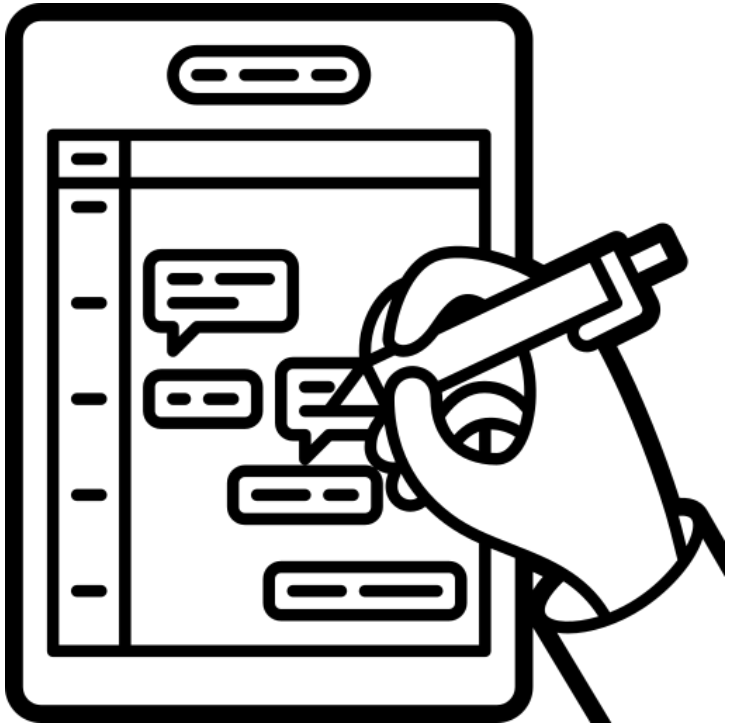
Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Идентификация, аутентификация и авторизация

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024



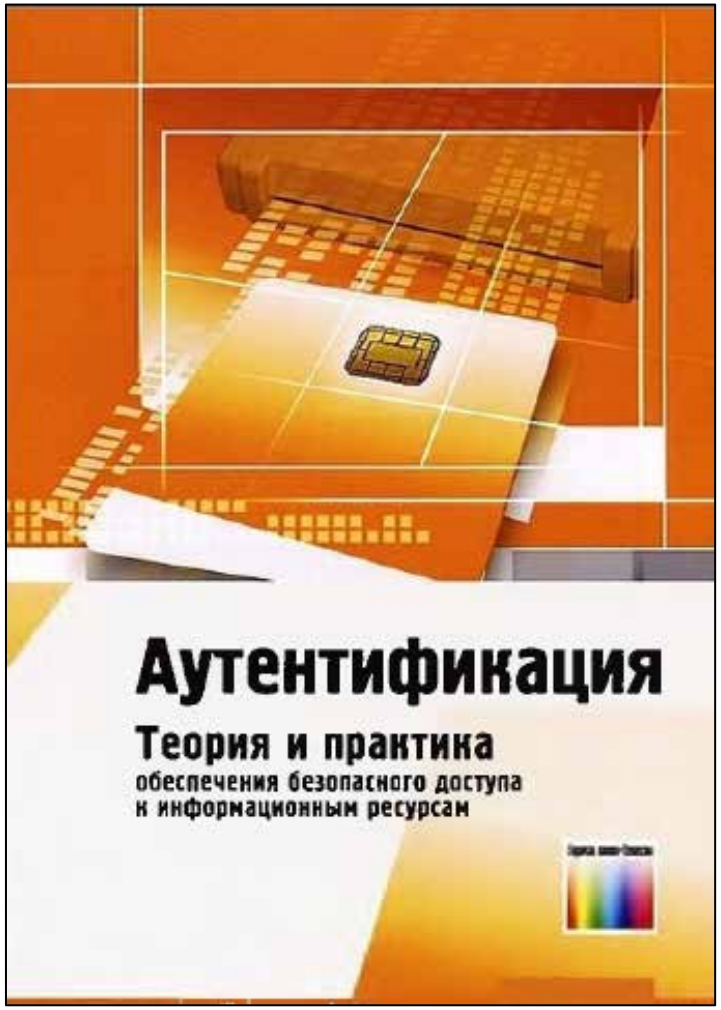
Защита от киберпреступников

Рекомендуемая литература по теме

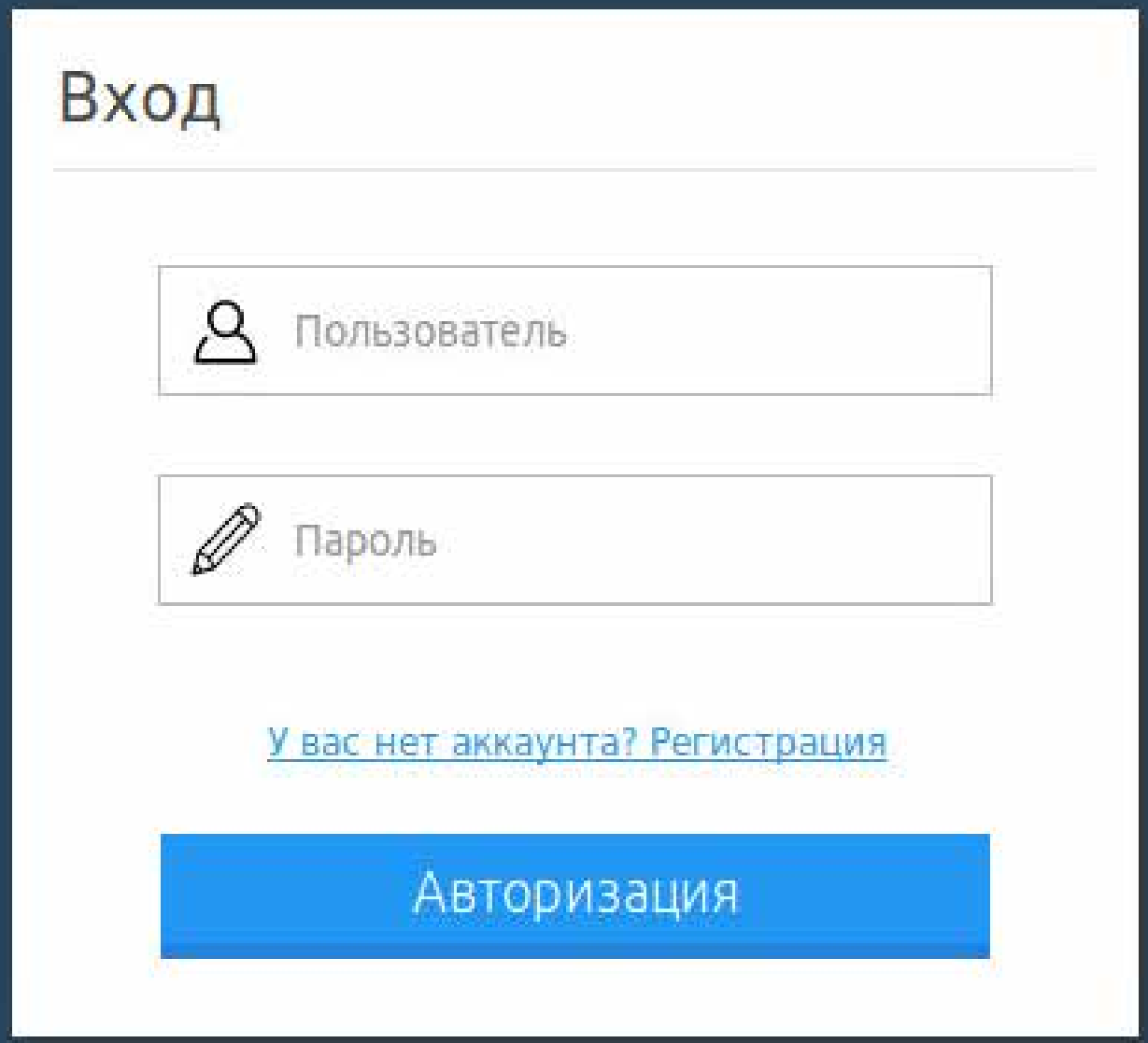
Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523

Пункт 5.3. Идентификация и аутентификация. стр.321 - 337

Рекомендуемая литература по теме



Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. — Москва: Горячая линия—Телеком, 2009. — 552 с.


