МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.18454/itech.2024.2.4

ТЕХНОЛОГИЯ ДОСТУПА К ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫМ РЕСУРСАМ СИСТЕМ ИКТ С НУЛЕВЫМ ДОВЕРИЕМ

Научная статья

Милаков А.С.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Студия MissoffDesign, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (9985585[at]gmail.com)

Аннотация

В статье рассматриваются актуальные вопросы кибербезопасности в условиях расширяющего ландшафта угроз, привнесённых цифровой трансформацией: интернет – интернет вещей (IoT), «облачные вычисления», искусственный интеллект (ИИ) и прочие новации ИТ-сферы. Особенно всё это касается систем критической информационной инфраструктуры (КИИ). Для предотвращения угроз кибербезопасности к таким объектам разработана новая технология доступа к ресурсам информационно-коммуникативных технологий (ИКТ) – Zero Trust («нулевое доверие»).

Рассмотрена концепция нулевого доверия, а также вопросы аутентификации и авторизации пользователей. Проанализированы основные модели разграничения доступа к объектам компьютерных систем Zero Trust со стороны их субъектов.

Обобщены основные принципы технологии нулевого доверия в виде базовых модельных положений.

Ключевые слова: нулевое доверие, концепция и архитектура Zero Trust, дискреционное разграничение доступа, мандатное разграничение доступа, ролевое разграничение доступа.

TECHNOLOGY FOR ZERO TRUST ACCESS TO INFORMATION AND COMPUTING RESOURCES OF ICT SYSTEMS

Research article

Milakov A.S.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Studio MissoffDesign, Saint-Petersburg, Russian Federation

* Corresponding author (9985585[at]gmail.com)

Abstract

The article examines current cybersecurity issues in the context of the expanding threat landscape brought by digital transformation: the Internet – the Internet of Things (IoT), cloud computing, artificial intelligence (AI) and other IT innovations. This is especially true for critical information infrastructure (CII) systems. To prevent cybersecurity threats to such facilities, a new technology of access to information and communication technology (ICT) resources – Zero Trust – has been developed.

The concept of Zero Trust is reviewed, as well as the issues of authentication and authorization of users. The main models of access control to the objects of Zero Trust computer systems by their subjects are analysed.

The basic principles of Zero Trust Technology are summarized in the form of basic model statements.

Keywords: Zero Trust, Zero Trust concept and architecture, discretionary access delimitation, mandated access control, role-based access control.

Введение

Цифровая трансформация (ЦТ, англ. digital transformation, DT или DX) производственных и общественных отношений, привнесённая 4–й промышленной революцией (*Индустрия 4.0*) породила новые технологии и сущности в современном социуме, такие как «облачные вычисления» и Интернет вещей (англ. Internet of Things, IoT), искусственный интеллект (ИИ, англ. artificial intelligence, AI), а также новые вызовы информационной безопасности (ИБ).

Традиционные модели безопасности уже не работают, они считаются слабыми и неэффективными для удовлетворения динамики доверия к информационно-коммуникационным технологиям (ИКТ).

Архитектура «Никому не доверяй» или «Архитектура нулевого доверия» (англ. Zero Trust Architecture, ZTA) – новая технология, которая призвана устранить пробел в области информационной безопасности путем применения политик, основанных на удостоверениях и непрерывной аутентификации, авторизации и проверке. Эта структура построена на нескольких уровнях доверия и логических компонентах, которые предназначены устранить разрыв доверия к ИБ, существующий в ИКТ.

Принятие этой концепции все еще находится на стадии развития, что является результатом нескольких вводящих в заблуждение выводов и предположений.

Материалы и методы

В статье был использован публикационный метод прогнозирования и прогнозирование на основе метода экспертных оценок. Исследование проводилось следующими способами:

1. Автор изучил источники по данной тематике (монографии, научные статьи, международные и государственные стандарты, материалы из Интернета и т.д.).

2. Далее была определена проблема доверия как философская концепция и описан ее смысл в кибербезопасности.

3. Затем была поставлена проблема недостаточности защиты с помощью периметра безопасности (укрепленной границы корпоративной сети). При выполнении обзора учитывалось мнение ведущих компаний в области кибербезопасности в виде аналитических данных. Также использовались международные стандарты в области ИБ.

4. Автор обосновал идею использования архитектуры нулевого доверия (ZTA) при построении систем безопасности в корпоративных сетях. В рамках концепции нулевого доверия также были описаны механизмы многофакторной аутентификации и классические модели разграничения доступа (дискреционная, мандатная, ролевая).

5. Автор использовал интуитивные методы в попытке отразить в этой научной публикации свой собственный опыт работы и исследований в ИБ-сфере, конкретно, в области построения систем корпоративной безопасности.

