Лекция 6: Аутентификация и управление учётными записями

Тема: Управление доступом и управление идентификацией

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Здравствуйте. На прошлой лекции мы рассмотрели модели управления доступом и кратко затронули тему аутентификации. Сегодня мы подробно изучим технологии аутентификации и практики управления учётными записями. Это, пожалуй, одна из наиболее критически важных областей современной безопасности, поскольку, как говорят, «идентичность — это новый периметр».

Позвольте привести статистику, которая должна вызывать беспокойство. Согласно отчёту Identity Defined Security Alliance (IDSA), отраслевого консорциума по безопасности на основе идентификации, за 2025 год, скомпрометированные учётные данные (credentials) остаются вектором атаки номер один, участвуя в более чем 80% случаев нарушения безопасности веб-приложений. Несмотря на десятилетия исследований и миллиарды долларов, вложенных в технологии безопасности, мы по-прежнему с трудом отвечаем на фундаментальный вопрос: «Действительно ли этот человек является тем, за кого себя выдаёт?»

Ландшафт аутентификации кардинально изменился в последние годы. Мы перешли от простых паролей к многофакторной аутентификации, от локальных хранилищ идентификации к облачным поставщикам идентификации и от безопасности на основе периметра к архитектурам нулевого доверия. Сегодня мы рассмотрим все эти темы, и я помогу вам понять не только то, что делают эти технологии, но и почему они важны и как они сочетаются друг с другом.

Часть 1: Факторы аутентификации

На предыдущей лекции я представил пять категорий факторов аутентификации. Сегодня рассмотрим каждую из них подробнее, уделяя особое внимание практической реализации и вопросам безопасности.

Факторы знания: проблема паролей

То, что вы знаете — пароли, PIN-коды, парольные фразы, контрольные вопросы — остаётся наиболее широко используемым фактором аутентификации, несмотря на то что является самым слабым. Причины устойчивости паролей просты: их дёшево реализовать, пользователи их понимают, и они не требуют специального оборудования.

Однако у паролей есть фундаментальные проблемы. Человеческая память ограничена, поэтому пользователи выбирают простые, легко запоминающиеся пароли.

NordPass, сервис управления паролями, в своём ежегодном отчёте о наиболее распространённых паролях неизменно показывает, что наиболее распространённые пароли — это такие, как: «123456», «password» и «qwerty». Даже когда пользователи пытаются создать сложные пароли, они часто следуют предсказуемым шаблонам — заглавная первая буква, цифра в конце, замена «а» на «@».

Повторное использование паролей приобрело характер эпидемии. Согласно исследованиям Dashlane, компании-разработчика менеджера паролей, средний пользователь имеет более 100 учётных записей в сети, но использует всего около дюжины уникальных паролей. Когда один сервис подвергается нарушению безопасности, злоумышленники пробуют эти учётные данные на других сервисах — техника, называемая подстановкой учётных данных (credential stuffing). В 2025 году мы наблюдали атаки подстановкой учётных данных, при которых миллионы украденных учётных данных проверялись на популярных сервисах в течение нескольких часов после раскрытия утечки.

Организации пытались решить проблему слабых паролей с помощью политик: минимальная длина, требования сложности, регулярная смена. Однако исследования NIST (National Institute of Standards and Technology, Национальный институт стандартов и технологий), задокументированные в Special Publication 800-63B, показали, что многие из этих политик контрпродуктивны. Требования сложности приводят к тому, что пользователи записывают пароли или используют предсказуемые шаблоны замены символов. Обязательная смена паролей приводит к последовательностям типа password1, password2, password3.

Современные рекомендации от NIST и других организаций изменились. Текущие рекомендации делают акцент на длине, а не на сложности — парольные фразы вроде «correct horse battery staple» одновременно более безопасны и легче запоминаются, чем «P@ssw0rd!». Принудительную смену паролей следует исключить, кроме случаев подозрения на компрометацию. Следует внедрять проверку на скомпрометированные пароли — блокировку паролей, которые встречаются в известных базах данных утечек.

Факторы владения: то, что у вас есть

То, что у вас есть, обеспечивает второй уровень безопасности. Даже если злоумышленник знает ваш пароль, он не сможет пройти аутентификацию без физического доступа к вашему токену или устройству. Эта категория включает аппаратные токены, смарт-карты, мобильные телефоны и ключи безопасности.

Токены одноразовых паролей (OTP) используются уже несколько десятилетий. Традиционные аппаратные токены, такие как RSA SecurID, генерируют новый шестизначный код каждые 30 или 60 секунд, синхронизированный с сервером аутентификации. Эти коды действительны только однократно и быстро истекают, поэтому даже если злоумышленник перехватит один из них, он будет бесполезен к моменту попытки использования.

Программные OTP в значительной степени заменили аппаратные токены. Приложения, такие как Google Authenticator, Microsoft Authenticator и Authy, реализуют алгоритм одноразового пароля на основе времени TOTP (Time-based One-Time Password), определённый в RFC 6238. Приложение и сервер используют общий секретный ключ, и оба используют этот ключ вместе с текущим временем для генерации одинакового кода. Это обеспечивает безопасность, эквивалентную аппаратным токенам, без дополнительных затрат.

OTP на основе SMS отправляет код на ваш телефон в виде текстового сообщения. Это удобно, поскольку не требует установки приложения, но имеет существенные недостатки в плане безопасности. Атаки с подменой SIM-карты, при которых злоумышленники убеждают мобильных операторов перенести ваш номер телефона на их SIM-карту, стали распространённым явлением. Уязвимости в сети SS7 (Signaling System 7, Система сигнализации номер 7) позволяют опытным злоумышленникам перехватывать текстовые сообщения. По этим причинам NIST объявил SMS устаревшим в качестве фактора аутентификации в 2016 году, хотя он по-прежнему широко используется благодаря своему удобству.