Вход
Пользователь
Пароль
У вас нет аккаунта? Регистрация
Авторизация

Идентификация и аутентификация

- **При разработке любых мер безопасности, будь то конкретные механизмы или целые инфраструктуры, во главу угла ставятся идентификация и аутентификация.**

- Если вкратце, то **идентификация** делает предположение о том, чем или кем является что-то или кто-то, а **аутентификация** позволяет понять, истинно ли это утверждение. Эти процессы возникают в жизни постоянно и проявляются разными способами.

Основы идентификации и аутентификации

- Одной из важных задач обеспечения зашиты от несанкционированного доступа является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны.
- С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов.
- Эту информацию называют идентификатором субъекта.
- Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным.
- **Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.**

Идентификация

- **Идентификация** — это процедура распознавания пользователя по его идентификатору (имени).
- Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

- **Проверка личности** — это уже нечто большее, чем идентификация, но еще не аутентификация.

Аутентификация

- **Аутентификация** — процедура проверки подлинности заявленного пользователя, процесса или устройства.
- Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль).

- **Многофакторная аутентификация** — это использование одного или нескольких факторов при проверке подлинности заявленного пользователя, процесса или устройства. Когда используется два фактора, **эту методику иногда называют двухфакторной аутентификацией**.
- **Взаимная аутентификация** — это механизм аутентификации, в котором обе стороны в транзакции аутентифицируют друг друга.

Элементы аутентификации

- Независимо от типа системы аутентификации в ней всегда присутствуют **пять элементов**.
  1. **Первый элемент** — конкретный человек или процесс, который должен проходить аутентификацию, — субъект доступа.
  2. **Второй элемент** — опознавательный так, идентификатор, который выделяет этого человека или этот процесс среди других.
  3. **Третий элемент** — отличительная характеристика (аутентификатор), подтверждающая принадлежность идентификатора субъекту доступа.
  4. **Четвертый элемент** — владелец системы (администратор), который несет ответственность за использование системы, и в разграничении авторизованных пользователей и остальных полагается на механизм аутентификации.
  5. **Пятый элемент** — механизм аутентификации, который позволяет проверить присутствие отличительной характеристики.
- При успешном прохождении аутентификации субъекту доступа должны быть выданы некоторые права (привилегии).
- Для этого служит механизм управления доступом. С помощью этого же механизма субъект доступа лишается прав (привилегий), если аутентификация была неуспешной.

Идентификация, аутентификация и авторизация

- **Идентификация и аутентификация** являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу.
- После идентификации и аутентификации субъекта выполняется его **авторизация**.

Идентификация и Аутентификация

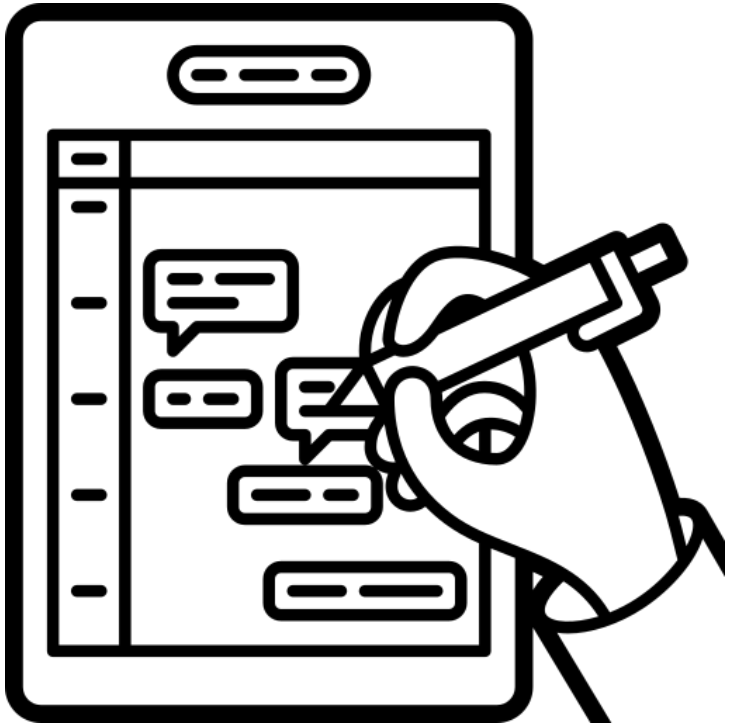
Идентификация

- Процедура распознавания субъекта/объекта доступа по его идентификатору

Аутентификация

- Процедура проверки подлинности субъекта или объекта доступа (подтверждение того, что субъект/объект доступ тот, за кого себя выдает)

Укрупненная классификация средств идентификации и аутентификации с точки зрения применяемых технологий



Идентификация

Идентификация

- **Идентифицировать человека или объект можно при помощи**:
  - Электронных ключей Touch Memory
  - RFID меток
  - NFC
  - Карт с магнитной полосой
  - Штрих-кодов
  - QR-кодов
  - Биометрии
  - и др.

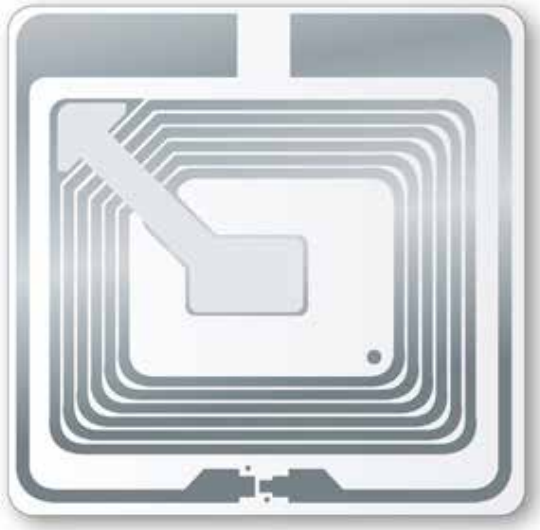
Электронные ключи Touch Memory

- **Электронные ключи Touch Memory** – одна из разновидностей электронных идентификаторов, широко применяемых во всем мире. По внешнему виду данный тип электронного ключа напоминает плоскую батарейку, толстую пуговицу или таблетку.

- Второе название электронных ключей данного семейства – ключи iButton, что означает Information Button (**“таблетка” с информацией**). Данное название пришло на смену Touch Memory в начале 1997 года. Под этим названием электронные ключи Touch Memory выпускаются по сегодняшний день.

RFID **метки**

- **Технология RFID (Radio Frequency Identification — радиочастотная идентификация)** – это технология, основанная на использовании радиочастотного электромагнитного излучения.



- **RFID-метка** – миниатюрное запоминающее устройство, которое состоит из микрочипа, хранящего информацию, и антенны, с помощью которой метка эти данные передает и получает.
- В памяти RFID-метки хранится ее собственный уникальный номер и пользовательская информация. Когда метка попадает в зону регистрации, эта информация принимается считывателем, специальным прибором, способным читать и записывать информацию в метках.

RFID **метки**

Внешний вид RFID-меток

для пластиковых контейнеров и возвратной тары; EPC Class1 Gen2 и ISO 18000-6C; Confidex

ключ для домофона; ISO 14443A

ушная клипса для животных; ISO 11784/11785

браслет; ISO10536/14443/15693

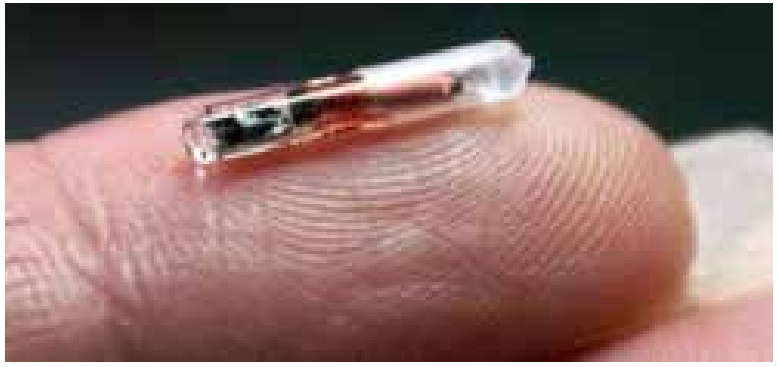
для прачечных производств, медицинских учреждений для автоматизированного учета и сортировки изделий из ткани, постельного белья, одежды; ISO 18000-3; HID

для дорогостоящих товаров; ISO 15693/18000-3; HID

на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex

Объем рынка RFID решений идентификации

RFID **чипы**



В 2015 году шведской фирме Epicenter посчитали карты-пропуски вчерашним днем, и решили вместо них вживить своим сотрудникам небольшой RFID чип непосредственно в руку.
Эти чипы заменяют пропуска, позволяя открывать двери офиса и использовать копировальные аппараты, просто поднося руку к детектору.

