Аналитическая статья
УДК 004.056.5; DOI: 10.61260/2218-13X-2025-3-175-188

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДОВ СЕГМЕНТАЦИИ СЕТИ ДЛЯ ЗАЩИТЫ ОТ ПЕРЕМЕЩЕНИЯ ЗЛОУМЫШЛЕННИКА В ИЗОЛИРОВАННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

✉**Игнатов Данил Юрьевич.**
**МИРЭА – Российский технологический университет, Москва, Россия**
✉***ignatov.d.y@edu.mirea.ru***

*Аннотация.* Представлен сравнительный анализ методов сетевой сегментации для противодействия латеральному перемещению злоумышленников в изолированных средах. На основе анализа предложена концепция преодоления системных ограничений существующих подходов сетевой сегментации. Методология основана на критическом анализе эволюции защитных парадигм – от традиционных решений на основе virtual local area network и access control list до современных концепций микросегментации и архитектуры «нулевого доверия» – с применением аналитики цепочек атак на основе фреймворка MITRE ATT&CK для оценки эффективности против ключевых техник перемещения. В качестве решения функциональных противоречий разработана концепция адаптивной динамической сегментации, интегрирующая иерархию уровней защиты, декларативную онтологию политик и механизм превентивной оркестрации границ на основе аналитики угроз. Научная новизна заключается в синтезе принципов динамической контекстуализации политик, предиктивной адаптации сегментов и непрерывной верификации сетевой активности.

*Ключевые слова:* сетевая сегментация, горизонтальное перемещение, микросегментация, VLAN, SDN, Zero Trust, информационная безопасность, изолированные компьютерные сети

**Для цитирования:** Игнатов Д.Ю. Сравнительный анализ эффективности методов сегментации сети для защиты от перемещения злоумышленника в изолированных компьютерных сетях // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 3. С. 175–188. DOI: 10.61260/2218-13X-2025-3-175-188.

Analytical article

# COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF NETWORK SEGMENTATION METHODS TO PROTECT AGAINST THE MOVEMENT OF AN ATTACKER IN ISOLATED COMPUTER NETWORKS

✉**Ignatov Danil Yu.**
**MIREA – Russian technological university, Moscow, Russia**
✉***ignatov.d.y@edu.mirea.ru***

*Abstract.* The article presents a comparative analysis of network segmentation methods to counteract the lateral movement of intruders in isolated environments. Based on the analysis, the concept of overcoming the systemic limitations of existing network segmentation approaches is proposed. The methodology is based on a critical analysis of the evolution of security paradigms – from traditional virtual local area network and access control list solutions to modern concepts of microsegmentation and zero-trust architecture – using attack chain analytics based on the MITRE ATT&CK framework to evaluate effectiveness against key relocation techniques. As a solution to functional contradictions, the concept of adaptive dynamic segmentation has been developed, integrating a hierarchy of protection levels, a declarative policy ontology, and a mechanism for preventive border orchestration based on threat analytics.

The scientific novelty lies in the synthesis of principles of dynamic contextualization of policies, predictive adaptation of segments and continuous verification of network activity.

*Keywords*: network segmentation, horizontal movement, microsegmentation, VLAN, SDN, Zero Trust, information security, isolated computer networks

**For citation**: Ignatov D.Yu. Comparative analysis of the effectiveness of network segmentation methods to protect against the movement of an attacker in isolated computer networks // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 3. P. 175–188. DOI: 10.61260/2218-13X-2025-3-175-188.

## Введение

Актуальность исследования обусловлена экспоненциальным ростом сложности кибератак, где традиционная периметровая защита неспособна предотвратить горизонтальное перемещение злоумышленника внутри сети после первоначальной компрометации. Как отмечают представители Positive Technologies, недостаточная сегментация сети является одной из основных причин успешности кибератак на инфраструктуру организаций. Реалии 2023–2024 гг. демонстрируют, что отсутствие сегментации сети позволяет атакующим с любой точки инфраструктуры получить информацию обо всех остальных ее узлах и оперативно определить приоритетные цели [1]. Большинство успешных атак включают этап горизонтального продвижения к критическим активам, что приводит к масштабным утечкам данных и финансовым потерям. В условиях цифровой трансформации государственных систем и промышленных сетей проблема изоляции рисков становится критической для национальной безопасности.

Состояние проблемы в научной литературе характеризуется противоречиями:

1. Эффективность vs Управляемость. Традиционные методы (Virtual Local Area Network (VLAN), Access Control List (ACL) снижают поверхность атаки, но их эксплуатация в динамических средах приводит к экспоненциальному росту сложности из-за ручного управления правилами на основе IP-адресов.

2. Гранулярность изоляции. Требования Федеральной службы Российской Федерации по техническому и экспортному контролю (ФСТЭК России) (приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер, ISO/IEC 27001, Payment Card Industry Data Security Standard, PCI DSS, предписывают обязательную сегментацию для изоляции критических сегментов (demilitarized zone, DMZ), управляющие системы). Однако физическая сегментация, обеспечивая максимальную безопасность, экономически нецелесообразна для распределенных сетей, а логические методы (например, virtual routing and forwarding, VRF) не всегда препятствуют продвижению атакующих через уязвимости уровня L2 модели OSI.

