассируемости (требование → компоненты).

Таблица 3

Requirements Traceability Matrix.

Требование	IdP/SSO	MFA	Posture (MDM/EDR)	ZTNA Policy	Connector	SIEM
SR-01	✓	✓				✓
SR-02			✓	✓		✓
SR-03	✓		✓	✓	✓	✓
SR-04	✓	✓	✓	✓	✓	✓
SR-05	✓	✓	✓	✓		✓

VPN остаётся применимым в ограниченных условиях и может быть оправдан как транспорт для отдельных категорий доступа, особенно при наличии legacy систем. Однако при росте распределённости приложений и усилении требований к контексту, аудиту и управлению рисками модель «туннель в сеть» становится архитектурно слабой из-за предоставления сетевой достижимости и повышенных рисков латерального перемещения.

ZTNA лучше соответствует принципам Zero Trust: выдаёт доступ точечно к приложениям/сессиям, учитывает контекст и сигналы риска, повышает управляемость политик и глубину аудита. SASE, в свою очередь, задаёт облачно ориентированный способ доставки таких функций с масштабированием через edge/PoP.

TOGAF (ADM) обеспечивает дисциплину перехода: от драйверов и принципов – к формализованным требованиям, целевой архитектуре, плану миграции и архитектурному контролю реализации.

Список литературы:

1. Грищенко В. В., Кузнецов А. А. Управление доступом и идентификацией в информационных системах: учебное пособие. СПб.: Питер, 2020. 304 с.

2. Макаренко С. И. Информационная безопасность распределённых информационных систем: учебное пособие. / 2-е изд., перераб. и доп. / М.: Инфра-М, 2021. 384 с.

3. Лапонина И. В., Киселёв А. А. Сетевая безопасность корпоративных информационных систем: учебное пособие. М.: МГУ им. М. В. Ломоносова, 2021. 272 с.

4. Зегжда П. Д., Полянский А. А. Безопасность информационных систем: архитектура, анализ, управление. – М.: Горячая линия – Телеком, 2021. 448 с.

5. Барт Д., Гилман Э., Морильо К., Райс Р. Сети с нулевым доверием. Построение безопасных систем в ненадёжных сетях: практическое руководство / пер. с англ. СПб.: БХВ-Петербург, 2022. – 336 с.

6. The Open Group. TOGAF® Standard. 10-е изд.: руководство / пер. с англ. / М.: ДМК Пресс. 2023. 820 с.

7. National Institute of Standards and Technology (NIST). Zero Trust Architecture: SP 800-207. 2020.

8. Методические рекомендации по защите информации в распределённых информационных системах // ФСТЭК России – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g

9. TOGAF. ADM Overview // The Open Group – URL: https://www.opengroup.org/togaf

UDC 004.771

COMPARATIVE ANALYSIS OF REMOTE ACCESS MODELS: VPN VS ZTNA/SASE AND THE ROLE OF TOGAF IN ZERO TRUST DESIGN

Natalya V. Kartechina
candidate of agricultural sciences, associate professor
kartechnatali@mail.ru
Nikita Al. Ulybyshev
student
avtocad68@yandex.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. The growth of remote work, hybrid IT infrastructure (on-prem + IaaS + SaaS), and identity attacks reduces the effectiveness of the classic approach to remote access based on the «tunnel to network» (VPN) model as a universal mechanism for secure access to corporate resources. The article provides a comparative analysis of VPN and ZTNA (Zero Trust Network Access) based on the architectural "access unit," attack surface, and risks of lateral movement, context, and auditing capabilities. It is also shown how the TOGAF (ADM) methodology helps to formalize requirements, describe

the target architecture, and plan migration to Zero Trust, as well as ensure the manageability of implementation through traceability of requirements and architectural management.

Keywords: remote access, VPN, ZTNA, SASE, Zero Trust, TOGAF ADM, contextual access, segmentation, audit.

Статья поступила в редакцию 25.02.2026; одобрена после рецензирования 20.03.2026; принята к публикации 31.03.2026.

The article was submitted 25.02.2026; approved after reviewing 20.03.2026; accepted for publication 31.03.2026.