RFID **чипы**


POWER
OK
MODE


POWER
OK
MODE
AD2000-M
1 2 3
4 5 6
7
DOOR BELL


POWER
OK
MODE
AD2000-M
1 2 3
4 5 6
7 8 9
* 0 #
DOOR BELL
RFID ACCESS CONTROL

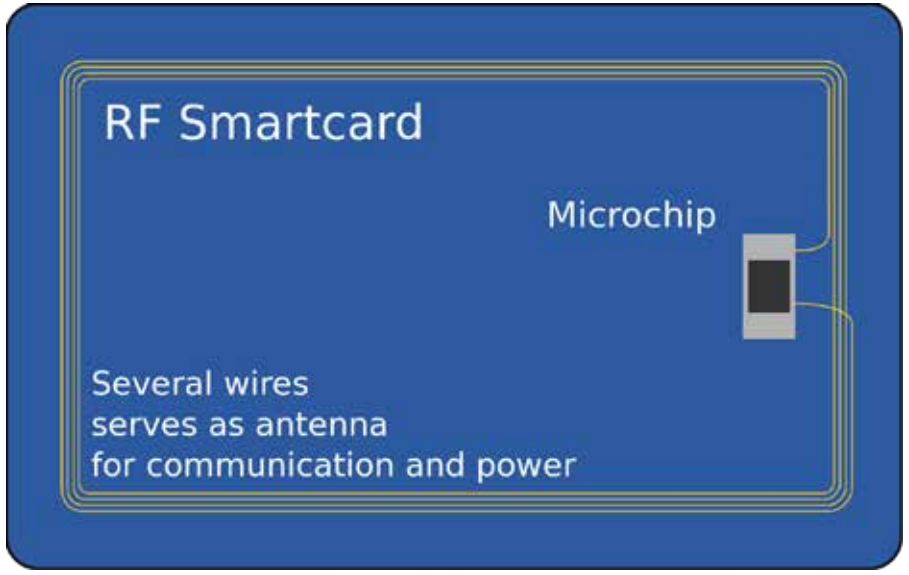
NFC

- **NFC (Near Field Communication)** — технология беспроводной высокочастотной связи малого радиуса действия (до 10 см), позволяющая осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях.

- **Технология NFC базируется на RFID** (Radio Frequency IDentification, радиочастотная идентификация).
- Три наиболее популярных варианта использования NFC технологии в мобильных телефонах:
  - **эмуляция карт** — телефон эмулирует карту, например пропуск или платежную карту;
  - **режим считывания** — телефон считывает пассивную метку (Tag), например для интерактивной рекламы;
  - **режим P2P** — два телефона связываются и обмениваются информацией

MIFARE

- **MIFARE** – одна из самых перспективных технологий для идентификации, часто ее можно встретить в системах управления доступом, проездных документах, визах и даже загранпаспортах.
- Mifare - торговая марка самой распространенной в России бесконтактной технологии смарт-карт принадлежащая Нидерландской компании NXP Semiconductors, компания NXP Semiconductors принадлежит Philips Austria GmbH.



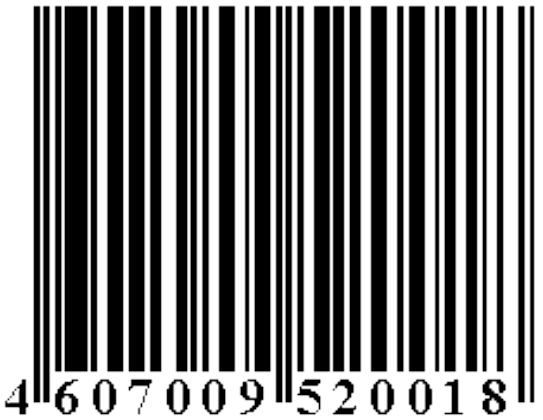
MIFARE

Карты с магнитной полосой

- **Карты с магнитной полосой.** В данном типе карты информация заносится на магнитную полосу. Карты с магнитной полосой бывают трёх форматов: ID-1, ID-2, ID-3. Магнитная полоса содержит 3 дорожки, на которые в закодированном виде записывают номер карты, срок ее действия, фамилию держателя карты и тому подобные данные. Объем записанной информации около 100 байт.

Штрих-код и QR-код

- **Штрих-код** — это наносимая в виде штрихов закодированная информация, считываемая при помощи специальных устройств. С помощью штрихового кода кодируют информацию о некоторых наиболее существенных параметрах объекта.



- **QR-код** (англ. quick response - быстрый отклик) – двумерный штрихкод, разработанный в 1994 году японской фирмой Denso-Wave. В нём кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы).

Биометрия

- **Биометрия** - это идентификация человека по уникальным биологическим признакам.
- **Методы биометрической идентификации делятся на две группы:**
  - **Статические методы** - основываются на уникальной физиологической (статической) характеристике человека, данной ему от рождения и неотъемлемой от него. (по отпечатку пальца; по форме ладони; по расположению вен на лицевой стороне ладони; по радужной оболочке глаза, по форме лица, по термограмме лица, по зубам, по ДНК и по многим другим параметрам)
  - **Динамические методы** - основываются на поведенческой (динамической) характеристике человека, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия. (по походке, по рукописному подчерку, по голосу и многим другим факторам)

Прогноз среднегодовых темпов роста глобального рынка биометрии (CAGR)