3. Парадигмы безопасности. Концепция «нулевого доверия» (Zero Trust, ZT) декларирует необходимость верификации каждого запроса, но ее реализация через микросегментацию требует глубокой интеграции с системами аутентификации, что сложно в гетерогенных средах. Альтернативная модель «максимального недоверия», сочетающая сегментацию по отделам, шифрование трафика и контроль привилегий, демонстрирует преимущества в защите от внутренних угроз, но увеличивает операционные расходы.

Цель исследования – сравнительный анализ методов сегментации сетей для выявления оптимальных решений, минимизирующих риски перемещения злоумышленников в изолированных компьютерных сетях.

## Методология исследования и классификация методов сетевой сегментации

Настоящее исследование базируется на системном подходе к анализу эффективности методов сетевой сегментации в контексте противодействия горизонтальному перемещению (Lateral Movement, LM) злоумышленников. Для достижения поставленной цели был применен комплекс методов, включающий:

1. Систематизацию и классификацию.

Выявление и группировка существующих методов сегментации на основе фундаментальных архитектурных принципов (физическая изоляция, логическое разделение на основе IP/портов, идентификация на уровне приложений/рабочих нагрузок, политико-ориентированное управление), механизмов реализации (аппаратные, программные, гибридные) и уровня гранулярности (макро-, микросегментация).

2. Анализ тактик, техник и процедур (TTPs) злоумышленников.

Сопоставление возможностей каждого метода сегментации с техниками продвижения атаки, документированными в рамках фреймворка MITRE ATT&CK. Это позволило оценить, на каком этапе цепочки атаки (kill chain) метод оказывает сдерживающее воздействие.

3. Формирование системы оценочных критериев.

Определение ключевых метрик эффективности, релевантных целям исследования:

– снижение поверхности атаки, то есть способность метода минимизировать количество доступных путей коммуникации между несвязанными сегментами/рабочими нагрузками. Измеряется как процентное уменьшение видимых узлов и сервисов из скомпрометированной зоны;

– эффективность сдерживания LM, то есть способность предотвращать или существенно затруднять выполнение конкретных техник LM (например, блокировка неавторизованного Remote Desktop Protocol (RDP)/Server Message Block (SMB), предотвращение сканирования подсетей);

– сложность управления и эксплуатации, то есть требования к ресурсам для развертывания, конфигурирования, мониторинга и поддержки решения (включая обучение персонала). Оценивается по шкале от низкой (например, базовые ACL) до высокой (например, детальная микросегментация с динамическими политиками);

– адаптивность, то есть способность решения динамически адаптироваться к изменениям в сети, а также к изменению ландшафта угроз;

– воздействие на производительность сети, то есть влияние на задержку, пропускную способность и время обработки пакетов (например, из-за глубокой инспекции или дополнительных проверок);

– устойчивость к обходу, то есть уязвимость метода к известным техникам обхода сегментации (например, использование разрешенных портов для туннелирования, злоупотребление доверенными хостами).

## Классификация методов сетевой сегментации

На основе анализа научной литературы, современных исследований и отраслевых практик можно выделить следующие основные методы сетевой сегментации, релевантные защите изолированных сетей от LM:

1. Традиционные методы:

– Физическая сегментация.

Полное физическое разделение сетей с использованием отдельных кабельных систем, коммутаторов и маршрутизаторов. Обеспечивает наивысший уровень изоляции, исключая возможность несанкционированного доступа на канальном уровне. Крайне эффективен для

защиты критических сегментов, но обладает катастрофически низкой масштабируемостью и гибкостью, высокой стоимостью и сложностью управления изменениями. Практически не адаптивен.

– Виртуальные локальные сети (VLAN).

Логическое разделение широковещательных доменов в рамках одной физической инфраструктуры на канальном уровне модели OSI. Также позволяет группировать хосты по функциональному признаку независимо от их физического расположения. VLAN является базовым механизмом изоляции, однако уязвим к атакам VLAN Hopping (Double Tagging, Switch Spoofing) и не обеспечивает защиту на сетевом уровне (L3). Управление статично, масштабирование ограничено лимитами коммутаторов (стандарт IEEE 802.1Q поддерживает до 4094 VLAN).

– Списки контроля доступа (ACL).

Фильтрация трафика на маршрутизаторах и коммутаторах L3 на основе IP-адресов источника/назначения, портов и протоколов (L3–L4). Основной инструмент контроля межсегментного трафика в традиционных сетях.

Главными недостатками являются статичность правил, экспоненциальный рост сложности управления с увеличением сети, зависимость от IP-адресации (проблема мобильности хостов и дефицита IPv4), сложность аудита и высокая вероятность ошибок конфигурации. Эффективность против современных угроз (адаптивные атаки, шифрованный трафик) ограничена.

2. Сегментация на основе программно-определяемых сетей (software-defined networking, SDN).

Использует принципы централизованного управления плоскостью управления (контроллер SDN) и отделения ее от плоскости данных (свитчи/маршрутизаторы). Позволяет определять потоки трафика и политики безопасности независимо от физической топологии. Примеры: OpenFlow, Cisco ACI, VMware NSX.