Цель работы:

1) обобщить литературные источники по архитектуре нулевого доверия (ZTA);

2) обозначить проблему доверия в области информационной безопасности и наметить пути ее решения;

3) показать, что классические методы противодействия угрозам и атакам на базе построения защищенного периметра корпоративной сети не всегда работают в современных сложных условиях при огромном росте киберпреступлений;

4) описать более надежные методы противостояния киберугрозам путем построения систем на базе архитектуры нулевого доверия (ZTA) с использованием многофакторной аутентификации и моделей разграничения доступа на базе методологий, изложенных в международных стандартах в области ИБ.

Концепция нулевого доверия

В материалах международной конференции ICCA 2020 [1, С. 1]. определили, что традиционная сетевая безопасность основана на концепции периметра безопасности, в соответствии с которой сеть делится на две части: внутреннюю доверенную сеть и внешнюю не доверенную сеть Основываясь на этом критерии разделения, хорошо структурированная защитная архитектура рассматривает безопасность сети как «матрёшку», где каждый периметр защищает область, которую он покрывает. По данным исследователей из компании Akamai [2], периметр – укрепленная граница сети, которая может включать пограничные маршрутизаторы, межсетевые экраны (МЭ, или брандмауэр, файрвол), системы обнаружения вторжений (СОВ, англ. Intrusion Detection System IDS), системы предотвращения вторжений (англ. Intrusion Prevention System, IPS), VPN-устройства (англ. Virtual Private Network, «виртуальная частная сеть»), программную архитектуру, демилитаризованную зону (англ. Demilitarized Zone, DMZ) и экранированные подсети.

Однако этот периметр безопасности представляет собой только однонаправленную защиту и бессилен против атак изнутри сети. Поэтому для защиты как от внутренних, так и от внешних угроз периметр безопасности необходимо усовершенствовать.

Концепция нулевого доверия, «никогда не доверяй, всегда проверяй», была впервые предложена Джоном Киндервагом в 2010 году [3] для решения проблем, вызванных внутренними угрозами для предприятия. В её основе лежит идея ограничения неявного доверия как признание ограниченности использования одиночных статических средств защиты в большой сети.

3.1. Доверие к кибербезопасности

Концепция доверия появилась задолго до кибербезопасности и обсуждалась и анализировалась учёными на протяжении многих десятилетий. Например, социологи определяют доверие, как «психологическое состояние, включающее намерение принять уязвимость, основанное на позитивных ожиданиях намерений или поведения другого человека».

Несмотря на то, что это общепринятое определение отражает междисциплинарную перспективу, оно не в полной мере отображает динамику и различные тонкости доверия. Таким образом, общепринятого научного определения доверия не существует. Значение и классификация доверия к кибербезопасности всегда определялись контекстом. Доверие может отражаться в надежности, полезности, доступности, репутации, риске, уверенности, качестве услуг и других понятиях. Однако ни одна из этих концепций точно не определяет доверие. Например, хотя некоторые специалисты по безопасности рассматривают доверие как метрику безопасности или методологию оценки, другие рассматривают его как отношения между сущностями. Направленность и требования к безопасности в различных сценариях влияют на доверие, наполняя его неопределенностью. Таким образом, внимание ученых сместилось с определения доверия на классификацию.

Из-за сложности и двусмысленности доверие классифицируется в зависимости от контекста. В безопасности разделяют доверие на явное и неявное. Явное доверие проистекает из четкого стандарта, полученной соответствующей информации, а также существующих законов и нормативных актов для объективного и справедливого суждения о доверии других людей. Это повышает безопасность, жертвуя практичностью. Имплицитное доверие, с другой стороны, проистекает из субъективного восприятия людьми надежности, основанной на эмоциях и опыте. Это приносит в жертву определенную степень безопасности ради большей практичности. Доверие конструируется на основе этических норм людей, а не установленных социальных норм, влияние которых ослабевает по мере углубления взаимного доверия между двумя сторонами.

В кибербезопасности существуют более четкие классификации доверия. Доверие, как фактор риска, убеждение, субъективная вероятность или транзитивность. Достоверность и точность полученной информации должна

оцениваться в заданном контексте. Доверие может отражать веру, уверенность или ожидания в отношении будущей деятельности/поведения целевого узла, а также взаимные отношения между узлами, которые ведут себя доверительным образом друг с другом. Например, в облачных вычислениях требуется как постоянное, так и динамическое доверие. Основное различие между постоянным и динамическим доверием заключается в продолжительности жизненного цикла доверия. Устойчивое доверие основано на долгосрочных базовых свойствах или инфраструктуре. Динамическое доверие, с другой стороны, существует в течение короткого времени в определенных состояниях, контекстах или для отдельной информации. Таким образом, надежность устойчивого доверия, в большей степени зависит от долгосрочных механизмов общества или промышленности, а динамическое доверие ближе к доверенным вычислениям, которыми пользуются современные компьютерные технологии. Однако эти определения и классификации доверия всегда опираются на традиционный периметр для разделения доверенных и не доверенных зон. Постепенное исчезновение традиционного периметра представляет собой проблему, которая побуждает к новому решению в области безопасности.