Объем глобального рынка биометрии

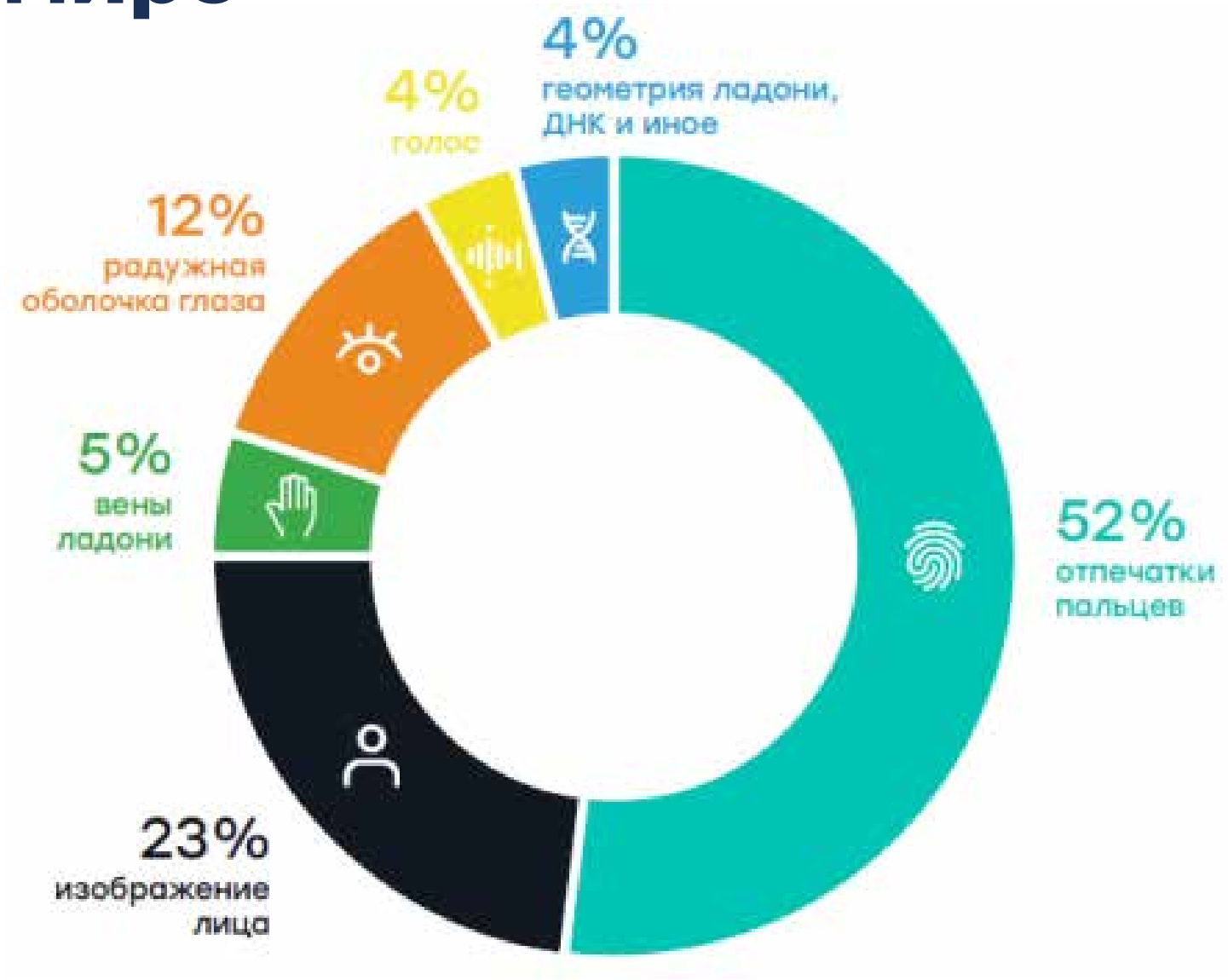
$14,45 МЛРД
в декабре 2020 года

$40,2 МЛРД
в декабре 2022 года

по данным
J'son & Partners

Популярность различных биометрических модальностей в мире

С начала 2020 года во всем мире гипер-востребованы бесконтактные биометрические технологии идентификации по лицу (в том числе, по лицу в маске) и по венам ладони, а также комплексные системы идентификации с термометрией.



Видеосюжет «Идентификация по венам ладони»

Видеосюжет «Идентификация по венам ладони»
https://www.youtube.com/watch?v=2PfGGGU41XE&t=155s