Ключевыми преимуществами является гибкость, централизованное управление политиками, автоматизация (оркестрация через application programming interface, API), возможность реализации более детализированных правил на основе контекста (пользователь, приложение), чем ACL [2]. При этом данный метод реализуем при построении сети с нуля или существенной модернизации инфраструктуры [3].

Стоит отметить, что применение данного метода создает определенные риски, выражающиеся в том, что контроллер SDN становится критической точкой отказа и потенциальной целью атаки [4, 5]. Эффективность сильно зависит от конкретной реализации и интеграции с другими системами безопасности.

3. Микросегментация.

Принципиально новый подход, переносящий границы сегментации с уровня сети на уровень отдельных рабочих нагрузок (виртуальные машины, контейнеры, физические серверы) или даже отдельных приложений/сервисов. Каждая рабочая нагрузка получает собственную «зону безопасности» с уникальными политиками.

При реализации данного метода обычно используются гипервизорные или хостовые агенты (Host-Based Firewalls, HBF), либо возможности коммуникации в среде виртуализации/контейнеризации (например, группы безопасности в VMware NSX, Calico Network Policy для Kubernetes, AWS Security Groups). Политики обычно определяются на основе идентификаторов рабочих нагрузок (теги, метаданные) или атрибутов приложений, а не IP-адресов.

Основным преимуществом данного метода является снижение поверхности атаки внутри сегмента сети. Даже при компрометации одной рабочей нагрузки, злоумышленник изолирован от других, если нет явного разрешения на коммуникацию между ними. Эффективно блокирует большую часть техник LM.

Однако при реализации данного метода существует риск резкого увеличения числа политик, сложности определения и поддержания актуальности правил для большого

количества динамически изменяющихся объектов, а также необходимы высокие требования к производительности систем управления политиками. Реализация данного подхода требует зрелых процессов управления конфигурацией и идентификацией активов.

4. Сегментация в рамках архитектуры «нулевого доверия» (ZT).

Данный подход не является отдельным технологическим методом, а представляет собой архитектурный принцип и набор практик, которые могут реализовываться с использованием различных технологий (включая микросегментацию, SDN). Основывается на постулате «никогда не доверяй, всегда проверяй» (Never trust, Always verify). Ключевые принципы данного подхода изложены в стандарте NIST SP 800-207 и включают в себя явную проверку всех запросов доступа, применение принципа минимальных привилегий, предположение о компрометации сети [6].

Реализация подхода на базе ZT требует строгой сегментации как механизма принуждения к постоянной проверке доступа между сегментами (макроуровень) и/или рабочими нагрузками (микроуровень) [7]. Доступ предоставляется на основе динамической оценки доверия, учитывающей идентичность пользователя/устройства, состояние устройства, контекст запроса, чувствительность ресурса и аномалии поведения.

Преимуществом данного подхода является максимальное снижение поверхности атаки за счет гранулярного контроля и постоянной верификации, адаптивность к динамичным средам и угрозам, а также соответствие современным концепциям безопасности гибридных сред [8].

При этом реализация данного подхода сопровождается высокой сложностью проектирования и внедрения, необходимостью интеграции множества систем (IAM, SIEM, EDR), зависимостью от точности контекстных данных, а также потенциальным влиянием на пользовательский опыт.

Таблица 1

**Сравнительный анализ категорий методов сегментации по ключевым критериям**

| Критерий оценки | Традиционные (VLAN/ACL) | SDN | Микросегментация | Zero Trust |
|---|---|---|---|---|
| Гранулярность | Сеть/подсеть (L3–L4) | Поток/группа (L2–L7) | Рабочая нагрузка/сервис | Ресурс/транзакция (L7) |
| Снижение поверхности атаки | Низкое | Среднее | Высокое | Высокое |
| Управляемость | Низкая (при масштабе) | Средняя – высокая | Низкая | Средняя – высокая (с автоматизацией) |
| Адаптивность | Низкая | Высокая | Средняя | Высокая |
| Производительность | Минимальное влияние | Среднее влияние | Среднее – высокое влияние | Зависит от реализации (может быть высоким) |
| Устойчивость к обходу | Низкая | Средняя | Высокая | Высокая |

Представленная классификация и система критериев создают основу для детального сравнительного анализа конкретных реализаций методов в следующем разделе, где будет проведена оценка их способности блокировать конкретные техники MITRE ATT&CK, эффективности в условиях ограничений (IPv4, IoT) и сбалансированности требований безопасности и операционной эффективности. Особое внимание будет уделено выявленным во введении противоречиям.

**Сравнительный анализ эффективности методов сегментации против техник горизонтального перемещения**

Основной целью сегментации в контексте противодействия горизонтальному перемещению является разрыв цепочки атаки злоумышленника путем изоляции скомпрометированных сегментов и блокировки путей перемещения. Для объективной оценки эффективности различных методов применим сформированную систему критериев к конкретным техникам LM, выделенным в матрице MITRE ATT&CK, наиболее релевантным для изолированных сетей [9]:

– T1021 – Remote Services (RDP, SMB, SSH);
– T1570 – Lateral Tool Transfer;
– T1018 – Remote System Discovery.

Анализ базируется на синтезе практики, а также данных, полученных в ходе моделирования техник в тестовой среде.

