Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/49-200**
Ссылка для цитирования этой статьи:
Кунтуганов М.Ф., Морозов С.А. Нулевое доверие: подход к безопасности коммутируемых соединений // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2025. №1

УДК 004.7 DOI:10.24412/2541-9269-2025-1-10-18

НУЛЕВОЕ ДОВЕРИЕ: ПОДХОД К БЕЗОПАСНОСТИ КОММУТИРУЕМЫХ СОЕДИНЕНИЙ

Кунтуганов М.Ф.[1], Морозов С.А.[2]
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, m.kuntuganov@yandex.ru
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, morozovsa@sstu.ru

ZERO TRUST: AN APPROACH TO SECURING COMMUTABLE CONNECTIONS

Kuntuganov M.F.[1], Morozov S.A.[2]
[2]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, m.kuntuganov@yandex.ru
[2]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, morozovsa@sstu.ru

Аннотация. Исследованы проблемы связанный с уязвимостями коммутируемых соединений актуальных для организаций. Проведен анализ отечественного и зарубежного опыта в сфере защиты периметра сети. Современное законодательство активно разрабатывается с целью регламентирования защиты от типовых угроз. Описывается подход к обеспечению безопасности подключений известный как zero trust в иностранных источниках. Предлагаются подходы к организации коммутируемых соединений на основе подхода нулевого доверия.

Ключевые слова: нулевое доверие, zero trust, информационная безопасность, коммутируемое соединений, угрозы безопасности.

Abstract. The problems related to the vulnerabilities of dial-up connections relevant to organizations are investigated. The analysis of domestic and foreign experience in the field of network perimeter protection is carried out. Modern legislation is being actively developed to regulate protection against typical threats. An approach to security assessment based on zero trust in foreign sources is described. Approaches to the organization of dial-up connections based on the zero-trust approach are proposed.

Keywords: zero trust, information security, dial-up connections, security threats.

В настоящее время Российская Федерация сталкивается с внешними вызовами в части усиления геополитического давления, выразившимся, в том числе в активизации кибератак со стороны ряда недружественных стран, включая государства Европейского союза, США, Японии и Южной Кореи. Отмечается кратное увеличение числа и интенсивности кибератак, направленных на государственные органы и организации на территории России. По оценкам экспертов, средний ущерб, наносимый компаниям кибератаками, составляет не менее 20 миллионов рублей в год, не учитывая репутационные потери, при этом наблюдается тенденция к увеличению данного показателя на треть в годовом исчислении (рис. 1). При этом 78% атак имели целевой характер.

Результаты исследований в области кибербезопасности, проведенных ФСТЭК, ФСБ и другими компетентными ведомствами, выявили ряд системных проблем, характерных для государственных и иных организаций Российской Федерации:

– Недостаточный уровень защищенности информационных систем.

– Неудовлетворительная подготовка персонала в вопросах обеспечения информационной безопасности.

– Дефицит квалифицированных специалистов в области кибербезопасности.

– Недостаточная квалификация администраторов информационных систем.