Аутентификация через push-уведомления является улучшением по сравнению с SMS. Вместо ввода кода вы получаете push-уведомление с вопросом «Вы только что попытались войти?» и просто нажимаете «Да» или «Нет». Этот метод более устойчив к фишингу, поскольку нет кода, который можно ввести на поддельном сайте. Однако пользователи могут привыкнуть подтверждать каждое уведомление не задумываясь — проблема, называемая «усталостью от MFA (Multi-Factor Authentication, многофакторная аутентификация)», которую злоумышленники эксплуатируют путём массовой рассылки уведомлений.

Аппаратные ключи безопасности, такие как YubiKey, представляют собой золотой стандарт для факторов владения. Эти небольшие USB- или NFC-устройства (NFC — Near Field Communication, связь ближнего поля) реализуют надёжные криптографические протоколы и устойчивы к фишингу по своей конструкции. Когда вы проходите аутентификацию с помощью ключа безопасности, ключ проверяет подлинность легитимного сайта перед ответом, поэтому фишинговый

сайт не может перехватить пригодные для использования учётные данные. Мы подробно обсудим их при рассмотрении FIDO2 (Fast Identity Online 2).

Биометрические факторы: то, чем вы являетесь

Биометрия использует физические или поведенческие характеристики для аутентификации. Отпечатки пальцев, распознавание лица, сканирование радужной оболочки глаза, голосовые отпечатки и даже анализ походки — всё это может служить факторами аутентификации.

Распознавание отпечатков пальцев — наиболее зрелая биометрическая технология. Современные датчики отпечатков пальцев не хранят изображение вашего отпечатка — они хранят математическое представление, называемое шаблоном. Когда вы прикасаетесь к датчику, он вычисляет новый шаблон и сравнивает его с сохранённым. Это сравнение должно быть нечётким, поскольку никакие два считывания не являются абсолютно идентичными, что создаёт возможность ложных совпадений.

Распознавание лица стало повсеместным благодаря смартфонам. Современные системы используют инфракрасные проекторы или проекторы структурированного света для создания трёхмерной модели лица, что делает их устойчивыми к фотографиям. Face ID от Apple, представленный в 2017 году, заявляет о вероятности ложного совпадения один к миллиону — значительно лучше, чем распознавание отпечатков пальцев Touch ID.

Проблема биометрии заключается в том, что биометрические данные невозможно изменить. Если данные вашего отпечатка пальца скомпрометированы, вы не можете получить новый отпечаток. Это уже случалось — утечка данных OPM (Office of Personnel Management, Управление кадровой службы США) в 2015 году привела к раскрытию данных отпечатков пальцев миллионов федеральных служащих и подрядчиков. По этой причине биометрия никогда не должна быть единственным фактором аутентификации для приложений с высоким уровнем безопасности.

Биометрические данные также вызывают серьёзные опасения в отношении конфиденциальности. В отличие от паролей, биометрия раскрывает информацию о том, кто вы. Распознавание лица, в частности, вызвало споры о слежке и гражданских свободах. Организации, внедряющие биометрию, должны тщательно учитывать последствия для конфиденциальности и обеспечивать соответствие таким нормативным актам, как GDPR (General Data Protection Regulation, Общий регламент защиты данных ЕС).

Крайне важно различать **удалённую (серверную) биометрию** и **локальную (клиентскую) биометрию**. В серверных системах биометрические шаблоны хранятся в центральной базе данных, создавая огромную цель для атаки. В локальной биометрии (как Apple Touch ID/Face ID или Windows Hello) биометрический шаблон никогда не покидает защищённого анклава (secure

enclave) устройства. Устройство проверяет пользователя и просто передаёт криптографический ключ на сервер (модель FIDO). Этот подход сохраняет конфиденциальность и исключает риск утечки центральной базы биометрических данных.

Контекстуальные факторы: где и как

Местоположение и поведение предоставляют дополнительные сигналы аутентификации. Ваш IP-адрес, координаты GPS, время суток, используемое устройство и ваши поведенческие паттерны — всё это может влиять на решения об аутентификации.

Аутентификация на основе рисков использует эти сигналы для регулирования требуемого уровня аутентификации. Если вы входите в систему с привычного устройства, в привычное время, из привычного места, система может принять только пароль. Если вы входите с нового устройства из другой страны в 3 часа ночи, система может потребовать дополнительные факторы или полностью заблокировать попытку.

Поведенческая биометрия анализирует то, как вы взаимодействуете с системами. Ваш ритм набора текста — время между нажатиями клавиш и длительность удержания каждой клавиши — удивительно уникален. Способ, которым вы перемещаете мышь, как вы держите телефон, и ваши жестовые паттерны на сенсорных экранах — всё это создаёт поведенческий отпечаток. Это может обеспечить непрерывную аутентификацию, проверяя вашу личность не только при входе, но и на протяжении всей сессии.

Преимущество контекстуальных факторов в том, что они невидимы для пользователя. Вам не нужно делать ничего дополнительного — система просто наблюдает за вашим обычным поведением. Трудность заключается в точности. Поведенческие паттерны варьируются, и отличить нормальные вариации от действий злоумышленника сложно. Ложные срабатывания — когда законные пользователи блокируются из-за того, что их поведение показалось необычным — вызывают разочарование и снижают безопасность за счёт обходных путей.