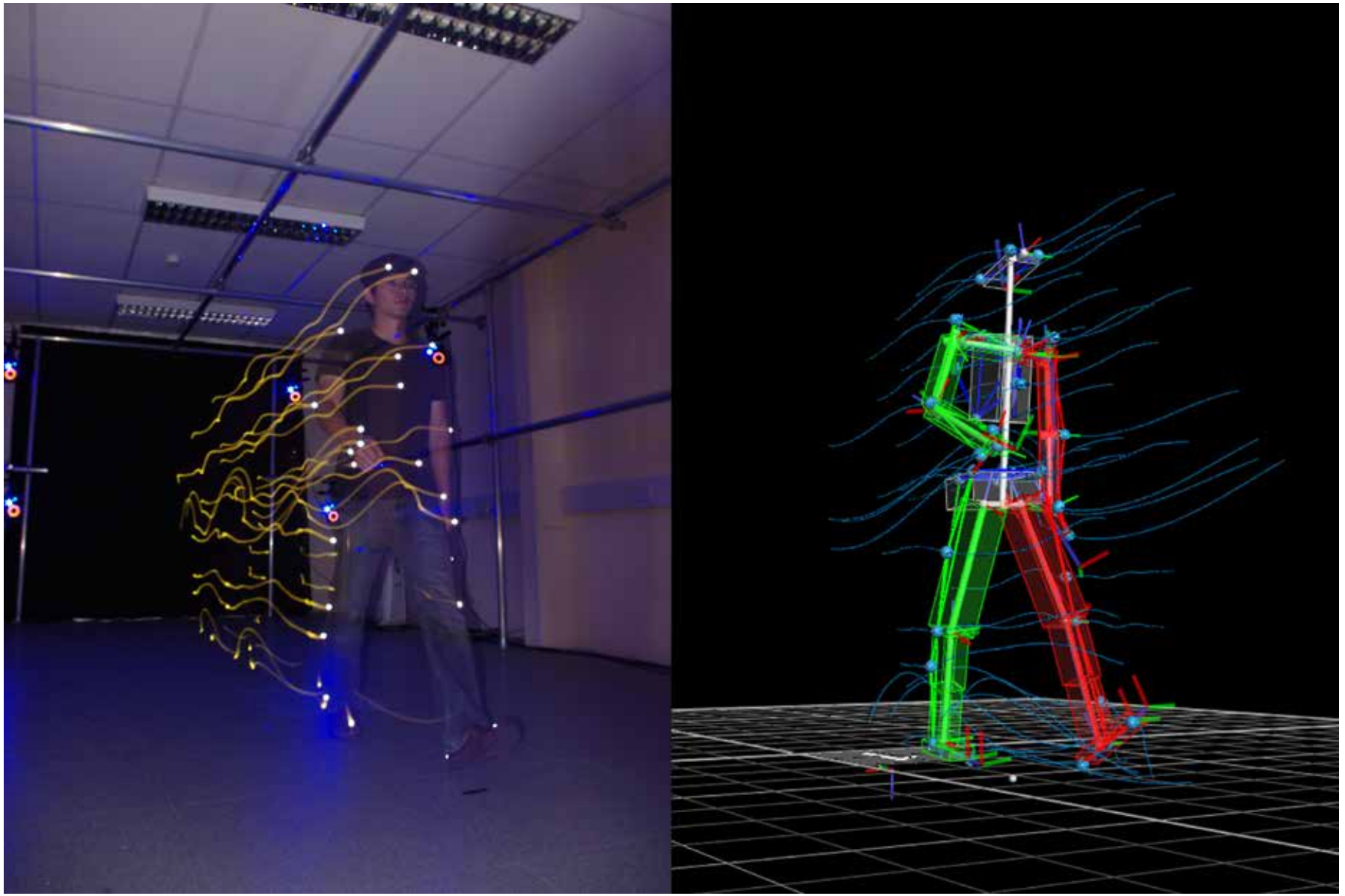
Биометрия

Прозрачная жизнь
https://www.youtube.com/watch?v=jJnOkB_s21Y

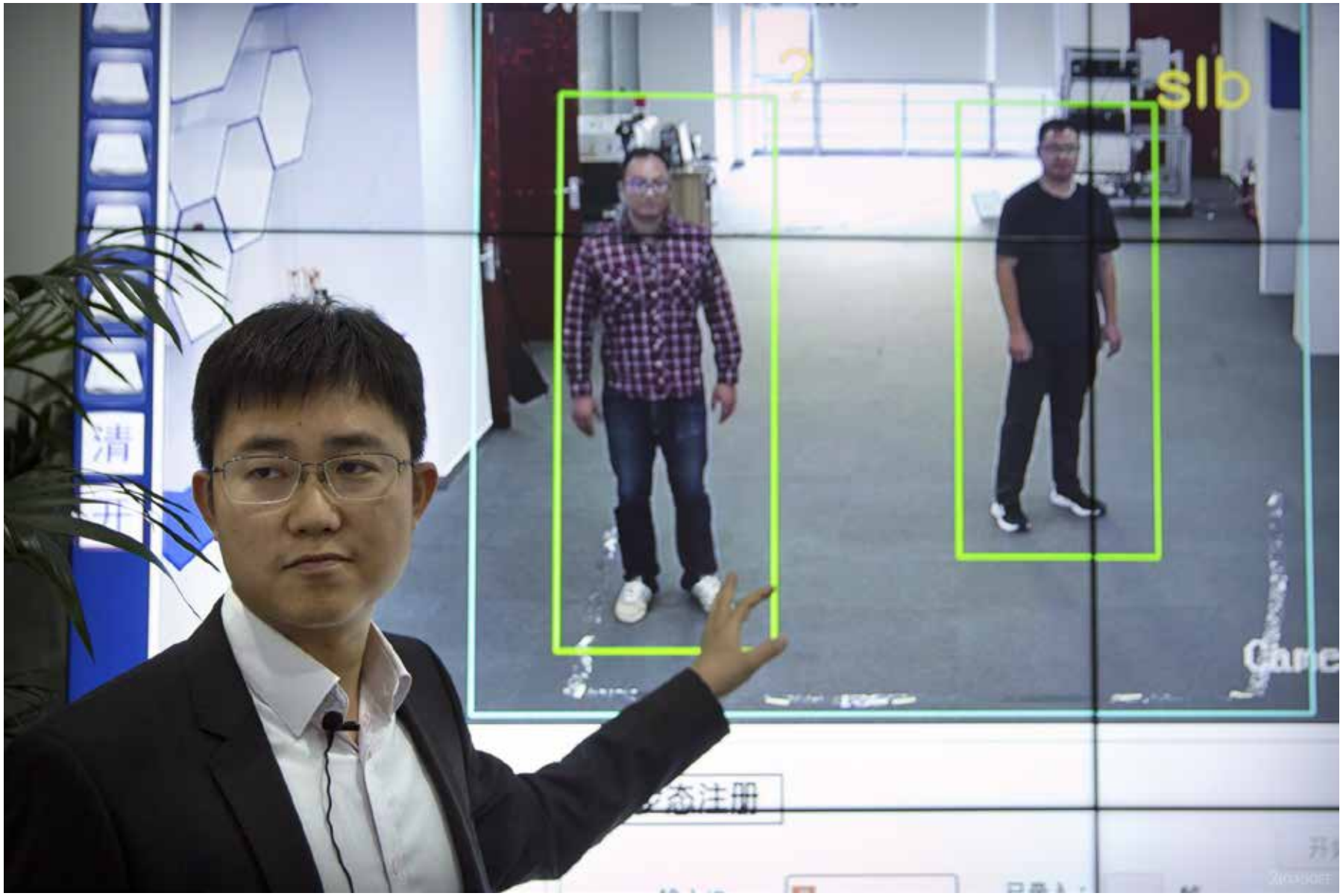
Биометрия

Крупнейшую систему слежения за людьми разрабатывают в КНР (новости)
https://www.youtube.com/watch?v=37OyuSDIdWE