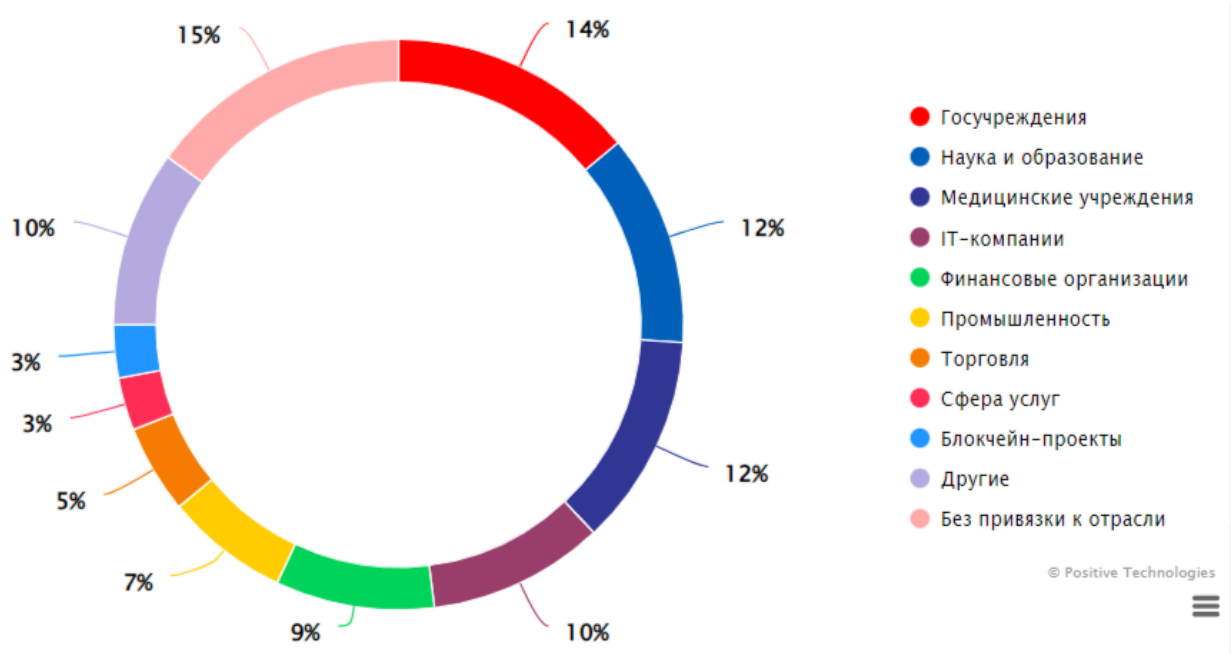

Рис. 1. График атак направленных на иформацииионную структуру орнизаций в России [1]

В сложившихся обстоятельствах Российская Федерация предпринимает активные меры реагирования на возникающие вызовы. В частности, 1 мая 2022

года Президентом Российской Федерации был подписан Указ № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации". Согласно данному указу, с 1 января 2025 года ряду организаций запрещается использовать средства защиты информации, происходящие из недружественных стран или от организаций, находящихся под их юрисдикцией. Также, Федеральной службой безопасности (ФСБ), Федеральной службой по техническому и экспортному контролю (ФСТЭК) и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) разрабатываются и реализуются дополнительные меры, направленные на усиление информационной безопасности [5].

Анализ отечественного и зарубежного опыта показывает, что традиционная модель защиты периметра корпоративной сети демонстрирует свою неэффективность в условиях динамично изменяющихся угроз. В связи с этим возникает необходимость внедрения новых подходов, одним из которых является концепция Zero Trust (Нулевое доверие). Данная модель ориентирована на минимизацию рисков путем применения строгой политики контроля доступа и постоянной проверки подлинности всех субъектов, взаимодействующих с информационными ресурсами.

Целью настоящего доклада является демонстрация актуальности внедрения концепции Zero Trust в российских организациях. Рассматриваются основные принципы и механизмы защиты коммутируемых соединений, а также подчеркивается необходимость перехода к данной модели безопасности в условиях растущих киберугроз и изменяющихся требований к защите информации.

Нулевое доверие — это комплексная стратегия безопасности, основанная по принципу «никогда не доверяй и всегда проверяй», которая отслеживает и контролирует шесть основных столпов безопасности: идентификационные данные, конечные точки, приложения, сеть, инфраструктуру и данные (рис. 2).

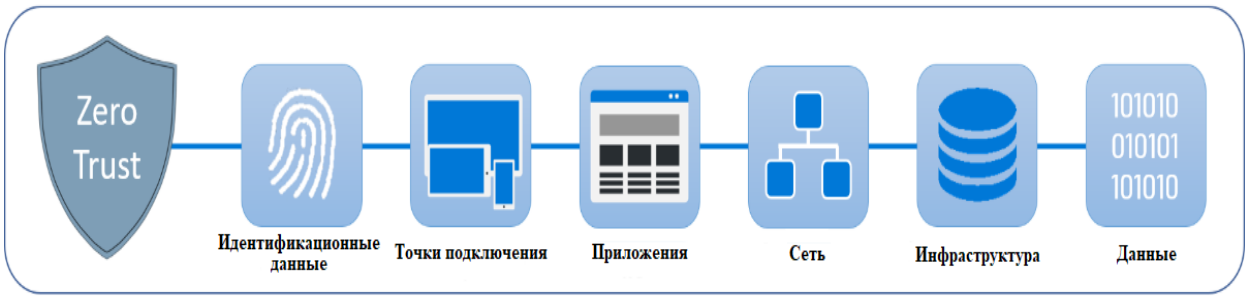

Рис. 2. Основные столпы безопасности стратегии Zero Trust

На практике правило «не доверяй никому и проверяй все» предполагает, что каждый запрос, устройство или пользователь не должны быть доверенными и должны рассматриваться как потенциальная угроза, пока не будут проверены методами строгой аутентификации, прежде чем будет разрешен доступ к сети. Это также означает, что пользователям и устройствам разрешен доступ только к тем конкретным приложениям или данным, которые им нужны. В таком виде концепцию сформулировал в 2010-м году John Kindervag - главный аналитик американской исследовательской компании Forrester Research.

Основной плюс стратегии в её исключительной надёжности. С точки зрения IT, Zero Trust – это значит отключить совершенно весь доступ пользователям, которых сеть компании не может надёжно идентифицировать.