Часть 2: Многофакторная аутентификация (MFA)

Многофакторная аутентификация требует от пользователей предоставления нескольких факторов аутентификации из разных категорий. Принцип заключается в эшелонированной защите — скомпрометировать несколько независимых факторов сложнее, чем один.

Настоящая MFA использует факторы из разных категорий. Пароль плюс ключ безопасности — это настоящая MFA: знание плюс владение. Пароль плюс отпечаток пальца — это настоящая MFA: знание плюс биометрия. Пароль плюс контрольный вопрос — это НЕ настоящая MFA: оба фактора относятся к категории знания, поэтому компрометация одного может привести к компрометации другого.

Улучшение безопасности благодаря MFA весьма значительно. Согласно отчёту Microsoft за 2023 год, MFA блокирует 99,9% автоматизированных атак. Google сообщает, что добавление фактора на основе телефона блокирует 100% автоматизированных ботов, 99% массовых фишинговых атак и 66% целевых атак.

Однако MFA не является панацеей. Опытные злоумышленники разработали техники обхода MFA. Фишинговые прокси реального времени перехватывают как пароль, так и код MFA, воспроизводя их на легитимном сайте до истечения срока действия кода. Социальная инженерия может обманом заставить пользователей подтвердить мошеннические запросы MFA. Подмена SIM-карты обходит MFA на основе SMS.

Реализация MFA имеет такое же значение, как и сам факт её внедрения. Организациям следует отдавать приоритет методам MFA, устойчивым к фишингу, таким как ключи безопасности FIDO2. Следует внедрять сопоставление номеров или отображение контекста для push-уведомлений с целью предотвращения атак на основе усталости от MFA. Необходимо обеспечить, чтобы MFA охватывала все пути доступа, включая VPN, облачные приложения и административные интерфейсы.

Часть 3: Беспарольная аутентификация

Беспарольная аутентификация полностью исключает пароли, как правило, заменяя их факторами владения (ключи безопасности или телефоны) и биометрическими факторами. Этот подход устраняет самое слабое звено в традиционной аутентификации, одновременно зачастую улучшая пользовательский опыт.

Движение к беспарольной аутентификации резко ускорилось с 2023 года. Microsoft сообщает, что более 90% их сотрудников используют беспарольную аутентификацию. Apple, Google и Microsoft реализовали поддержку ключей доступа (passkey) в своих операционных системах и браузерах. Согласно FIDO Alliance (Fast Identity Online, отраслевой альянс по стандартам аутентификации), доступность ключей доступа достигла критической массы в 2025 году, с поддержкой на всех основных платформах.

Преимущества беспарольной аутентификации существенны. Пользователи не могут выбрать слабый пароль, если паролей нет. Фишинг становится значительно сложнее, когда нет учётных данных для ввода. Затраты на службу поддержки значительно снижаются — сброс паролей является одной из крупнейших статей

расходов ИТ-поддержки. Пользовательский опыт улучшается, поскольку приложить палец к датчику отпечатков быстрее, чем набирать пароль.

Проблемы беспарольной аутентификации связаны с восстановлением доступа и пограничными случаями. Что происходит, когда пользователь теряет ключ безопасности или получает новый телефон? Как пользователи проходят аутентификацию с общих или публичных компьютеров? Организации, внедряющие беспарольную аутентификацию, должны тщательно проектировать процедуры восстановления, которые поддерживают безопасность и при этом остаются удобными.

Часть 4: FIDO2 и WebAuthn

FIDO2 (Fast Identity Online 2) — это технический стандарт, обеспечивающий современную беспарольную аутентификацию. Он состоит из двух компонентов: WebAuthn (Web Authentication API) — API веб-браузера, и CTAP2 (Client to Authenticator Protocol, что переводится как протокол взаимодействия клиента с аутентификатором) — протокола для взаимодействия с аутентификаторами, такими как ключи безопасности.

Позвольте объяснить, как работает FIDO2. При регистрации на сервисе с поддержкой FIDO2 ваш аутентификатор генерирует новую пару открытого и закрытого ключей, уникальную для данного сервиса. Закрытый ключ никогда не покидает аутентификатор — он хранится в защищённом аппаратном обеспечении. Открытый ключ отправляется сервису и сохраняется вместе с вашей учётной записью.

При входе в систему сервис отправляет запрос — случайное число. Ваш аутентификатор подписывает этот запрос закрытым ключом и возвращает подпись. Сервис проверяет подпись с помощью вашего открытого ключа. Если подпись действительна, вы аутентифицированы.

Безопасность FIDO2 обеспечивается несколькими свойствами. Во-первых, учётные данные уникальны для каждого сервиса — нет учётных данных, которые можно повторно использовать на других сайтах. Во-вторых, учётные данные привязаны к источнику легитимного сервиса — аутентификатор проверяет домен и не отвечает фишинговому сайту. В-третьих, закрытый ключ никогда не покидает аутентификатор — нечего красть при утечке данных сервера.

Аутентификаторы FIDO2 существуют в нескольких формах. Переносные аутентификаторы — это отдельные аппаратные устройства, такие как YubiKey, которые вы носите с собой. Платформенные аутентификаторы встроены в ваше устройство — Windows Hello, Touch ID, Face ID и биометрия Android функционируют как аутентификаторы FIDO2. Это означает, что большинство современных устройств уже поддерживают FIDO2 без дополнительного оборудования.

Часть 5: Ключи доступа (Passkeys)

Ключи доступа (passkeys) представляют собой потребительское развитие FIDO2. В то время как FIDO2 изначально был разработан для аппаратных ключей безопасности, ключи доступа делают ту же технологию доступной для всех через платформенные аутентификаторы и облачную синхронизацию.