Национальный институт стандартов США (National Institute of Standards and Technology, NIST) опубликовал опубликовал документ «Описание архитектуры нулевого доверия» (Special Publication on Zero Trust Architecture, SP 800-207) [4], где были определены основные понятия архитектуры нулевого доверия.

Архитектура нулевого доверия, согласно SP 800-207, разделяется на плоскость управления и плоскость данных (см. рис. 1).

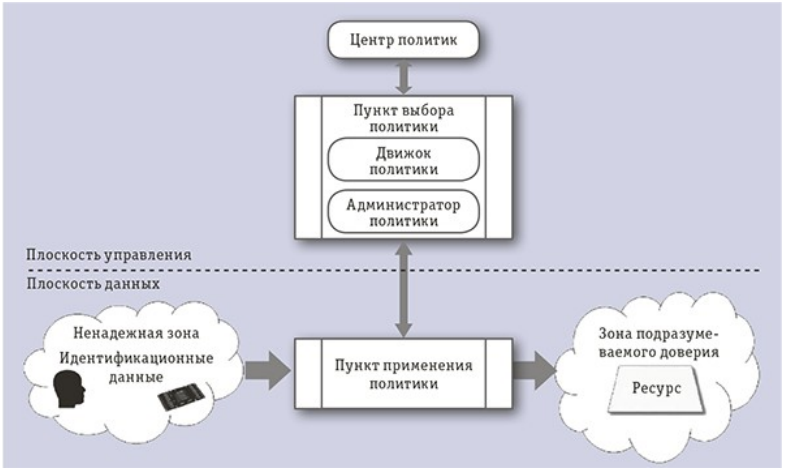

Рисунок 1 - Архитектура нулевого доверия NIST
DOI: https://doi.org/10.18454/itech.2024.2.4.1

Центр политики состоит из взаимосвязанных частей: движка политики и администратора политики, которые вместе образуют пункт выбора политики, определяющий, разрешен ли доступ к данным. В плоскости данных находится пункт применения политики, который предоставляет или запрещает доступ к ресурсу, в зависимости от принятого решения. Соответствующие функции, как правило, реализуются на единой платформе.

Когда пользователь в ненадежной зоне пытается осуществить доступ к ресурсу (данным или приложению), в первую очередь выполняется проверка его личности. В рамках следующей проверки выясняется, соответствует ли пользователь требованиям к безопасности. Система аутентификации принимает решение, руководствуясь политиками на основе рисков, которые могут меняться в зависимости от текущей ситуации на основе алгоритма оценки доверия.

По данным компании Microsoft [5], полноценная архитектура Zero Trust состоит из множества элементов, в числе которых инфраструктура открытых ключей (ИОК, англ. PKI, Public Key Infrastructure), система разведки угроз, подсистема регистрации событий и мониторинга, подсистема непрерывной диагностики и устранения последствий, система управления информацией и событиями безопасности (англ. Security Information and Event Management, SIEM).

Компания Forrester предложила расширенную архитектуру нулевого доверия (Zero Trust Extended, ZTX), охватывающую более широкий круг потоков данных, в том числе проходящих через локальные сети, облака, внешние приложения, сайты и различные виды конечных устройств, в том числе, датчики Интернета вещей и др. (см. рис. 2).

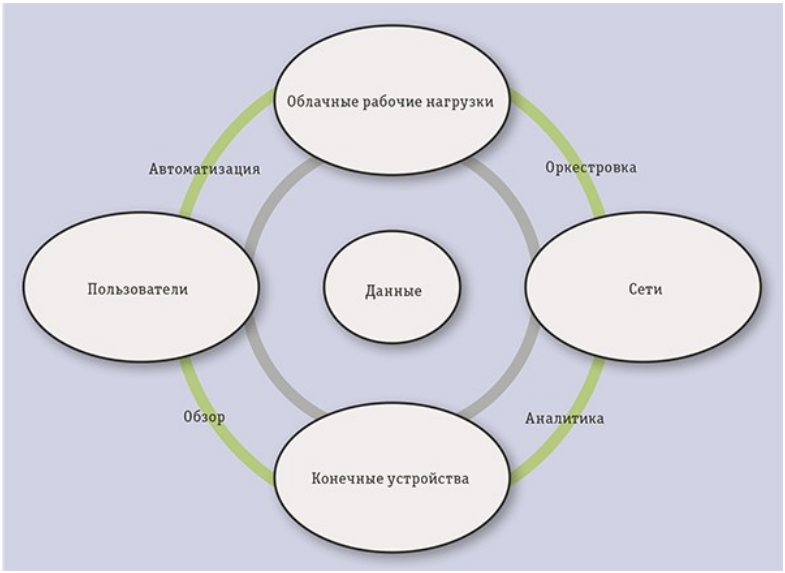

Рисунок 2 - Парадигма расширенной архитектуры нулевого доверия ZTX
DOI: https://doi.org/10.18454/itech.2024.2.4.2

Компания Gartner, основываясь на принципе непрерывной адаптивной оценки риска и доверия, также выдвинула идею о расширенной архитектуре нулевого доверия.