ZTA (Zero Trust Architecture) построен на следующих основных постулатах [7]:

1. Все источники данных и компьютерные сервисы считаются ресурсами.
2. Все сеансы связи должны быть защищены независимо от местонахождения сети.
3. Доступ к индивидуальным ресурсам предприятия предоставляется только на один сеанс.
4. Возможность доступа к ресурсам определяется с помощью динамической политики с использованием триггерных условий и правил, установленных администратором политики.
5. На предприятии должны обеспечиваться гарантии того, что все устройства, подключаемые к сети, являются защищенными.
6. Аутентификация и авторизация на ресурсах происходят динамически.
7. Выполняется сбор информации о сетевой среде.

На основании вышеизложенных предположений считается, что модель нулевого доверия соответствует следующим основным принципам:

1. Никому не доверять по умолчанию:

– Все пользователи, устройства и приложения должны проходить проверку перед получением доступа к ресурсам.

– Не существует «доверенной» внутренней сети – каждый запрос рассматривается как потенциально опасный.

2. Минимизация привилегий (Least Privilege Access):

– Доступ предоставляется по принципу "минимально необходимого" (Just-in-Time и Just-Enough-Access).

– Даже авторизованные пользователи получают только те права, которые необходимы для выполнения их задач.

3. Постоянная проверка и верификация:

– Используются многофакторная аутентификация (MFA) и адаптивные механизмы контроля доступа.

– Каждое устройство и соединение проверяются на соответствие политике безопасности.

4. Микросегментация сети:

– Разделение сети на небольшие изолированные зоны, что предотвращает горизонтальное перемещение злоумышленников.

– Введение строгих политик взаимодействия между сегментами.

5. Мониторинг и анализ поведения:

– Использование инструментов анализа трафика и поведенческой аналитики (UEBA) для выявления аномалий.

– Реагирование на инциденты в режиме реального времени.

6. Безопасность устройств (Endpoint Security):

– Контроль состояния устройств перед предоставлением доступа (NAC – Network Access Control).

– Использование Zero Trust Network Access (ZTNA) вместо традиционных VPN, где VPN предоставляют пользователю полный доступ к сети, в то время как ZTNA предоставляет доступ только к необходимым приложениям и сервисам на основе политик контроля доступа.

1. Более половины организаций испытывают трудности с реализацией основных возможностей Zero Trust из-за отсутствия четкой стратегии.

2. Концепция Zero Trust охватывает обширную область систем предприятий, которые необходимо связать между собой, при этом не все системы интегрируются в концепцию Zero Trust.

3. Устаревшие устройства и программное обеспечение могут ограничить воплощение концепции, а их замена требует капитальных вложений и времени.

4. Требуется полный пересмотр всех правил, установленных в сети, что является трудоемким процессом.

5. Внедрение Zero Trust может вызывать неявное сопротивление со стороны ИТ-служб из-за большого объема работ по пересмотру правил, а также сопротивление сотрудников из-за ухудшения пользовательского опыта.

6. Нехватка квалифицированных специалистов в области информационной безопасности замедляет применение концепции.

7. Внедрение Zero Trust требует значительных инвестиций, времени и ресурсов.

8. Внедрение Zero Trust может привести к снижению продуктивности персонала, по крайней мере, на период внедрения.

9. Реализация Zero Trust требует глубокого понимания сетевых активов, поведения пользователей и потоков данных.

10. Обилие разрозненных инструментов, управляющих данными, может нарушить непрерывный поток данных, уменьшить видимость и увеличить риск неправильной конфигурации политик безопасности.

11. Несогласованность между бизнесом, ИТ-департаментом и департаментом информационной безопасности может затруднить внедрение.

12. Обосновать пользу и необходимость Zero Trust на уровне топ-менеджмента сложно, что препятствует широкому распространению.

1. Повышение уровня киберустойчивости.

Благодаря строгому контролю доступа и постоянной проверке подлинности всех пользователей и устройств, организация снижает вероятность успешных атак, включая фишинг, инсайдерские угрозы и компрометацию учетных данных.

2. Минимизация ущерба от взломов.

В случае компрометации одной части инфраструктуры атакующий не получит доступ ко всей системе, поскольку концепция Zero Trust предусматривает сегментацию сети и ограничение привилегий пользователей и устройств. Это уменьшает масштаб возможных атак.

3. Соответствие требованиям регуляторов.

Многие отрасли предъявляют строгие требования к защите данных (например федеральные законы Российской Федерации, указы президента РФ, постановления правительства, нормативные акты ФСБ, ФСТЭК, внутренние распорядительные акты организаций). Внедрение Zero Trust помогает компаниям соответствовать этим требованиям, снижая риски штрафов и юридической ответственности.