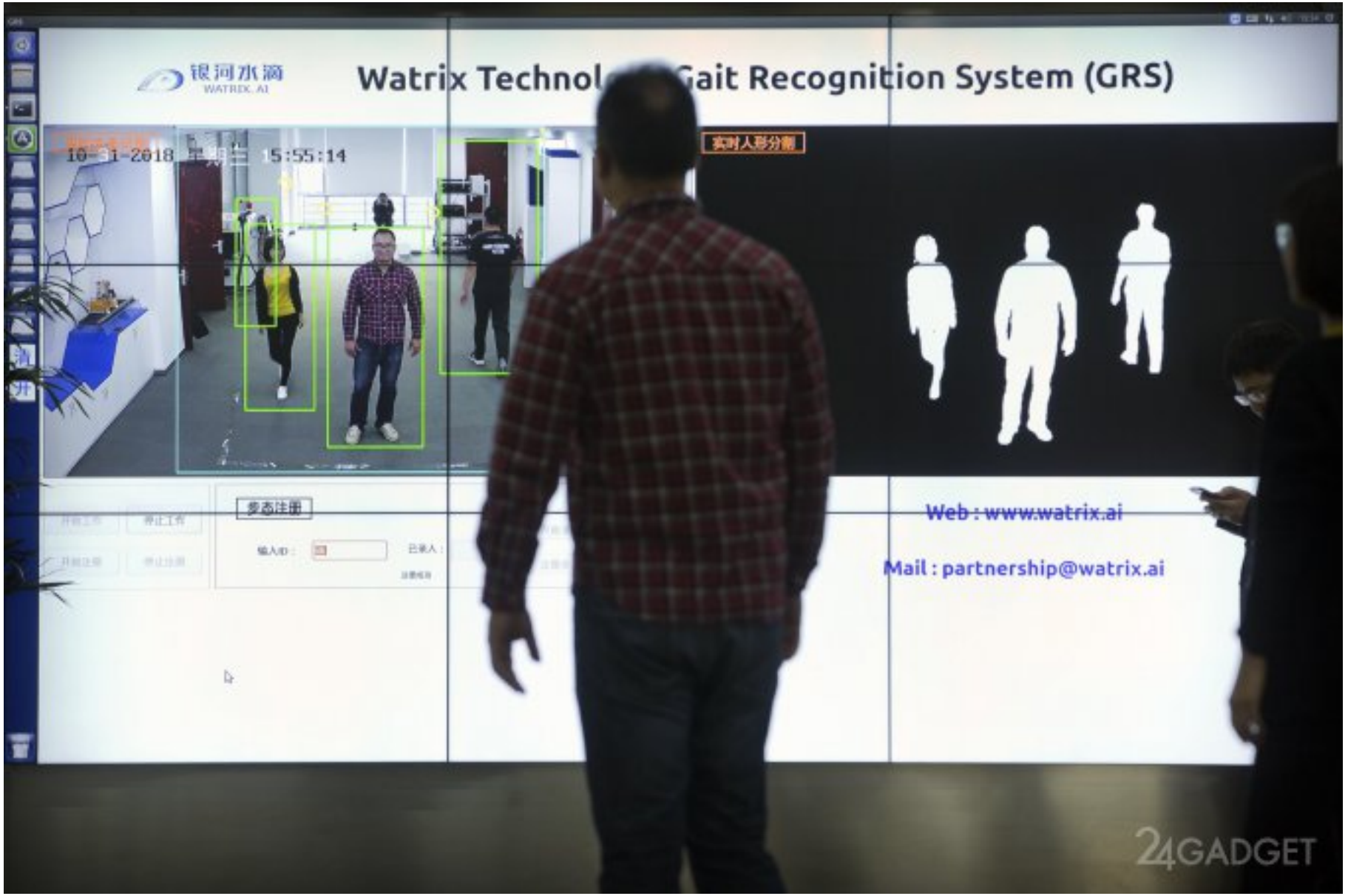
Идентификация человека по походке



Идентификация человека по походке



Идентификация человека по походке



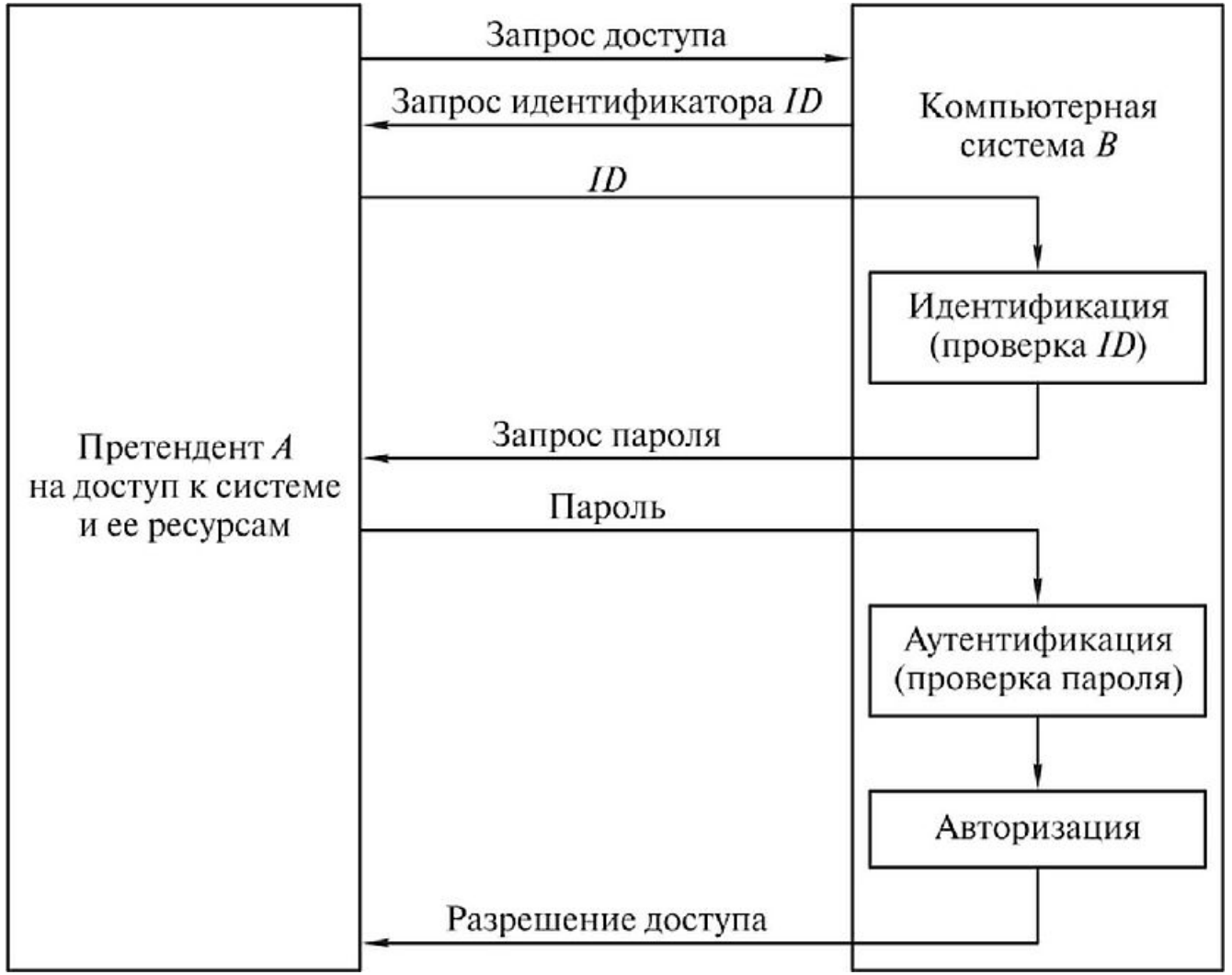
Идентификация человека по походке

Биометрия. YouTube

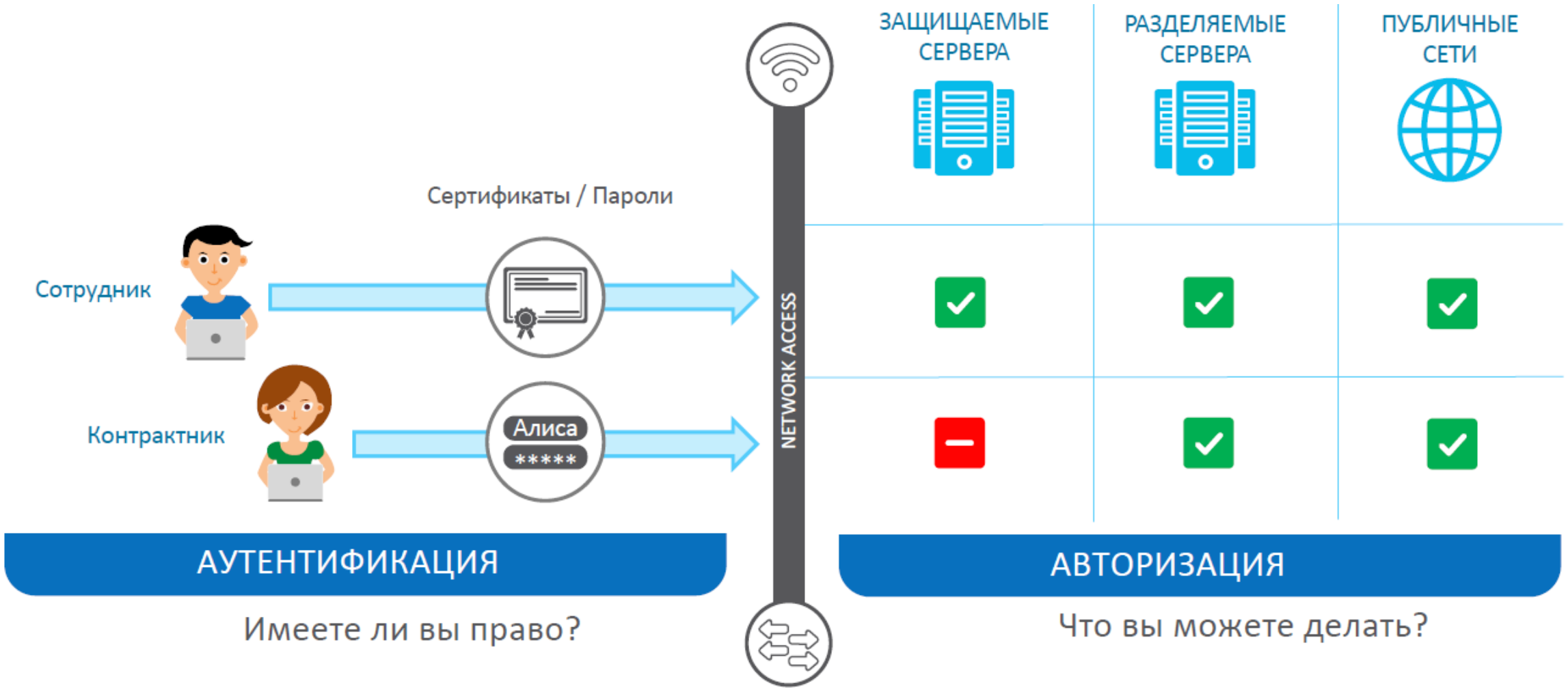
- Минск. Посмотрел и оплатил. Как работает новая система в метро и когда ее запустят (2020)
https://www.youtube.com/watch?v=241m89ne1SA
- Минск. Проезд в Минском метрополитене теперь можно оплатить с помощью технологии распознавания лиц (2021)
https://www.youtube.com/watch?v=YiVFBeG6Uvc
- Беларусь. Биометрические паспорта, фото-, видеоконтроль как норма жизни. (2021)
https://www.youtube.com/watch?v=FwklE3Bf6MQ
- Россия. Купить товар лицом: как биометрия меняет жизнь россиян – Россия 24 (2021)
https://www.youtube.com/watch?v=9ZoMwgy6xeE
- Москва. Они следят за всеми: умные камеры доказали свою успешность в борьбе с преступностью - Россия 24 (2020)
https://www.youtube.com/watch?v=2J23LNlWszo
- В Москве состоялась презентация системы «Безопасный город» (2016)
https://www.youtube.com/watch?v=D8OcXCe_w7w
- Камеры с распознаванием лиц. Как работает система слежки в России | Медиазона (2021)
https://www.youtube.com/watch?v=Cu2J8XKtaZw
- Все нейронные сети в видеонаблюдении, которые реально используются на практике для безопасности и.. (2020)
https://www.youtube.com/watch?v=S0C_u74cz-w
- Биометрия везде (2020)
https://www.youtube.com/watch?v=SaUvkLISSbQ
- Биометрия: возможности и преимущества - НТВ (2021)
https://www.youtube.com/watch?v=css69XkvNf8

Аутентификация

Пример процесса идентификации и аутентификации



Аутентификация и авторизация



Авторизация (authorization)

- **Авторизация** — процедура предоставления субъекту определенных полномочий и ресурсов в данной системе.
- **Авторизация** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

- Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы.
- Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены.

Идентификация, Аутентификация и Авторизация

- **Не всегда аутентификация связана с паролями**, но как правило
  - Представление своих персональных данных на этапе регистрации (идентификация)
  - Представление своего e-mail на этапе захода на вебинар (идентификация)
  - Проверка наличия введенного e-mail (аутентификация)
  - Предоставление доступа на вебинар (авторизация)

Администрирование

- **С процедурами идентификации и авторизации тесно связана процедура администрирования действий пользователя**.
- **Администрирование** — это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам.
- Хотя эта учетная информация может быть использована для выписывания счета, с позиций безопасности она особенно важна для обнаружения, анализа инцидентов безопасности в сети и соответствующего реагирования на них.
- Записи в системном журнале, аудиторские проверки и администрирование ПО — все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

Аутентификация. Подтверждение подлинности

- **Для подтверждения своей подлинности субъект может предъявлять системе разные сущности.**
- В зависимости от предъявляемых субъектом сущностей **процессы аутентификации могут быть разделены на** следующие **категории**:
  1. **На основе знания чего-либо.** Примерами могут служить пароль, персональный идентификационный код (P/N), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос-ответ.
  2. **На основе обладания чем-либо.** Обычно это магнитные карты, смарт-карты, сертификаты и устройства touch memory.
  3. **На основе каких-либо неотъемлемых характеристик.** Эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др.) В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике.