Ключ доступа — это просто учётные данные FIDO2, которые могут синхронизироваться между вашими устройствами. Когда вы создаёте ключ доступа на iPhone, он сохраняется в iCloud Keychain и становится доступным на других устройствах Apple. Аналогично, Google Password Manager синхронизирует ключи доступа между устройствами Android и браузерами Chrome, а Microsoft синхронизирует ключи доступа между устройствами Windows.

Это решает проблему восстановления, которая ограничивала распространение FIDO2. С аппаратными ключами безопасности потеря ключа означала потерю доступа. С ключами доступа ваши учётные данные сохраняются при потере устройства, поскольку они резервируются в облако. Сама резервная копия защищена сквозным шифрованием, поэтому даже облачный провайдер не может получить доступ к вашим ключам.

Распространение ключей доступа было впечатляющим. В 2025 году крупные сервисы, включая Google, Microsoft, Apple, Amazon, PayPal и многие другие, поддерживают аутентификацию по ключам доступа. Согласно прогнозу Gartner, аналитической компании в сфере информационных технологий, ключи доступа станут доминирующим методом потребительской аутентификации к 2027 году, наконец воплощая в жизнь многолетнее обещание устранения паролей.

С точки зрения безопасности ключи доступа представляют собой значительное улучшение по сравнению с паролями. Они устойчивы к фишингу по своей конструкции. Они не могут быть слабыми или повторно используемыми. Они обеспечивают криптографическое подтверждение владения. Однако они создают новые соображения относительно безопасности облачной учётной записи — если ваша учётная запись Google скомпрометирована, ваши синхронизированные через Google ключи доступа могут оказаться под угрозой.

Часть 6: Единая точка входа и федеративная идентификация

Единая точка входа, или SSO (Single Sign-On), позволяет пользователям пройти аутентификацию один раз и получить доступ к нескольким приложениям без повторной аутентификации. Федеративная идентификация расширяет эту концепцию за пределы организационных границ, позволяя пользователям одной организации получать доступ к ресурсам другой.

SSO значительно улучшает пользовательский опыт и снижает распространение паролей. Вместо ведения отдельных учётных данных для каждого приложения пользователи поддерживают учётные данные у поставщика идентификации, или IdP (Identity Provider), и используют эти учётные данные повсюду. Это уменьшает количество паролей, которые пользователям необходимо запоминать, что снижает повторное использование паролей и выбор слабых паролей.

С точки зрения безопасности SSO концентрирует аутентификацию в одном месте. Это может быть полезно — вы можете реализовать надёжную аутентификацию один раз, и она будет защищать всё. Но это также создаёт высокоценную цель — скомпрометируйте IdP, и вы скомпрометируете всё. Системы SSO должны проектироваться и эксплуатироваться с соблюдением наивысших стандартов безопасности.

Основные корпоративные протоколы SSO — это Kerberos, SAML, OAuth 2.0 и OpenID Connect. Рассмотрим каждый из них.

Kerberos: рабочая лошадка предприятия

До эпохи веба **Kerberos** (Ке́рберос, разработанный в MIT, Massachusetts Institute of Technology, Массачусетский технологический институт) стал доминирующим стандартом для локальных сетей (on-premise), особенно в Microsoft Active Directory. Он полагается на доверенную третью сторону, называемую **Key Distribution Center** (KDC, Центр распределения ключей).

В потоке Kerberos пользователь входит в систему один раз в KDC и получает **Ticket Granting Ticket** (TGT, билет на получение билета). Когда он хочет получить доступ к конкретному ресурсу (например, файловому серверу или принтеру), он предъявляет TGT центру KDC для получения Сервисного Билета (Service Ticket). Этот билет разрешает доступ к конкретному ресурсу.

Что особенно важно, Kerberos обеспечивает **взаимную аутентификацию** — пользователь подтверждает свою личность серверу, а сервер подтверждает свою личность пользователю. Хотя Kerberos менее распространён в публичном вебе, он остаётся основой безопасности внутренних корпоративных сетей.

SAML: Security Assertion Markup Language

SAML (Security Assertion Markup Language, язык разметки утверждений безопасности), разработанный в начале 2000-х годов, является традиционным стандартом корпоративной единой точки входа. Он использует утверждения на основе XML (eXtensible Markup Language, расширяемый язык разметки) для передачи информации об аутентификации и атрибутах между поставщиком идентификации и поставщиком услуг.

В типичном потоке SAML, когда вы обращаетесь к приложению (поставщику услуг), оно перенаправляет вас к поставщику идентификации вашей организации.

Вы проходите аутентификацию у IdP, который создаёт утверждение SAML — подписанный XML-документ, содержащий вашу идентичность и атрибуты. Это утверждение отправляется обратно поставщику услуг, который проверяет подпись и предоставляет доступ.

SAML широко используется на предприятиях, с поддержкой всеми основными поставщиками идентификации (Azure AD от Microsoft, Okta и Ping Identity, компании-поставщики облачных решений управления идентификацией) и тысячами приложений. Однако SAML имеет ограничения. Протокол на основе XML сложен и многословен. Он был разработан для веб-браузеров и плохо работает для мобильных приложений или API. Он не обеспечивает нативную поддержку авторизации — SAML решает вопрос «кто вы», но не «что вы можете делать».

OAuth 2.0: фреймворк авторизации

OAuth 2.0, несмотря на то что подсказывает название, не является протоколом аутентификации — это фреймворк авторизации. OAuth отвечает на вопрос «Имеет ли это приложение разрешение на доступ к моим данным?», а не «Кто я?»