Улучшенная модель нулевого доверия расширяет архитектуру, предложенную NIST, обеспечивая более полную осведомленность о ситуации и учитывает практические особенности ввода в эксплуатацию (см. рис. 3). Согласно такой модели, в процессе выбора решений принимаются во внимание и субъект, и конечная точка, включая степень их соответствия требованиям безопасности.

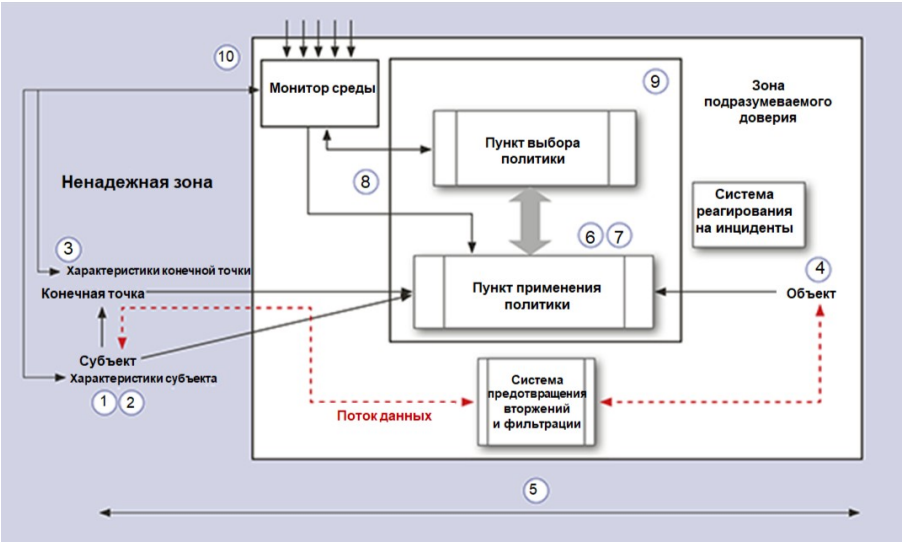

Рисунок 3 - Улучшенная модель нулевого доверия
DOI: https://doi.org/10.18454/itech.2024.2.4.3

Примечание: Расшифровку обозначений 1–10 см. в таблице 1

Ниже в таблице 1 приведен расширенный перечень требований (цифры в кружочках на рис. 3) к модели нулевого доверия, базирующийся на документе NIST.

Таблица 1 - Расширенный перечень требований улучшенной модели нулевого доверия

DOI: https://doi.org/10.18454/itech.2024.2.4.4

Требование	Описание
1. Все субъекты считаются ненадёжными и подлежат контролю доступа.	Все пользователи, в том числе работающие локально и удалённо, поставщики услуг и подрядчики, считаются подключёнными к ненадёжной сети и должны проходить контроль доступа через единый портал.
2. ИТ-системы считаются субъектами, требующими доступа.	Запрашивать доступ может не только пользователь, но и приложение на том же или другом сервере, устройства Интернета вещей, система ИИ или другая автономная система. К ним предъявляются такие же требования контроля доступа, как и к пользователям.
3. Для всех конечных устройств нужен контроль доступа.	В рамках решения нулевого доверия надёжность механизма, используемого субъектом для доступа к данным, является важным фактором выбора политики доступа, поэтому оценка конечной точки доступа и её соответствия требованиям ИБ – есть необходимый элемент запроса доступа. При этом, сама конечная точка доступа может быть аппаратным датчиком, рабочей станцией, сервером, облаком и т.д.
4. Все объекты подлежат микросегментации. Доступ к ним осуществляется через пункт применения политики.	Когда субъект делает запрос к данным или сервису, такой запрос может включать несколько дискретных объектов (ресурсов), например балансировщиков нагрузки, серверов приложений и хранилищ данных. Каждый из таких объектов защищён своим периметром и требует решения о доступе на основе политики безопасности.
5. Необходима сквозная защита всех сеансов связи от конечной точки до объекта. Требуется обеспечить аутентификацию, конфиденциальность и целостность источника данных.	Защита данных – один из ключевых аспектов нулевого доверия. Соблюдение этого принципа гарантирует, что источник информации, ещё не охваченный архитектурой нулевого доверия, будет защищён в момент входа.
6. Доступ предоставляется к каждому объекту в отдельности и только на один сеанс.	Доверие к субъекту и конечной точке оценивается непосредственно во время обращения с учётом правил доступа к запрашиваемому объекту. На основании этого принимается решение о предоставлении доступа. Аутентификация и авторизация происходит в режиме реального времени, причём срок действия и объём полномочий определяются соответственно длительностью и назначением сеанса. Для доступа к некоторым или всем объектам может выполнятся многофакторная или иная расширенная аутентификация. В соответствии с политикой безопасности, на протяжении всего сеанса выполняется мониторинг и могут потребоваться повторная аутентификация и авторизация. Доступ к одному объекту (ресурсу) не предполагает автоматического одобрения доступа к другому объекту в рамках того же сеанса.
7. Привилегии, необходимые для выполнения действий с объектом, предоставляются в отдельности для каждого объекта и на один сеанс.	Для каждого сеанса применяется принцип наименьших привилегий, чтобы ограничить субъекту обзор и доступ строго необходимым. Привилегии, предоставленные для работы с одним объектом, не предоставляются другим.