*Эффективность методов сегментации против ключевых техник горизонтального перемещения MITRE ATT&CK*

1. T1021 – Remote Services (использование удаленных сервисов).

1) Традиционные методы сегментации (VLAN/ACL) эффективны на базовом уровне, блокируя доступ к сервисам (порты 3389/RDP, 445/SMB, 22/SSH) между сегментами на L3/L4. Однако уязвимы к:

– обходу через разрешенные порты (например, туннелирование RDP через HTTP/HTTPS на порт 80/443, если они разрешены для веб-доступа);

– компрометации узла внутри сегмента, имеющего доступ к целевым сервисам других узлов внутри того же широковещательного домена или подсети (особенно критично в плоских сетях);

– сложности управления при частых изменениях легитимных источников доступа.

2) Метод на основе SDN повышает эффективность за счет централизованного управления и возможности привязки правил не только к IP-портам, но и к контексту (например, группам пользователей или времени). Может динамически блокировать подозрительные RDP-сессии на основе данных IDS/IPS, интегрированных с контроллером. Однако эффективность зависит от детализации политик и качества интеграции с системами мониторинга.

3) Микросегментация обеспечивает максимальную защиту, так как политики «default-deny» на уровне ВМ/контейнера/сервиса запрещают любые соединения, кроме явно разрешенных между конкретными парами «источник-назначение-сервис». Даже если злоумышленник получил доступ к одной ВМ, он не сможет подключиться по RDP/SMB/SSH к соседним, если это не предусмотрено политикой. Высокая устойчивость к обходу.

4) Zero Trust наиболее эффективен, так как заменяет прямой сетевой доступ к сервисам на проксирование через доверенный шлюз (Policy Enforcement Point (PEP). Доступ к RDP/SMB/SSH предоставляется только после строгой аутентификации и авторизации (с учетом контекста) конкретного пользователя/устройства к конкретному приложению/серверу, а не к сети. Полностью исключает сканирование и прямой доступ к портам сервисов из неавторизованных мест.

2. T1570 – Lateral Tool Transfer (Передача инструментов для горизонтального перемещения).

1) Традиционные методы слабо эффективны. ACL, разрешающие общий доступ к файловым ресурсам (SMB, NFS) или использование легитимных каналов (HTTP, FTP) внутри сегмента, позволяют беспрепятственно передавать инструменты. Фильтрация по типам файлов (если используется) легко обходится.

2) Метод на основе SDN может повысить защиту за счет интеграции с DLP-системами или песочницами, анализирующими передаваемый контент на границах сегментов. Однако сложность и производительность ограничивают применение в реальном времени.

3) Микросегментация эффективна, так как явно запрещает несанкционированные соединения между рабочими нагрузками, используемые для передачи файлов. Разрешенные каналы (например, доступ к конкретному файловому серверу) можно дополнительно контролировать. Существенно затрудняет передачу инструментов между скомпрометированными хостами.

4) Zero Trust дополняет микросегментацию строгим контролем контента и контекста передачи. PEP может инспектировать трафик (даже зашифрованный, если используется TLS-инспекция с доверенными сертификатами), блокировать известные вредоносные исполняемые файлы или подозрительные действия. Требует интеграции с системами анализа угроз.

3. T1018 – Remote System Discovery (обнаружение удаленных систем).

1) Традиционные методы сегментации обладают ограниченной эффективностью. VLAN изолируют широковещательный трафик (ARP), препятствуя обнаружению хостов в других VLAN на уровне L2. ACL на маршрутизаторах могут блокировать протоколы сканирования (ICMP, TCP SYN) между сегментами. Однако внутри одного сегмента сети сканирование остается тривиальным. Статические ARP-таблицы или Port security на коммутаторах уровня L2 могут частично помочь, но сложны в управлении.

2) Метод на основе SDN может эффективно подавлять сканирование, так как контроллер имеет глобальное представление о топологии и может детектировать аномально высокую активность сканирования (например, множество запросов ARP, TCP или SYN от одного источника за короткое время) и блокировать ее на уровне потоков.

3) Микросегментация крайне эффективна, поскольку политики «default-deny» блокируют все несанкционированные соединения, попытки сканирования портов соседних хостов (например, с помощью инструмента nmap) будут блокироваться межсетевым экраном хоста или гипервизора. Злоумышленник видит только те хосты и порты, к которым он получил доступ. Резко снижает видимость сети для атакующего.

4) Для Zero Trust принцип «минимальной видимости» является базовым. Сервисы и ресурсы не объявляют себя в сети и не отвечают на запросы от неавторизованных сущностей. Обнаружение систем возможно только через авторизованные и контролируемые каналы доступа, что делает пассивное и активное сканирование неэффективным.

*Анализ ключевых противоречий и ограничений*

1. Детализация сегментации vs Дефицит IPv4.

Проблема: традиционные методы (особенно ACL) и, в меньшей степени, SDN полагаются на IP-адресацию для определения политик. Детальная сегментация (требующая множества мелких подсетей) усугубляет дефицит IPv4, вынуждая к сложным схемам network address translation, NAT, или переходу на IPv6, что не всегда возможно в унаследованных сетях.