Классический сценарий использования OAuth — доступ третьей стороны. Когда вы используете «Войти через Google» для создания учётной записи в новом сервисе, вы предоставляете этому сервису разрешение на чтение информации вашего профиля Google. Google аутентифицирует вас, но сторонний сервис получает маркер доступа, а не ваши учётные данные. Сервис никогда не видит ваш пароль Google.

OAuth 2.0 определяет несколько типов грантов для различных сценариев. Грант кода авторизации используется для веб-приложений. Расширение PKCE (Proof Key for Code Exchange, ключ подтверждения для обмена кодом) добавляет безопасность для мобильных и одностраничных приложений. Грант клиентских учётных данных используется для межсервисного взаимодействия. Каждый тип гранта учитывает различные требования безопасности и модели угроз.

Ключевые понятия в OAuth — это токены. Маркеры доступа предъявляются API для подтверждения авторизации — они обычно имеют короткий срок действия (от минут до часов). Маркеры обновления используются для получения новых маркеров доступа — они имеют более длительный срок действия (от дней до месяцев) и должны храниться безопасно.

Недавние обновления, такие как **OAuth 2.1**, консолидируют лучшие практики, объявляя устаревшими небезопасные потоки (такие как Implicit Grant, неявное разрешение) и требуя использования PKCE для всех клиентов. Более того, для предотвращения кражи токенов индустрия движется к **DPoP** (Demonstrating Proof-of-Possession, демонстрация доказательства владения). В отличие от стандартных токенов Bearer (на предъявителя), которые подобны наличным деньгам (любой, у кого они есть, может их использовать), DPoP привязывает токен

к криптографическому ключу клиента. Если злоумышленник украдёт токен DPoP, но у него не будет закрытого ключа, токен будет бесполезен.

OpenID Connect: аутентификация поверх OAuth

OpenID Connect, сокращённо OIDC, добавляет уровень аутентификации поверх OAuth 2.0. В то время как OAuth сообщает, что пользователь авторизовал, OIDC сообщает, кто этот пользователь. Это делает OIDC подходящим для сценариев единой точки входа.

OIDC вводит идентификационный токен — JWT (JSON Web Token, веб-токен в формате JSON), содержащий утверждения об аутентифицированном пользователе: его идентификатор, имя, электронную почту и другие атрибуты. В отличие от маркеров доступа, которые непрозрачны для приложения, идентификационные токены предназначены для разбора и понимания.

Комбинация OAuth 2.0 и OIDC стала современным стандартом для управления идентификацией. OIDC обеспечивает аутентификацию и предоставляет информацию о пользователе. OAuth 2.0 обеспечивает авторизацию и предоставляет доступ к API. Вместе они обеспечивают полное решение для управления идентификацией, работающее в веб-, мобильных и API-приложениях.

OIDC в значительной степени заменил SAML для новых развёртываний благодаря более простому формату на основе JSON и лучшей поддержке архитектур современных приложений. Однако SAML остаётся прочно укоренившимся на предприятиях с унаследованными приложениями, поэтому понимание обоих протоколов является необходимым.

Часть 7: Архитектура нулевого доверия

Нулевое доверие (Zero Trust) — это модель безопасности, основанная на принципе «никогда не доверяй, всегда проверяй». В отличие от традиционной безопасности на основе периметра, которая предполагает, что всё внутри сети является доверенным, нулевое доверие предполагает наличие нарушения безопасности и проверяет каждый запрос, как если бы он исходил из ненадёжной сети.

Модель нулевого доверия была сформулирована Forrester Research, исследовательской компанией в сфере технологий, в 2010 году и приобрела известность после публикации Google своей реализации BeyondCorp в 2014 году. К 2025 году нулевое доверие стало доминирующей философией архитектуры безопасности, обусловленной внедрением облачных технологий, удалённой работой и всё более изощрёнными атаками.

Основные принципы нулевого доверия:

- Во-первых, явная проверка. Всегда аутентифицируйте и авторизуйте на основе всех доступных точек данных — идентичности, устройства, местоположения, сервиса, классификации данных, аномалий. Не предполагайте, что если кто-то прошёл аутентификацию утром, он по-прежнему является легитимным пользователем после обеда.
- Во-вторых, используйте доступ с минимальными привилегиями. Ограничивайте доступ с помощью подхода «точно в срок» и «ровно столько, сколько нужно». Применяйте адаптивные политики на основе рисков. Защищайте данные и системы с помощью микросегментации.
- В-третьих, предполагайте нарушение безопасности. Минимизируйте зону поражения и сегментируйте доступ. Обеспечивайте сквозное шифрование. Используйте аналитику для получения видимости, обнаружения угроз и улучшения защиты.

Реализация нулевого доверия требует возможностей в нескольких областях. Идентификация является основой — надёжная аутентификация, управление идентификацией и непрерывная проверка. Устройства должны быть известны и соответствовать требованиям — регистрация устройств, аттестация состояния и политики соответствия. Сети обеспечивают сегментацию и шифрование — микросегментация, зашифрованные коммуникации и защита от угроз. Приложения обеспечивают выполнение политик — управление доступом, безопасность облачного доступа и пограничный сервис безопасного доступа. Данные классифицируются и защищаются — классификация данных, шифрование и предотвращение утечки данных.

Нулевое доверие — это не продукт, который можно купить, а архитектурный подход, требующий изменений в людях, процессах и технологиях. Организации обычно внедряют нулевое доверие постепенно, начиная с идентификации и расширяясь на другие области со временем.