8. Для принятия решений о доступе используются адаптивные политики.	Политика, определяющая уровни доверия и решения о доступе, является динамической и может меняться в зависимости от состояния сети. Политики могут основываться на правилах или алгоритмах машинного обучения. В любом случае права субъекта или конечной точки со временем могут меняться. Например, может измениться уровень угрозы в сети или система мониторинга определит, что ПО конечной точки уязвимо для нового эксплойта, что повлияет на решение о доступе.
9. Механизмы безопасности в рамках архитектуры нулевого доверия должны быть достаточно надёжными, чтобы обеспечить необходимый уровень доверия.	Системы безопасности, используемые в среде нулевого доверия, должны иметь сертификаты, подтверждающие, что их разработка и выпуск осуществлялись с использованием формальных методов проверки надёжности и что эти системы соответствуют требованиям действующих стандартов безопасности.
10. Для повышения качества принимаемых решений производится сбор ситуационной информации с учётом требований конфиденциальности.	Для повышения эффективности формирования и применения политик безопасности собираются эксплуатационные данные, в том числе, об обновлениях сетевой инфраструктуры, новых угрозах, характере трафика, запросах доступа и пр. Эти данные могут также использоваться для предоставления контекстных сведений о запросах доступа, но при этом следует учитывать право пользователей на защиту персональных данных. Основным фильтром источником собираемых данных является система анализа угроз, которая в непрерывном цикле обеспечивает мониторинг доступа, проверку и оценку угроз, адаптацию и переоценку доверия к текущим сеансам связи.

Комбинация требований к системе нулевого доверия и принципы её функционирования, изложенные на рисунке 3 и в таблице 1, на наш взгляд, дают достаточное полное представление об архитектуре нулевого доверия.

3.2. Многофакторная аутентификация (MFA)

А. Ю. Щеглов в книге «Модели, методы и средства контроля доступа к ресурсам вычислительных систем» [6, С. 40] дает определение многофакторной аутентификации (Multi-factor Authentication, MFA) как процессу входа в систему, который состоит из нескольких шагов и требует от субъекта указать кроме пароля дополнительную информацию. Кроме пароля, MFA может запросить идентификатор или код, отправленный на электронную почту, ответить на секретный вопрос или сканировать отпечатки пальцев.

Система сохраняет этот идентификатор и информацию о пользователе, чтобы проверить пользователя при следующем входе в систему. Вход в систему – это многоступенчатый процесс, в ходе которого проверяется пароль и другая идентификационная информация.

Схематично процесс работы MFA представлен на рисунке 4.