Анализ: микросегментация и ZT, опирающиеся на идентификаторы рабочей нагрузки/приложения/пользователя (теги, метаданные, сертификаты), а не на IP-адреса, частично снимают это противоречие. Они позволяют достичь высокой гранулярности без дробления адресного пространства. Однако для управления политиками ZT/микросегментации IP-адреса необходимы для своей работы и коммуникации.

Предложение: внедрение гибридных моделей. Для повышения эффективности сегментирования сети в контексте защиты от горизонтального перемещения злоумышленника рекомендуется:

– использовать микросегментацию на уровне критических активов (серверы, базы данных (БД), контроллеры внутри более крупных подсетей, управляемых традиционными методами или SDN;

– активно применять идентификаторы на основе тегов/метаданных в SDN и системах микросегментации, минимизируя зависимость от IP для политик;

– поэтапное внедрение IPv6 в новых сегментах или на границах.

2. Безопасность vs Производительность.

Проблема: детализированные проверки (глубокая инспекция пакетов – Deep Packet Inspection (DPI) в Zero Trust Network Access (ZTNA)/PEP, анализ контента в микросегментации, обработка сложных динамических политик в SDN) вносят дополнительную задержку. В сетях реального времени (промышленный IoT, финансовые транзакции) это неприемлемо.

Анализ: традиционные методы (VLAN, базовые ACL) имеют минимальное влияние. SDN и микросегментация дают умеренное увеличение задержек. ZT с TLS-инспекцией и контекстным анализом оказывает наибольшее влияние.

Предложения:

– дифференциация политик: применять наиболее строгие и ресурсоемкие проверки (DPI, анализ угроз) только к трафику, направленному к высококритичным активам или исходящему из зон повышенного риска. Для менее критичных потоков использовать более легковесные проверки (L3/L4 ACL, базовые сигнатуры);

– аппаратное ускорение: использование специализированных платформ (SmartNICs, DPU – Data Processing Units) для выгрузки функций безопасности (шифрование, DPI, фильтрация) с центрального процессора основных серверов и сетевых устройств;

– оптимизация политик: регулярный аудит и очистка политик от устаревших и избыточных правил для снижения вычислительной нагрузки.

3. Управляемость vs. Гранулярность и адаптивность.

Проблема: достижение высокой гранулярности (микросегментация) и адаптивности (SDN, ZT) неизбежно ведет к экспоненциальному росту числа политик и сложности их согласованного управления. Риск ошибок конфигурации, создающих уязвимости в безопасности или блокирующих легитимный трафик, возрастает. Поддержание актуальности политик при динамичных изменениях (DevOps, оркестрация контейнеров) становится ключевой проблемой.

Анализ: традиционные методы плохо масштабируются, но относительно просты в небольших сетях. SDN централизует управление, но сложен в настройке. Микросегментация и ZT требуют зрелых процессов и инструментов оркестрации.

Предложения:

– автоматизация на основе Infrastructure as Code (IaC): управление политиками безопасности как кодом с использованием инструментов (Terraform, Ansible, специфические API VMware NSX, Cisco ACI, Zscaler ZPA) для обеспечения согласованности, версионности и автоматического развертывания;

– интеграция с CI/CD: встраивание проверок политик безопасности в конвейеры разработки и поставки приложений (DevSecOps). Политики определяются разработчиками/архитекторами вместе с приложением;

– машинное обучение для управления политиками: использование ML-алгоритмов для автоматического предложения политик на основе наблюдаемых шаблонов легитимного трафика, выявления аномалий в существующих политиках, оптимизации набора правил для производительности.

Данный анализ демонстрирует, что выбор метода сегментации является стратегическим решением, требующим тщательного учета специфики изолированной сети, ресурсных ограничений и приемлемого уровня операционных рисков.

**Предложения по адаптивной сегментации**

На основании выявленных противоречий и ограничений существующих методов сегментации предлагается концепция адаптивной динамической сегментации (АДС). Концепция АДС интегрирует преимущества микросегментации, принципов «нулевого доверия» и программно-определяемых сетей, дополняя их тремя инновационными компонентами:

1. Контекстно-зависимые политики безопасности, формируемые на основе:

– реального сетевого поведения;

– уровня критичности ресурсов;

– динамической оценки риска (интеграция с SIEM, EDR, системами управления уязвимостями);

– телеметрии состояния устройств (патчи, конфигурации, признаки компрометации).

2. Многоуровневая архитектура исполнения, реализующая принцип «разделения обязанностей»:

– уровень 1 – периметр сегмента с использованием SDN-контроллеров для макрополитик (изоляция групп VLAN/VXLAN);

– уровень 2 – граница рабочей нагрузки с использованием гипервизорных/контейнерных межсетевых экранов для микросегментации;

– уровень 3 – граница уровня приложений с использованием ZTNA-шлюзов для верификации трафика на уровне L7;

– уровень 4 – граница уровня данных с использвоанием криптографической сегментации (MACsec, IPsec).

3. Система оркестрации на базе машинного обучения, обеспечивающая:

– автоматическое обнаружение дрейфа политик;

– прогнозирование возможности реализации техник злоумышленника;

– оптимизацию правил межсетевого экрана через обучение с подкреплением;

– адаптацию к изменениям топологии в реальном времени.