Часть 8: Непрерывное адаптивное доверие и непрерывная оценка доступа

Традиционная аутентификация — это проверка в определённый момент времени: как только пользователь аутентифицирован и получает токен, ему доверяют до истечения срока действия этого токена. Это создаёт окно уязвимости. Если устройство пользователя скомпрометировано или его учётная запись заблокирована, у него всё ещё может сохраняться доступ в течение нескольких часов.

Непрерывное адаптивное доверие (Continuous Adaptive Trust, CAT) решает эту проблему путём постоянной оценки профиля риска пользователя на протяжении всей сессии. Вместо бинарного решения «доверяем» или «не доверяем»

при входе, CAT динамически корректирует доступ на основе поведенческой биометрии, состояния устройства и контекстуальных сигналов.

Практической реализацией этой концепции является **непрерывная оценка доступа** (Continuous Access Evaluation, CAE). CAE, впервые реализованная Microsoft и ставшая открытым стандартом, позволяет поставщикам идентификации мгновенно отзывать маркеры доступа при наступлении критических событий. Например, если пароль пользователя был изменён, его учётная запись заблокирована или его местоположение внезапно сменилось на страну с высоким уровнем риска, поставщик идентификации отправляет сигнал поставщику услуг (например, Exchange Online или SharePoint) для немедленного отклонения активного токена пользователя и принудительной повторной аутентификации. Это фактически закрывает окно уязвимости долгоживущих маркеров доступа.

Часть 9: Управление привилегированным доступом (PAM)

Привилегированные учётные записи — администраторы, учётные записи root, сервисные учётные записи — обладают повышенным доступом, что делает их высокоценными целями. Управление привилегированным доступом, сокращённо PAM (Privileged Access Management), — это практика обеспечения безопасности, контроля и мониторинга привилегированного доступа.

Риски привилегированных учётных записей серьёзны. По данным Forrester, 80% нарушений безопасности связаны с привилегированными учётными данными. Скомпрометированная учётная запись администратора может обходить контроли безопасности, получать доступ к любым данным и скрывать следы. Внутренние угрозы от привилегированных пользователей особенно опасны, поскольку эти пользователи обладают знаниями и доступом для нанесения максимального ущерба.

Решения PAM обычно включают несколько компонентов:

- Хранилище привилегированных учётных данных, которое размещает административные учётные данные в зашифрованном хранилище, вместо того чтобы позволять администраторам знать фактические пароли. Когда администраторам нужен доступ, они получают учётные данные на ограниченное время. Хранилище может автоматически ротировать пароли после каждого использования.
- Управление сессиями, которе записывает и отслеживает привилегированные сессии. Каждая команда, которую вводит администратор, каждый экран, который он видит, регистрируется. Это обеспечивает криминалистические доказательства в случае инцидентов и сдерживает злоупотребления.

Продвинутые решения могут обнаруживать подозрительное поведение в реальном времени и прекращать сессии.

- Доступ точно в срок, который предоставляет повышенные привилегии только тогда, когда это необходимо, и только на столько, сколько это необходимо. Вместо постоянных прав администратора пользователи запрашивают повышенный доступ для конкретных задач. Запрос может потребовать согласования, а доступ автоматически истекает.
- Управление сервисными учётными записями, которое расширяет PAM на нечеловеческие идентичности. Сервисные учётные записи, ключи API и другие учётные данные приложений часто забываются после начального развёртывания. Решения PAM обнаруживают, помещают в хранилище и ротируют эти учётные данные.

Ведущие поставщики PAM включают CyberArk, BeyondTrust и Delinea, компании-разработчики решений кибербезопасности, а также Hashicorp Vault, платформу управления секретами. Облачные провайдеры также предлагают нативные возможности PAM — AWS Systems Manager Session Manager, Azure Privileged Identity Management и GCP Identity-Aware Proxy обеспечивают контроли привилегированного доступа.

Часть 10: Управление жизненным циклом учётных записей

Управление жизненным циклом учётных записей охватывает создание, изменение и удаление учётных записей пользователей на протяжении всего их существования. Это звучит обыденно, но ошибки в этом процессе создают значительные риски безопасности.

Стандартом для этой автоматизации является **SCIM** (System for Cross-domain Identity Management, система междоменного управления идентификацией), определённый в RFC 7644. SCIM предоставляет стандартизированный API для создания, обновления и удаления идентификационных данных пользователей в различных системах. Например, когда пользователь добавляется в HR-систему (такую как Workday, разработчик облачных HR-систем), SCIM автоматически создаёт (провижинит) его учётную запись в Azure AD, Slack и Salesforce, обеспечивая согласованность и скорость.

Жизненный цикл начинается с выделения ресурсов — создания учётных записей и предоставления начального доступа. В современных организациях выделение ресурсов должно быть автоматизировано на основе авторитетных данных отдела кадров. Когда сотрудника принимают на работу, его учётная запись должна создаваться автоматически с соответствующими членствами в группах и правами

доступа на основе его роли и подразделения. Этот процесс называется провижинингом (provisioning).

Модификация происходит на протяжении всей жизни учётной записи. Пользователи меняют роли, принимают на себя новые обязанности, присоединяются к новым проектам. Каждое изменение должно обновлять их права доступа. Именно здесь возникает проблема накопления привилегий — пользователи приобретают доступ для новых обязанностей, но редко теряют доступ для старых. Пользователь, проработавший в организации 20 лет и несколько раз сменивший роли, может накопить доступ, значительно превышающий то, что требует его текущая роль.