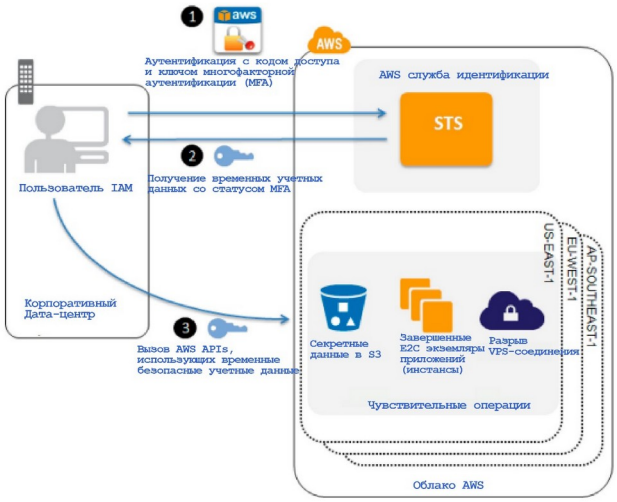

Рисунок 4 - Процесс входа в систему нулевого доверия с помощью MFA

DOI: https://doi.org/10.18454/itech.2024.2.4.5

Механизмы доступа к объектам системы нулевого доверия

4.1. Дискреционная модель разграничения доступа

Согласно мнению эксперта в области кибербезопасности Katlyn Gallo [7], дискреционный контроль доступа (англ. Discretionary Access Control, DAC) – это один из многих методов контроля доступа, обеспечивающих безопасность информационных систем. DAC — это метод, который предоставляет пользователям контроль над разрешениями на их ресурсы, позволяя владельцам информационных систем и данных решать, кто может получить доступ к соответствующим ресурсам и какой уровень доступа они могут иметь. Этот подход поддерживает принцип наименьших привилегий – концепцию, которая выступает за предоставление пользователям минимального объема доступа, необходимого для выполнения их работы. Поскольку дискреционный контроль доступа полагается на принятие решений человеком при предоставлении доступа, информационная система или владелец данных должны тщательно проверять запросы на доступ, чтобы гарантировать, что не будут предоставлены чрезмерно широкие права.

На самом верхнем уровне DAC использует списки управления доступом (англ. Access Control List, ACL) для назначения разрешений использования ресурсов. Списки ACL содержат либо пользователей, либо предопределенные группы пользователей и соответствующие им уровни доступа. Эти уровни обычно включают доступ для чтения, записи и выполнения, что позволяет человеку просматривать, изменять или запускать процесс, или программу соответственно.

Например, представьте, что пользователь пытается открыть общий файловый ресурс в корпоративной сети. Когда этот пользователь запрашивает доступ, система DAC проверяет информацию аутентификации и сравнивает ее со списком управления доступом, связанным с ресурсом, к которому пользователь пытается получить доступ. Если информация соответствует записи ACL, пользователю предоставляется доступ, определенный в ACL, будь то чтение, запись или выполнение. Если информация о пользователе не соответствует ACL, запрос отклоняется.

Хотя дискреционный контроль доступа обеспечивает гибкость и свободу действий пользователя, он имеет некоторые недостатки и ограничения.

Поскольку DAC полагается на владельцев ресурсов при принятии решений по управлению доступом, неправильно настроенный ACL или неправильное понимание требований безопасности может привести к раскрытию данных и несанкционированному доступу.

DAC не является масштабируемым методом контроля доступа, поскольку управление доступом для многих ресурсов и пользователей может оказаться трудоемким и сложным.

В DAC отсутствует централизованное управление, поскольку доступ применяется на уровне ресурсов. Это затрудняет внедрение определенных политик безопасности в организации и оценку существующих политик.

DAC не обеспечивает адекватной защиты от внутренних угроз, когда авторизованные пользователи могут злоупотреблять своими привилегиями для доступа или кражи конфиденциальных данных, предоставления разрешений неавторизованным пользователям или раскрытия информации неавторизованным лицам.

4.2. Мандатная модель разграничения доступа

Отмеченных недостатков дискреционной модели во многом лишено мандатное разграничение доступа (англ. Mandatory Access Control, MAC), подчеркивает А. Ю. Щеглов в книге «Модели, методы и средства контроля доступа к ресурсам вычислительных систем» [6, С. 28].

В модели MAC политика контроля доступа применяется системой, а не по усмотрению владельца ресурса. Хотя MAC предлагает меньшую гибкость и может быть более сложным, он имеет более безопасную структуру контроля доступа, ориентированную на обеспечение соответствия доступа заданной классификации данных и уровням чувствительности. По этой причине MAC часто используется для сетей и информационных систем, которые обрабатывают высокочувствительную или конфиденциальную информацию, например, в государственных учреждениях для доступа к ресурсам информации ограниченного доступа или ресурсам критической информационной инфраструктуры (КИИ).

Мандатный механизм управления доступом – это политика контроля доступа, которая единообразно применяется ко всем субъектам и объектам в пределах информационной системы. Субъекту, которому предоставлен доступ к информации, запрещено выполнять любое из следующих действий:

– передавать информацию неавторизованным субъектам или объектам;

– предоставлять свои привилегии другим субъектам;

– изменять один или нескольких атрибутов безопасности субъектов, объектов, информационной системы или компонентов системы;

– выбирать атрибуты безопасности, которые будут связаны с вновь созданными или измененными объектами;

– изменять правила, регулирующие контроль доступа.

Субъектам, определенным организацией, могут быть явно предоставлены определенные организацией привилегии (т. е. они являются доверенными субъектами), так что они не ограничены некоторыми или всеми из вышеперечисленных ограничений.

А. Ю. Щеглов в книге «Модели, методы и средства контроля доступа к ресурсам вычислительных систем» [6, С. 47] для мандатного разграничения доступа к объектам компьютерной системы доказывает теорему: ***«Если начальное состояние компьютерной системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое последующее состояние компьютерной системы также безопасно»***.