Таблица 2

**Аналитическая модель функционирования адаптивной динамической сегментации**

| Уровень | Что проверяет? | Технологии | Цель | Главное преимущество |
|---|---|---|---|---|
| Уровень 1. Сети | – Источник трафика (IP-адрес, подсеть)<br>– Куда он направлен?<br>– На какой порт?<br>– По какому протоколу (TCP/UDP)? | – Традиционные ACL на маршрутизаторах/ коммутаторах<br>– Программно-определяемые сети (SDN)<br>– Межсетевые экраны | – Блокировка грубых атак между крупными сегментами (например, между отделами)<br>– Базовая изоляция сегментов (VLAN) | Скорость: быстрая обработка больших потоков трафика |
| Уровень 2. Рабочей нагрузки | – КТО общается (не IP, а ИДЕНТИФИКАТОР сервера/контейнера /ВМ)?<br>– С КЕМ он хочет связаться?<br>– ДЛЯ ЧЕГО (конкретный сервис/порт)? | – Микросегмен-тация (VMware NSX Groups, AWS Security Groups, Kubernetes Network Policies)<br>– Хостовые МСЭ | – Защита внутри зоны (например, между веб-сервером и БД)<br>– Блокировка перемещения после взлома одной машины | Точность: блокирует ненужные связи даже внутри одной подсети. «Default-Deny» для всего |

| Уровень | Что проверяет? | Технологии | Цель | Главное преимущество |
|---|---|---|---|---|
| Уровень 3. Пользователя/Приложения | – КТО пользователь/ устройство?<br>– ИХ СТАТУС (обновления? вирусы? риск?)<br>– КУДА и ЗАЧЕМ они идут? (Конкретное приложение, а не сервер!)<br>– КОГДА и ОТКУДА? | – Zero Trust Network Access<br>– Identity-Aware Proxies<br>– Системы контроля доступа (IAM) | – Доступ пользователей/ устройств к внутренним приложениям (например, CRM, базам)<br>– Защита от кражи учетных данных и нелегитимного доступа | Контекст: проверяет не только «что», но и «кто», «как» и «почему» |
| Уровень 4. Данных | Целостность и конфиденциальность данных при передаче или хранении | – Шифрование канала (TLS 1.3, IPsec VPN, MACsec)<br>– Шифрование данных (Database Encryption, FileVault/BitLocker)<br>– Системы DLP (Data Loss Prevention) | – Защита критичных данных | Защита данных: даже если злоумышленник прошел все уровни, данные останутся нечитаемыми |

*Пример работы АДС при реализации атаки*

Сценарий: злоумышленник украл пароль сотрудника (userA) и пытается получить доступ к базе данных (DB-Prod) с использованием скомпрометированного устройства (Device-X).

Уровень 1 (сеть):

Трафик с Device-X (IP 10.0.1.15) направлен в подсеть 10.0.50.0/24, где размещен DB-Prod.

Проверка: разрешено ли хосту 10.0.1.15 обращаться к подсети 10.0.50.0/24? Допустим, правило ACL разрешает подсети (10.0.1.0/24) доступ к серверной (10.0.50.0/24). Трафик пропущен.

Уровень 2 (рабочая нагрузка):

Device-X пытается подключиться напрямую к DB-Prod на порт 3306 (MySQL).

Проверка: есть ли правило микросегментации, разрешающее Device-X (идентификатор tag:device=employee-laptop) соединяться с DB-Prod (идентификатор tag:app=db-prod) на порту 3306? Нет! Правила разрешают доступ только конкретным веб-серверам (tag:app=frontend). Трафик будет заблокирован.

Результат: несанкционированное перемещение в сети будет остановлено на этом уровне. Злоумышленник не смог добраться до БД напрямую.

В случае, если Уровень 2 был сконфигурирован неверно (и пропустил трафик), сработал бы Уровень 3: userA с Device-X пытается получить доступ через приложение (например, веб-интерфейс администрирования БД на app-db-admin.example.com).

Проверка Уровня 3 (ZTNA):

Аутентификация userA + MFA: УСПЕХ.

Состояние Device-X: антивирус выключен, критичные обновления не установлены. Риск высокий (например, 0,8).

Политика: доступ к app-db-admin разрешен только при риске сессии < 0,3. В доступе будет отказано.

Трафик заблокирован. Атакующий не смог использовать украденный пароль.

Уровень 4 (Данные): если бы атакующий все-таки смог получить доступ к БД (например, через эксплойт на веб-сервере, который имеет доступ к БД по правилу Уровня 2), данные были бы зашифрованы (TLS, шифрование БД на диске). Украденные данные бесполезны.

*Решения функциональных проблем и противоречий при использовании АДС:*

1. Проблема: Зависимость от IP-адресации.

Решение АДС: уровни 2 и 3 не зависят от IP. Они используют идентификаторы (теги, имена сервисов, сертификаты устройств). IP важен только на Уровне 1 для базовой маршрутизации. Можно иметь крупные подсети (экономия IPv4), но при этом детально контролировать доступ внутри них через Уровень 2.

2. Проблема: Безопасность vs Производительность.