Технологии аутентификации

- **Технологии аутентификации**
  - **Однофакторная аутентификация** – аутентификация с одним фактором, чаще всего логин/пароль
  - **Двухфакторная аутентификация** – аутентификация с двумя фактором
  - **Многофакторная аутентификация** – в процессе которой используются аутентификационные факторы нескольких типов (более 2-х).

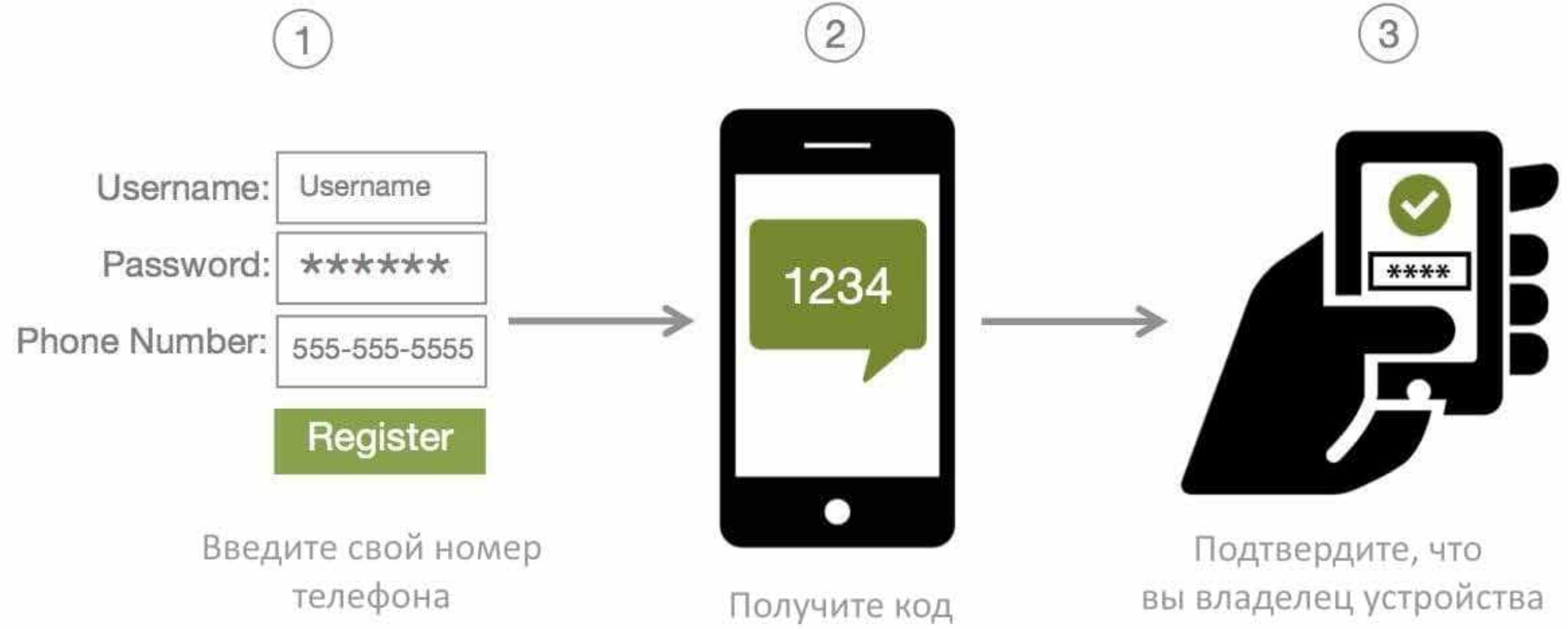
Технологии аутентификации
Двухфакторная аутентификация

- **Двухфакторная аутентификация** — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта.
- **На практике это обычно выглядит так**: **первый рубеж** — это логин и пароль, **второй** — специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя.
- *В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.*

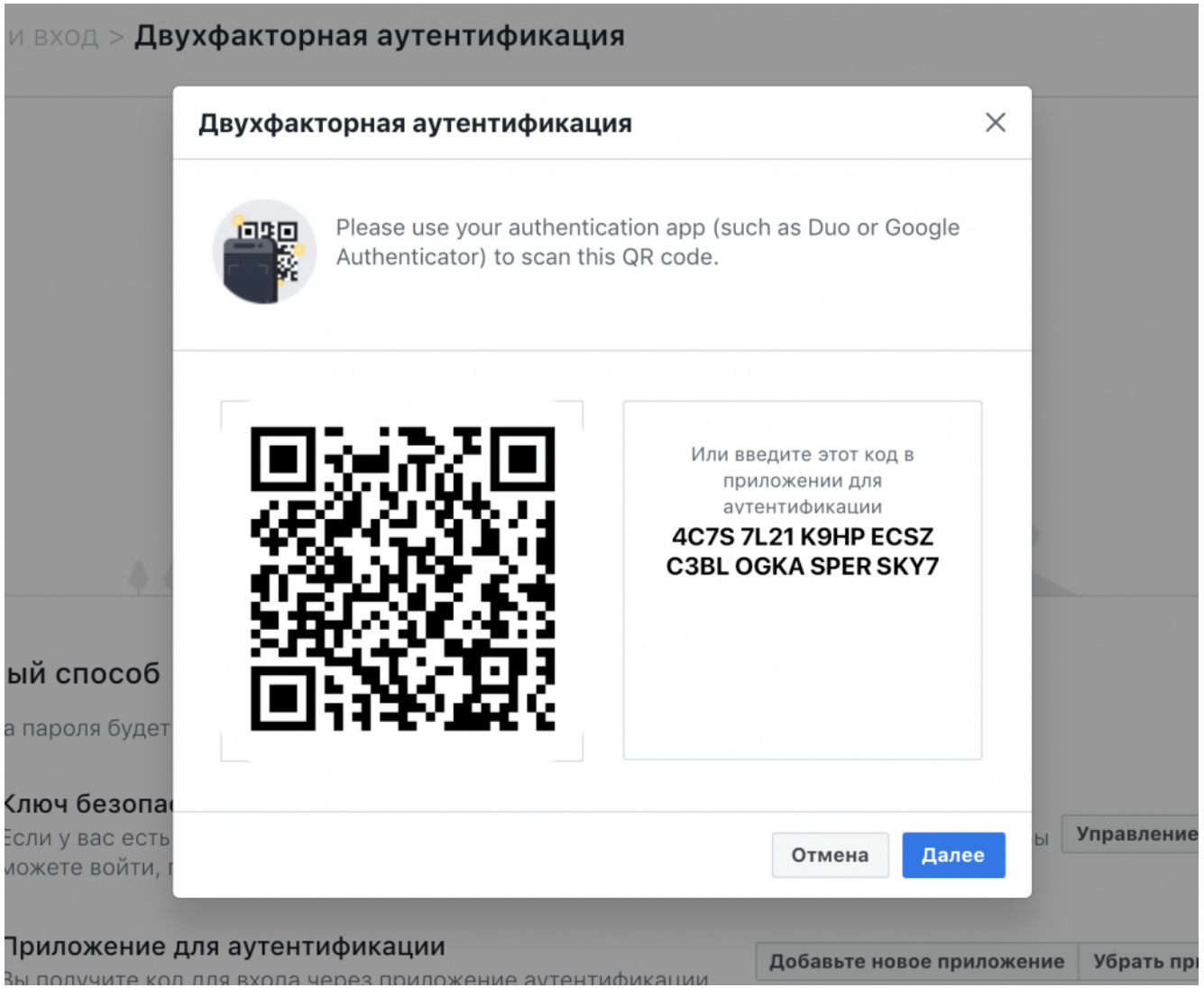
Технологии аутентификации
Двухфакторная аутентификация

- Пример двухфакторной аутентификации, как это сделано в Telegram/Viber/WhatsApp.
- А именно реализуются следующие шаги:
  - Пользователь вводит свой номер телефона и ему на телефон приходит СМС с кодом.
  - Пользователь вводит код из СМС и приложение его аутентифицирует и авторизует.
  - Пользователь открывает приложение повторно, и он уже аутентифицирован и авторизован.