Проверки доступа или сертификация доступа — это периодические процессы, при которых руководители или владельцы ресурсов проверяют, кто имеет доступ, и подтверждают его обоснованность. Эти проверки часто являются требованиями соответствия, но они также важны с операционной точки зрения для выявления и удаления ненужного доступа. Современные решения по управлению идентификацией автоматизируют значительную часть этого процесса, предоставляя проверяющим контекст и рекомендации.

Отзыв ресурсов — отключение или удаление учётных записей при уходе пользователей — является критически важным процессом и часто выполняется неудовлетворительно. Согласно исследованиям Ponemon Institute, исследовательской организации в области безопасности, в средней организации существуют тысячи «осиротевших» учётных записей — учётных записей, принадлежащих бывшим сотрудникам, которые так и не были отключены. Эти учётные записи являются привлекательными целями для злоумышленников, поскольку за ними никто не следит.

Эффективный отзыв ресурсов требует интеграции между кадровыми системами и системой управления идентификацией. Когда сотрудник увольняется в кадровой системе, его учётные записи должны быть немедленно отключены. Для увольнений с высоким уровнем риска — пользователей с обширным доступом, пользователей, уходящих при негативных обстоятельствах — учётные записи должны быть отключены до того, как сотрудник будет даже уведомлён.

Часть 11: Управление и администрирование идентификации (IGA)

Управление и администрирование идентификации, сокращённо IGA (Identity Governance and Administration), охватывает политики, процессы и технологии для управления цифровыми идентичностями и их правами доступа. IGA выходит за рамки базового управления идентификацией и включает функции управления, такие как соответствие, управление рисками и обеспечение выполнения политик.

Ключевые возможности решений IGA включают:

- Управление жизненным циклом идентификации, которое мы только что обсудили. Это включает выделение ресурсов, модификации и отзыв ресурсов, в идеале автоматизированные и управляемые политиками.
- Процессы запроса и согласования доступа, которые позволяют пользователям запрашивать доступ через портал самообслуживания. Запросы направляются соответствующим согласующим лицам в зависимости от ресурса и заявителя. Это обеспечивает документированный и проверяемый процесс предоставления доступа.
- Сертификация доступа, которая автоматизирует процесс периодической проверки. Система генерирует кампании проверки, уведомляя руководителей о доступе, который необходимо проверить. Проверяющие могут одобрить, отозвать или отметить для расследования. Результаты документируются для целей соответствия.
- Обеспечение разделения обязанностей, которое предотвращает накопление пользователями опасных комбинаций доступа. Система может блокировать запросы, которые создали бы нарушения, или отмечать существующие нарушения для исправления.
- Управление ролями, которое помогает организациям определять, поддерживать и оптимизировать свою ролевую структуру. Это включает выявление ролей — анализ существующих паттернов доступа для определения потенциальных ролей — и проектирование ролей — разработку ролей на основе бизнес-требований.
- Отчётность и аналитика, которые обеспечивают видимость данных об идентификации и доступе. Информационные панели показывают метрики рисков доступа. Отчёты демонстрируют соответствие политикам и нормативным требованиям. Аналитика выявляет аномалии и возможности оптимизации.

Ведущие поставщики IGA включают SailPoint, Saviynt, Omada и One Identity, компании-разработчики решений управления идентификацией. Облачные провайдеры расширяют свои возможности управления идентификацией: Azure AD governance, AWS Identity Center и Google Cloud Identity добавляют функции управления.

Часть 12: Обнаружение и реагирование на угрозы идентификации (ITDR)

По мере того как организации усиливали защиту своих сетей и конечных точек, злоумышленники сместили фокус на саму инфраструктуру идентификации.

Обнаружение и реагирование на угрозы идентификации (Identity Threat Detection and Response, ITDR) — это относительно новая категория инструментов безопасности, специально разработанных для защиты систем идентификации, таких как Active Directory, Entra ID и платформы управления идентификацией и доступом (IAM, Identity and Access Management).

В то время как EDR (Endpoint Detection and Response, обнаружение и реагирование на конечных точках) защищает устройство, ITDR защищает учётные данные и системы, которые ими управляют. Решения ITDR выявляют специфические для идентификации атаки: попытки извлечения учётных данных из памяти, модификации групповых политик Active Directory, создание несанкционированных сервисных учётных записей или эксплуатацию уязвимостей в самом поставщике идентификации (например, атаку Golden SAML, при которой злоумышленники подделывают утверждения аутентификации SAML).

Надёжная стратегия ITDR включает непрерывную оценку состояния идентификации (выявление ошибок конфигурации или избыточных привилегий) и активный мониторинг атак на основе идентификации в реальном времени, устраняя разрыв между управлением идентификацией и операциями безопасности.

Часть 13: Перспективные тенденции в аутентификации

Позвольте завершить обсуждением перспективных тенденций, которые будут формировать аутентификацию в ближайшие годы.

Децентрализованная идентификация использует блокчейн и технологии распределённых реестров для предоставления пользователям контроля над своими идентификационными данными. Вместо того чтобы полагаться на централизованных поставщиков идентификации, пользователи хранят проверяемые удостоверения в цифровых кошельках. Они могут выборочно раскрывать атрибуты — например, доказать, что они старше 21 года, не раскрывая дату рождения. Хотя технология ещё находится в стадии развития, пилотные проекты децентрализованной идентификации реализуются в государственном и финансовом секторах.

Непрерывная аутентификация выходит за рамки разовой проверки к постоянному подтверждению идентичности на протяжении всей сессии. Используя поведенческую биометрию, сигналы устройства и контекстуальные факторы, системы могут обнаруживать, когда кто-то, отличный от аутентифицированного пользователя, может использовать сессию. Это решает проблему перехвата сессии и совместного использования учётных данных.