4. Гибкость в управлении удаленным доступом.

В условиях распространенной удаленной работы традиционные методы защиты теряют эффективность. Zero Trust обеспечивает безопасный доступ сотрудников к корпоративным системам, независимо от их местоположения, что делает работу с облачными сервисами и VPN более защищенной.

5. Эффективное использование ресурсов безопасности.

Концепция Zero Trust позволяет компаниям оптимизировать расходы на кибербезопасность за счет фокусировки на наиболее критичных аспектах защиты. Организации могут перераспределять бюджет, инвестируя в актуальные инструменты, такие как многофакторная аутентификация, мониторинг поведения пользователей и автоматизированный анализ угроз.

6. Снижение влияния человеческого фактора.

Большинство атак на инфраструктуру связаны с ошибками сотрудников (неосторожное открытие вложений, слабые пароли и т. д.). Zero Trust снижает зависимость от человеческого фактора, внедряя автоматизированные механизмы проверки и строгие политики доступа.

7. Интеграция с современными технологиями.

Zero Trust облегчает интеграцию с технологиями, такими как искусственный интеллект и машинное обучение, которые могут анализировать аномальное поведение пользователей, выявлять подозрительные действия в сети и автоматически применять меры по их блокировке.

В условиях возрастающего давления на информационную инфраструктуру России со стороны внешних киберугроз традиционные модели защиты перестают обеспечивать необходимый уровень безопасности. Внедрение концепции Zero Trust становится актуальной задачей для российских организаций, позволяя минимизировать риски утечек данных, атак на критически важные системы и несанкционированного доступа.

Анализ показал, что Zero Trust может стать ключевым инструментом в повышении уровня защиты отечественных предприятий и государственных структур. Однако процесс ее внедрения в России сталкивается с рядом сложностей, включая необходимость модернизации существующих ИТ-систем, значительные финансовые затраты и дефицит квалифицированных специалистов в области кибербезопасности. Дополнительным фактором, влияющим на реализацию Zero Trust, является необходимость адаптации модели к специфике российского законодательства и нормативных требований.

Несмотря на существующие вызовы, развитие Zero Trust в российских организациях открывает новые перспективы для защиты цифровых активов. В условиях импортозамещения особую значимость приобретает разработка отечественных решений в рамках данной концепции, что позволит минимизировать зависимость от зарубежных технологий и обеспечить соответствие национальным стандартам безопасности. Внедрение Zero Trust в будущем станет неотъемлемой частью стратегии кибербезопасности России, укрепляя ее защиту от современных и будущих угроз.

Литература

1. Актуальные киберугрозы IV квартала 2023 года по версии Positive Technologies. URL: https://d-russia.ru/aktualnye-kiberugrozy-iv-kvartala-2023-goda-po-versii-positive-technologies.html (дата обращения: Пресс-релиз - 29.02.2024)
2. Баранов С.А., Иванов П.В. "Информационная безопасность корпоративных сетей". Москва: Издательство "Бином", 2021.
3. Гостев А.В. "Кибербезопасность: угрозы, тренды и защита". Москва: Альпина Паблишер, 2019.
4. Каширин А.В., Смирнов Д.О. "Методы и средства защиты информации в условиях современных киберугроз". Санкт-Петербург: Питер, 2020
5. Приказ Аппарата Правительства Псковской области от 3 мая 2024 г. N 41-од "О внесении изменений в Положение об Управлении цифрового развития и связи Правительства Псковской области"
6. ФСТЭК России. "Методические рекомендации по обеспечению информационной безопасности в автоматизированных системах". Москва: ФСТЭК, 2022
7. NIST Special Publication 800-207 Zero Trust Architecture URL: https://doi.org/10.6028/NIST.SP.800-207 (Дата обращения: 01.02.2025)
8. Cisco Systems. "Zero Trust Security for the Enterprise". San Jose: Cisco Press, 2021.
9. Google Cloud. "BeyondCorp: A New Approach to Enterprise Security". Mountain View: Google, 2019.
10. Kindervag J. "Zero Trust Networks: Building Secure Systems in Untrusted Networks". Sebastopol: O'Reilly Media, 2017.
11. Microsoft Corporation. "Zero Trust Adoption Guide". Redmond: Microsoft Press, 2022.
12. Oltsik J. "The Rise of Zero Trust Security Strategies". Boston: Enterprise Strategy Group (ESG), 2021.
13. Rose S., Borchert O., Mitchell S., Connelly S. "Zero Trust Architecture". Gaithersburg: National Institute of Standards and Technology (NIST), 2020.