При использовании мандатного разграничения доступа к объектам необходимо также обеспечить достоверное подтверждение назначенного пользователю уровня допуска даже при отсутствии защищенного канала связи с сервером аутентификации. Согласно материалам компании Microsoft [5] это может быть обеспечено при использовании инфраструктуры открытых ключей X.509 (англ. Public Key Infrastructure, PKI).

4.3. Ролевое разграничение доступа

По определению экспертов Microsoft [9] ролевое разграничение доступа (англ. Role-Based Access Control, RBAC) – это система авторизации которая обеспечивает детальное управление доступом к ресурсам системы с нулевым доверием, основанная на том факте, что в реальной жизни организации ее сотрудники выполняют определенные функциональные обязанности не от своего имени, а в рамках некоторой занимаемой ими должности (или роли). Реализация ролевого разграничения доступа к объектам компьютерной системы требует разработки набора (библиотеки) ролей, определяемых как набор прав доступа к объектам информационной системы (прав на выполнение над ними определенного набора действий). Этот набор прав должен соответствовать выполняемой работником трудовой функции.

Назначение роли состоит из трех элементов: участника безопасности, определения роли и области действия.

Ролевая модель разграничения доступа сочетает элементы мандатного разграничения (объединение субъектов и объектов доступа в одном правиле) и дискреционного разграничения (назначение ролей отдельным субъектам).

Преимущества ролевого разграничения доступа к объектам проявляются при организации коллективного доступа к ресурсам сложных информационных систем с большим количеством пользователей и объектов.

К недостаткам ролевого разграничения доступа относится отсутствие формальных доказательств безопасности компьютерной системы, возможность внесения дублирования и избыточности при предоставлении пользователям прав доступа, сложность конструирования ролей.

Заключение

Всесторонне рассмотрев различные архитектуры модели «Никому не доверяй», можно заметить, что она представляет собой целостное решение, охватывающее весь жизненный цикл корпоративной сети. Модель охватывает такие аспекты, как аутентификация, контроль доступа, защита данных, сетевая безопасность, безопасность приложений и мониторинг угроз. Интегрируя эти технологии в архитектуру, модель «Никому не доверяй» достигает своих целей в области безопасности. С точки зрения доверия, именно доверие, установленное с помощью этих

аспектов, обеспечивает общую безопасность архитектуры нулевого доверия, как следует из материалов симпозиума ACM (2019 г.) [10].

В контексте проверки подлинности удостоверений доверие является производным от проверки легитимности запрашивающей сущности и служит фундаментальным фактором при создании архитектуры нулевого доверия. Независимо от того, идет ли речь о традиционных механизмах аутентификации пользователей или более контекстно-зависимых и непрерывных методах проверки подлинности удостоверений, а также о механизмах проверки подлинности устройств, ориентированных на цифровую идентификацию, эти технологии проверки подлинности имеют одинаковое значение в архитектуре нулевого доверия. Специалистам по безопасности с нулевым доверием необходимо выборочно применять соответствующие технологии в зависимости от конкретных сценариев и бизнес-требований.

В сфере управления доступом доверие возникает из фактического предоставления и ограничения разрешений сущностям во время доступа, что формирует фундаментальную гарантию принципа минимальных привилегий в нулевом доверии. Механизмы управления доступом на основе удостоверений, ролей, атрибутов, намерений и рисков, которые помогают в детализации доступа, предоставлении разрешений и управлении политиками, являются важнейшими факторами при проектировании и реализации архитектуры нулевого доверия. Эти механизмы должны быть приняты во внимание исследователями систем безопасности с нулевым доверием. Что касается защиты данных, доверие зависит от надежности алгоритмов шифрования, а реализация архитектуры нулевого доверия требует выбора подходящих решений на основе конкретных требований безопасности, форматов данных и вычислительных ресурсов данного сценария [11, С. 129].

С точки зрения сетевой безопасности доверие строится на эффективности сегментации сети, что является важным аспектом, который необходимо определить перед развертыванием архитектуры нулевого доверия. Различные стратегии сегментации будут влиять на выбор конкретных технологий в других областях, что в конечном итоге повлияет на гибкость архитектуры нулевого доверия.

С другой стороны, безопасность приложений и мониторинг угроз еще больше смягчают неопределенности, связанные с человеческим фактором в архитектуре нулевого доверия. Оперативно обнаруживая аномальные события и реагируя на них, эти методы помогают снизить риски безопасности.

Однако важно отметить, что конечной целью модели «Никому не доверяй» является защита от внутренних угроз, от которых существующие модели безопасности не могут защитить, что требует реалистичного развертывания систем ИБ для проверки теоретической и методологической осуществимости и надежности защиты. Кроме того, исследования инсайдерских угроз — это область, на которой должны сосредоточиться исследователи модели нулевого доверия. Только всестороннее понимание внутренних угроз может сделать результаты исследований нулевого доверия полезными и осуществимыми для решения практических задач.