Адаптивная аутентификация динамически регулирует требования аутентификации на основе риска. Сценарии с низким уровнем риска могут требовать только пароль. Сценарии с более высоким уровнем риска — необычное местоположение, доступ к конфиденциальным данным, привилегированные операции — могут требовать дополнительных факторов или повышения уровня аутентификации. Это обеспечивает баланс между безопасностью и удобством для пользователя.

Управление машинными идентичностями решает проблему растущей популяции нечеловеческих идентичностей — сервисных учётных записей, API, ботов, устройств Интернета вещей и агентов ИИ. Эти идентичности часто превосходят по количеству человеческие идентичности и нередко забываются или плохо управляются. По мере того как организации внедряют больше автоматизации и ИИ, управление машинными идентичностями становится критически важным.

ИИ в аутентификации использует машинное обучение для улучшения как безопасности, так и пользовательского опыта. ИИ может обнаруживать аномалии, указывающие на скомпрометированные учётные записи, выявлять паттерны, свидетельствующие об атаках подстановкой учётных данных, и снижать количество ложных срабатываний в аутентификации на основе рисков. Однако ИИ также делает возможными новые атаки, включая дипфейковое аудио и видео для обмана биометрических систем.

Заключение

Аутентификация и управление учётными записями находятся в центре системы безопасности. Они определяют, кто может получить доступ к вашим системам и данным, и часто являются первой линией обороны от злоумышленников. Правильная реализация аутентификации является необходимым условием; ошибки в ней делают вас уязвимыми вне зависимости от того, какие другие контроли безопасности вы внедряете.

Сегодня мы рассмотрели обширный материал — от факторов аутентификации через современные протоколы до управления жизненным циклом учётных записей. Ключевые темы, которые следует запомнить: используйте множество факторов, отдавайте предпочтение методам, устойчивым к фишингу, применяйте принципы нулевого доверия, управляйте всем жизненным циклом идентификации и будьте в курсе развивающихся угроз и технологий.

На следующей лекции мы рассмотрим технологии сетевой безопасности — межсетевые экраны, VPN, обнаружение вторжений и многое другое. Мы увидим, как сетевая безопасность дополняет безопасность идентификации в стратегии эшелонированной защиты.

Вопросы для обсуждения

1. Будут ли пароли в конечном счёте полностью заменены беспарольной аутентификацией, и какие препятствия остаются?
2. Как модель нулевого доверия меняет роль аутентификации по сравнению с традиционной безопасностью на основе периметра?
3. Какие риски создаёт консолидация поставщиков идентификации и как организациям следует их снижать?

Благодарю за внимание. Увидимся в следующий раз.

Контрольные вопросы

1. Сравните и сопоставьте пять категорий факторов аутентификации. Каковы сильные и слабые стороны каждой из них?
2. Почему MFA на основе SMS считается менее безопасной, чем TOTP на основе приложений или аппаратные ключи безопасности?
3. Объясните, как FIDO2/WebAuthn обеспечивает устойчивость к фишингу.
4. В чём разница между OAuth 2.0 и OpenID Connect? Когда следует использовать каждый из них?
5. Опишите три основных принципа архитектуры нулевого доверия.
6. Что такое управление привилегированным доступом и почему оно важно?
7. Объясните концепцию сертификации доступа и её роль в управлении идентификацией.
8. Что такое ключи доступа (passkeys) и чем они отличаются от традиционных учётных данных FIDO2?
9. В чём разница между аутентификацией в определённый момент времени и непрерывной оценкой доступа (CAE)?

Ключевые термины

- **Управление жизненным циклом учётных записей**: процесс управления учётными записями пользователей от создания через модификацию до деактивации и удаления
- **Фактор аутентификации**: категория доказательств, используемых для проверки идентичности

- **CAE**: Continuous Access Evaluation, непрерывная оценка доступа — механизм мгновенного отзыва маркеров доступа при наступлении критических событий
- **CAT**: Continuous Adaptive Trust, непрерывное адаптивное доверие — динамическая корректировка доступа на основе профиля риска на протяжении всей сессии
- **Подстановка учётных данных**: автоматизированная атака с использованием украденных пар имя пользователя—пароль из утечек данных для получения несанкционированного доступа
- **CTAP2**: Client to Authenticator Protocol, часть FIDO2
- **Децентрализованная идентификация**: модель самосуверенной идентификации, в которой люди контролируют собственные учётные данные без зависимости от центрального органа
- **Федеративная идентификация**: идентификация, которая может использоваться за пределами организационных границ
- **FIDO2**: Fast Identity Online 2, современный стандарт беспарольной аутентификации
- **IGA**: управление и администрирование идентификации
- **ITDR**: обнаружение и реагирование на угрозы идентификации — возможности безопасности, направленные на обнаружение и реагирование на атаки, основанные на идентификации
- **MFA**: многофакторная аутентификация — аутентификация с использованием нескольких факторов из разных категорий
- **OAuth 2.0**: фреймворк авторизации для делегированного доступа
- **OIDC**: OpenID Connect, уровень аутентификации поверх OAuth
- **PAM**: управление привилегированным доступом
- **Passkey**: учётные данные FIDO2, синхронизируемые между устройствами
- **SAML**: Security Assertion Markup Language
- **SSO**: единая точка входа
- **TOTP**: одноразовый пароль на основе времени
- **WebAuthn**: Web Authentication API, часть FIDO2
- **Нулевое доверие (Zero Trust)**: модель безопасности, основанная на принципе «никогда не доверяй, всегда проверяй»