Решение АДС:

– Уровень 1: быстрые, простые проверки (IP/порт) – обрабатывают основной поток трафика;

– Уровень 2: более детальные проверки (идентификаторы), но только для критичных сервисов (БД, контроллеры);

– Уровень 3: ресурсоемкие проверки (аутентификация, контекстный риск) только для доступа пользователей к приложениям.

Итог: сложные проверки выполняются точечно, где они необходимы, не оказывая влияния на производительность.

3. Проблема: сложность управления политиками.

Решение АДС:

– центр управления: одна система (например, на базе SDN-контроллера + ZTNA-консоли + IaC) генерирует правила для всех уровней на основе декларативных политик («Разрешено: Веб-серверы -> БД по порту 3306»; «Запрещено: Пользователи с высоким риском -> Критичные приложения»);

– автоматизация: при изменении сети (добавился сервер) Центр управления автоматически обновит правила на Уровне 2 (микросегментация) и Уровне 1 (ACL/SDN), не требуя ручной правки.

4. Проблема: неадаптивность к угрозам.

Решение АДС: интеграция Центра управления с системами аналитики (SIEM, EDR, Threat Intel). Пример:

– появилась новая угроза (эксплойт для MySQL – CVE-2025-XXXXX);

– SIEM/TI подает сигнал в Центр управления АДС;

– центр управления автоматически и временно на Уровне 2 блокирует все соединения с БД на порту 3306, кроме абсолютно необходимых, а на Уровне 3 повышает порог риска для доступа к интерфейсам администратора БД (например, требует привести состояние устройства к необходимым требованиям).

– после установки необходимых обновлений политики автоматически возвращаются в норму.

Предложенная концепция АДС (4 уровня + централизованное управление) обеспечивает глубокую защиту от перемещения злоумышленника внутри сети, а также решает основные противоречия и может внедряться поэтапно.

## Заключение

Проведенный анализ методов сегментации сетей для противодействия перемещению злоумышленников в изолированных средах позволил выявить фундаментальную трансформацию подходов к обеспечению информационной безопасности. Классические методы, основанные на физическом разделении и логической сегментации уровня сети, демонстрируют нарастающую неэффективность в условиях современных угроз,

характеризуемых высокой адаптивностью и использованием сложных цепочек. Их ограниченность проистекает из статичности, зависимости от IP-адресации и неспособности обеспечить необходимую гранулярность контроля в динамичных гибридных средах, что создает значительные возможности для злоумышленника после получения первоначального доступа.

Напротив, эволюция методов сегментации движется в сторону повышения детализации контроля и контекстной осведомленности. Программно-определяемые сети обеспечивают гибкость централизованного управления потоками, но истинный прорыв в противодействии перемещению злоумышленника в сети связан с появлением микросегментации и архитектурных принципов «нулевого доверия» (ZT). Микросегментация, перенося границы безопасности на уровень отдельных рабочих нагрузок и реализуя политику «запрещено по умолчанию», радикально сокращает поверхность атаки внутри сети. Архитектура «нулевого доверия», формализованная в NIST SP 800-207, дополняет этот подход непрерывной верификацией доступа на основе идентификации сущностей (пользователей, устройств, приложений), динамической оценки риска и контекста взаимодействия, исключая слепое доверие внутри сети. Синергия этих подходов позволяет блокировать ключевые техники злоумышленника, направленные на перемещение внутри сети.

Предложенная идея АДС представляет собой концептуальный ответ на выявленные системные противоречия: между необходимостью детальной сегментации и ограничением адресации, между требованиями безопасности и сохранением производительности сети, между сложностью управления гранулярными политиками и потребностью в операционной гибкости. АДС реализуется как многоуровневая система эшелонированной защиты, где каждый уровень выполняет специфическую функцию. Ключевым элементом АДС является централизованная система оркестрации, основанная на декларативных политиках безопасности и обогащенная аналитикой машинного обучения. Эта система автоматически транслирует высокоуровневые политики в конфигурации для различных технологических платформ на всех уровнях, обеспечивает непрерывный мониторинг соответствия, проактивно адаптирует правила на основе данных об угрозах от SIEM/EDR-систем и оптимизирует производительность, распределяя ресурсоемкие проверки целевым образом.

Перспективы дальнейших исследований видятся в нескольких ключевых направлениях:

– совершенствование алгоритмов искусственного интеллекта и машинного обучения в системах оркестрации для прогнозирования атак и автономной адаптации политик;

– исследование архитектур адресно-независимых сетей для окончательного преодоления ограничений IPv4 и повышения устойчивости к обходу сегментации.

Стратегическим выводом работы является утверждение, что эффективная защита от перемещения злоумышленника в изолированных сетях достижима только через принятие адаптивной, гранулярной и контекстно-зависимой модели сегментации, воплощенной в концепции АДС. Сетевая безопасность перестала быть вопросом статичного разграничения периметров, она стала непрерывным процессом динамической изоляции, где каждый акт коммуникации есть результат явной верификации намерения в рамках многоуровневой системы доверия. Предложенная модель обеспечивает не только высокий уровень защищенности, но и необходимую операционную устойчивость в условиях постоянно эволюционирующего ландшафта угроз.