Научная новизна работы заключается в инновационном подходе к изучению внедрения ZTA для защиты ИТ-инфраструктуры компаний от киберугроз, особенно от внутренних угроз (которые трудно поддаются нейтрализации классическими способами, к примеру, с помощью построения периметра безопасности). Автор провел глубокий анализ зарубежных и российских литературных источников по данной тематике. В отличие от подобных исследований зарубежных авторов, которые перечислены в списке литературы, была проделана исследовательская работа по анализу применимости архитектуры нулевого доверия в совокупности с многофакторной аутентификацией и моделями разграничения доступа.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Ahmed I. Protection of Sensitive Data in Zero Trust Model / I. Ahmed, T. Nahar [et al.] // In Proceedings of the International Conference on Computing Advancements (ICCA 2020). — 2020. — № 63. — P. 1–6. DOI: 10.1145/3377049.3377114

2. Zero Trust Security. — URL: https://www.akamai.com/solutions/security/zero-trust-security (accessed: 23.02.2024).

3. Kindervag J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security / J. Kindervag // Forrester Research, For Security & Risk Professionals. — URL: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (accessed: 23.01.2024).

4. Chandramouli R. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-location / R. Chandramouli, Z. Butcher // Environments NIST Special Publication. DOI:10.6028/NIST.SP.800-207A

5. Сертификаты открытого ключа X.509. — URL: https://learn.microsoft.com/ru-ru/windows/win32/seccertenroll/about-x-509-public-key-certificates (дата обращения: 23.02.2024).

6. Щеглов А. Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем / А. Ю. Щеглов. — СПб.: Университет ИТМО, 2014. — 95 с. — URL: https://books.ifmo.ru/file/pdf/1764.pdf (дата обращения: 23.02.2024).

7. Guide to Discretionary Access Control (DAC) With Examples. — URL: https://builtin.com/cybersecurity/discretionary-access-control (accessed: 23.02.2024).

8. Mandatory Access Control (MAC). — URL: https://csrc.nist.gov/glossary/term/mandatory_access_control (accessed: 23.02.2024).

9. What is Azure role-based access control (Azure RBAC)? — URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview (accessed: 23.02.2024).

10. Zaheer Z. eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices / Z. Zaheer, H. Chang, S. Mukherjee [et al.] / Proceedings of the 2019 ACM Symposium on SDN Research. — 2019. DOI: 10.1145/3314148.3314349

11. Jiang H. OZTrust: An O-RAN Zero-Trust Security System / H. Jiang, H. Chang, S. Mukherjee [et al.] // IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). — 2023. — P. 129–134.

Список литературы на английском языке / References in English

1. Ahmed I. Protection of Sensitive Data in Zero Trust Model / I. Ahmed, T. Nahar [et al.] // In Proceedings of the International Conference on Computing Advancements (ICCA 2020). — 2020. — № 63. — P. 1–6. DOI: 10.1145/3377049.3377114

2. Zero Trust Security. — URL: https://www.akamai.com/solutions/security/zero-trust-security (accessed: 23.02.2024).

3. Kindervag J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security / J. Kindervag // Forrester Research, For Security & Risk Professionals. — URL: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (accessed: 23.01.2024).

4. Chandramouli R. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-location / R. Chandramouli, Z. Butcher // Environments NIST Special Publication. DOI:10.6028/NIST.SP.800-207A

5. Sertifikaty otkrytogo kljucha X.509 [X.509 Public Key Certificates]. — URL: https://learn.microsoft.com/ru-ru/windows/win32/seccertenroll/about-x-509-public-key-certificates (accessed: 23.02.2024). [in Russian]

6. Shcheglov A. Yu. Modeli, metody i sredstva kontrolja dostupa k resursam vychislitel'nyh sistem [Models, Methods and Means of Access Control to Computer System Resources] / A. Yu. Shcheglov. — St. Petersburg: ITMO University, 2014. — 95 p. — URL: https://books.ifmo.ru/file/pdf/1764.pdf (accessed: 23.02.2024). [in Russian]

7. Guide to Discretionary Access Control (DAC) With Examples. — URL: https://builtin.com/cybersecurity/discretionary-access-control (accessed: 23.02.2024).

8. Mandatory Access Control (MAC). — URL: https://csrc.nist.gov/glossary/term/mandatory_access_control (accessed: 23.02.2024).

9. What is Azure role-based access control (Azure RBAC)? — URL: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview (accessed: 23.02.2024).

10. Zaheer Z. eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices / Z. Zaheer, H. Chang, S. Mukherjee [et al.] / Proceedings of the 2019 ACM Symposium on SDN Research. — 2019. DOI: 10.1145/3314148.3314349

11. Jiang H. OZTrust: An O-RAN Zero-Trust Security System / H. Jiang, H. Chang, S. Mukherjee [et al.] // IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). — 2023. — P. 129–134.