**Список источников**

1. Итоги проектов по расследованию инцидентов и ретроспективному анализу – 2023–2024 // Официальный сайт Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/itogi-proektov-po-rassledovaniyu-inczidentov-i-retrospektivnomu-analizu-2023-2024/#id1 (дата обращения: 06.11.2024).

2. Нурудинов Г.М. Адаптивное управление трафиком в SDN-сетях с применением машинного обучения // Экономика и качество систем связи. 2024. № 1 (31). С. 114–122. EDN SXEGZB.

3. Ной А.И., Лиманова Н.И., Козлов В.В. Применение SDN и NFV в современных сетях, преимущества и недостатки // Бюллетень науки и практики. 2024. Т. 10. № 7. С. 387–391. DOI: 10.33619/2414-2948/104/41. EDN DBTRPD.

4. Ван С. Методы снижения возникновения рисков информационной безопасности в сетях SDN // Современная наука: актуальные проблемы теории и практики. Сер.: Естественные и технические науки. 2024. № 1. С. 42–45. DOI: 10.37882/2223-2966.2024.01.11. EDN UNCXOV.

5. Оценка и регулирование рисков нарушения доступности информации при реализации атак на сети Интернета вещей, построенные на базе технологии SDN / С.А. Ермаков [и др.] // Информация и безопасность. 2023. Т. 26. № 1. С. 31–38. DOI: 10.36622/VSTU.2023.26.1.004. EDN TXOKSA.

6. NIST. (2020). Special Publication 800-207, Zero Trust Architecture. National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.SP.800-207 (дата обращения: 08.07.2025).

7. Иванов П.А., Капгер И.В., Шабуров А.С. Модель реализации управления доступом к информационным активам в концепции нулевого доверия // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2023. № 45. С. 147–163. DOI: 10.15593/2224-9397/2023.1.07. EDN ZHSITI.

8. Нгуен Ф.Х., Нгуен Т.А., Зарипова Р.С. Zero Trust как инструмент защиты информационных активов компаний // Научно-технический вестник Поволжья. 2023. № 12. С. 656–658. EDN CECSSU.

9. Enterprise Matrix MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 08.07.2025).

**References**

1. Itogi proektov po rassledovaniyu incidentov i retrospektivnomu analizu – 2023–2024 // Oficial'nyj sajt Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/itogi-proektov-po-rassledovaniyu-inczidentov-i-retrospektivnomu-analizu-2023-2024/#id1 (data obrashcheniya: 06.11.2024).

2. Nurudinov G.M. Adaptivnoe upravlenie trafikom v SDN-setyah s primeneniem mashinnogo obucheniya // Ekonomika i kachestvo sistem svyazi. 2024. № 1 (31). S. 114–122. EDN SXEGZB.

3. Noj A.I., Limanova N.I., Kozlov V.V. Primenenie SDN i NFV v sovremennyh setyah, preimushchestva i nedostatki // Byulleten' nauki i praktiki. 2024. T. 10. № 7. S. 387–391. DOI: 10.33619/2414-2948/104/41. EDN DBTRPD.

4. Van S. Metody snizheniya vozniknoveniya riskov informacionnoj bezopasnosti v setyah SDN // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Ser.: Estestvennye i tekhnicheskie nauki. 2024. № 1. S. 42–45. DOI: 10.37882/2223-2966.2024.01.11. EDN UNCXOV.

5. Ocenka i regulirovanie riskov narusheniya dostupnosti informacii pri realizacii atak na seti Interneta veshchej, postroennye na baze tekhnologii SDN / S.A. Ermakov [i dr.] // Informaciya i bezopasnost'. 2023. T. 26. № 1. S. 31–38. DOI: 10.36622/VSTU.2023.26.1.004. EDN TXOKSA.

6. NIST. (2020). Special Publication 800-207, Zero Trust Architecture. National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.SP.800-207 (data obrashcheniya: 08.07.2025).

7. Ivanov P.A., Kapger I.V., Shaburov A.S. Model' realizacii upravleniya dostupom k informacionnym aktivam v koncepcii nulevogo doveriya // Vestnik Permskogo nacional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya. 2023. № 45. S. 147–163. DOI: 10.15593/2224-9397/2023.1.07. EDN ZHSITI.

8. Nguen F.H., Nguen T.A., Zaripova R.S. Zero Trust kak instrument zashchity informacionnyh aktivov kompanij // Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 12. S. 656–658. EDN CECSSU.

9. Enterprise Matrix MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (data obrashcheniya: 08.07.2025).

**Информация о статье:**
Статья поступила в редакцию: 26.06.2025; одобрена после рецензирования: 28.07.2025;
принята к публикации: 30.07.2025
**Information about the article:**
The article was submitted to the editorial office: 26.06.2025; approved after review: 28.07.2025;
accepted for publication: 30.07.2025

*Информация об авторах:*
**Игнатов Данил Юрьевич**, аспирант кафедры КБ-4 «Интеллектуальные системы информационной безопасности» МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), e-mail: ignatov.d.y@edu.mirea.ru, SPIN-код: 5064-2031

*Information about authors:*
**Ignatov Danil Yu.**, postgraduate student of the department of intelligent information security systems of the MIREA – Russian university of technology (119454, Moscow, Vernadsky ave., 78), e-mail: ignatov.d.y@edu.mirea.ru, SPIN: 5064-2031