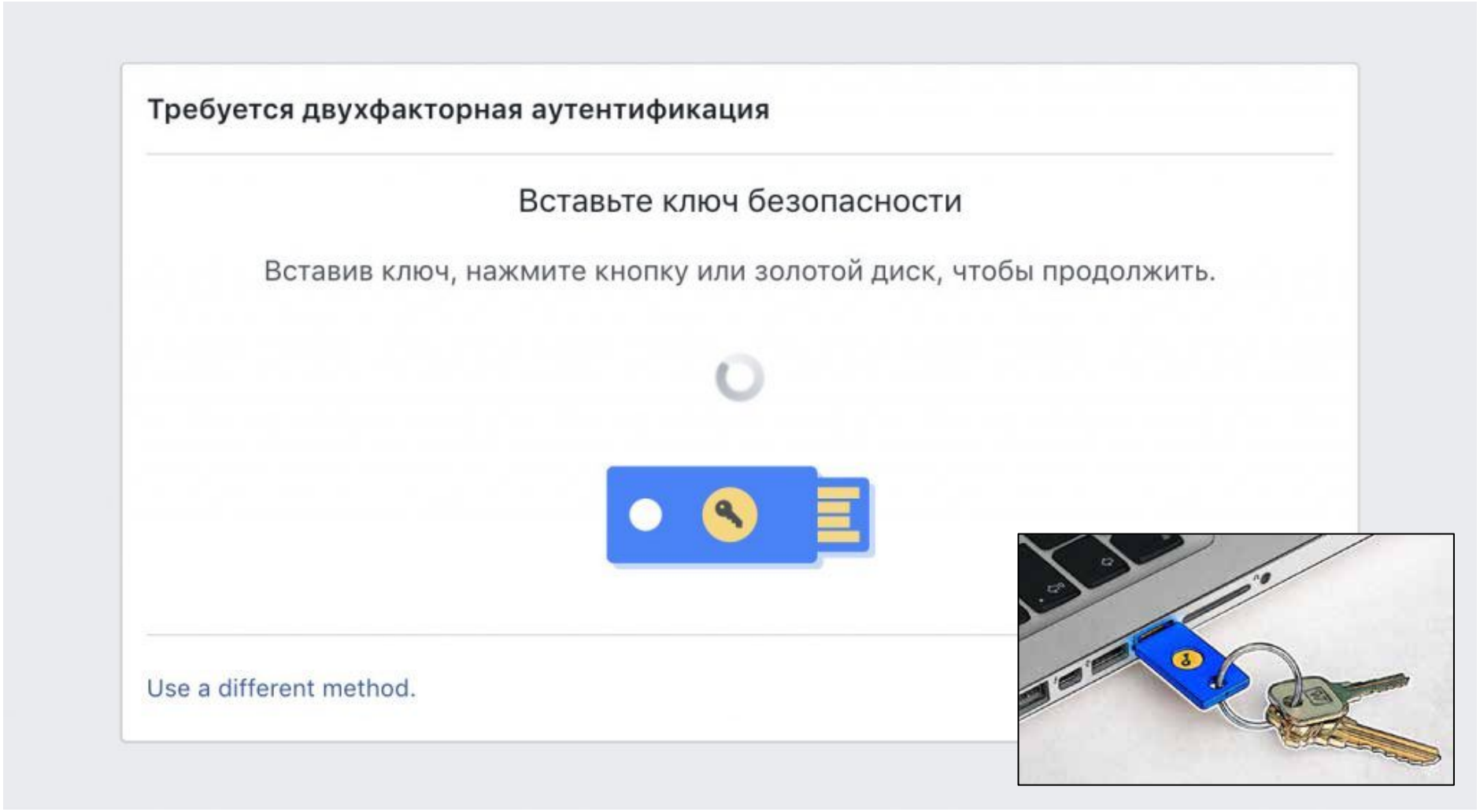
Технологии аутентификации
Двухфакторная аутентификация



Технологии аутентификации
Двухфакторная аутентификация



Технологии аутентификации
Двухфакторная аутентификация



Аутентификация

- **Процессы аутентификации укрупненно можно разделить на следующие типы**:
  1) аутентификация, использующая пароли и PIN-коды;
  2) строгая аутентификация на основе использования криптографических методов и средств;
  3) биометрическая аутентификация пользователей.
- С точки зрения безопасности, каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Классификация протоколов аутентификации

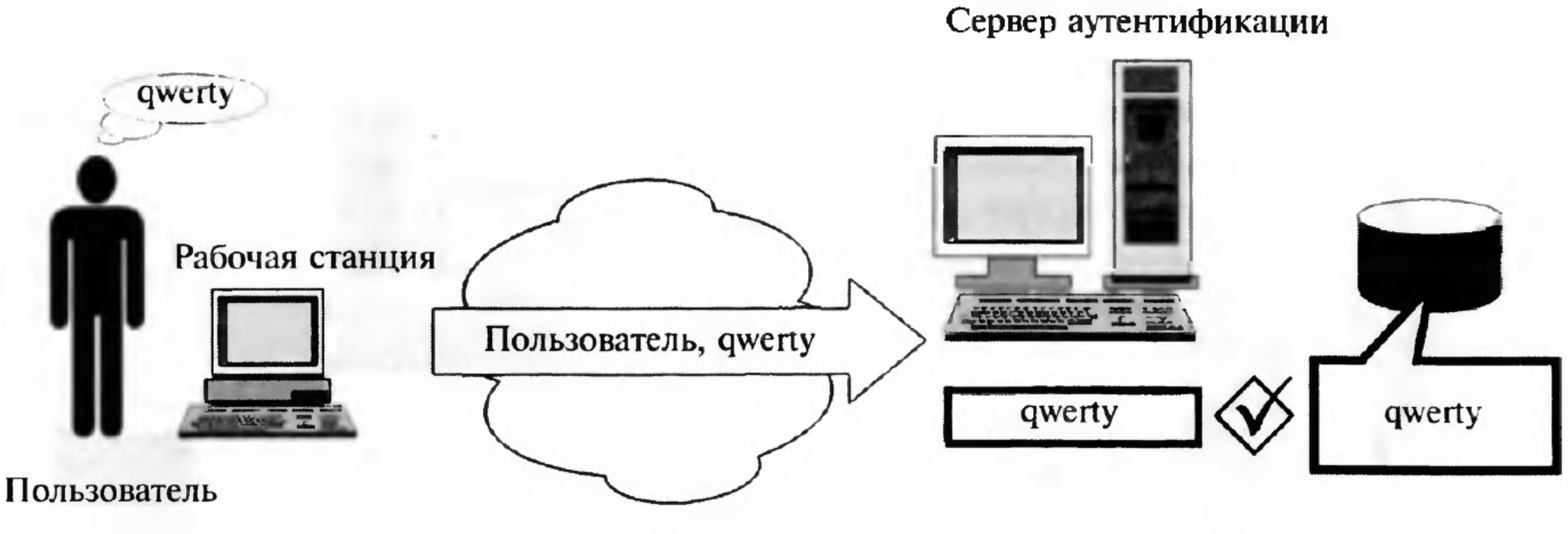
Классификация протоколов аутентификации

Аутентификация на основании паролей

Пароль

- **Пароль** — это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.
- **Персональный идентификационный код PIN** является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN -кода должно быть известно только держателю карты.
- **Динамический (одноразовый) пароль** — это пароль, который после одноразового применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

Аутентификация на основе открытого пароля



Имя пользователя и пароль передаются по сети в открытом виде

Аутентификация на основе хэшированного пароля

Однонаправленные хэш-функции не позволяют восстановить исходную информацию. Поэтому, если посторонний человек получит доступ к базе данных аутентификации, он не сможет восстановить пароль из хранящегося в базе хэш-значения.

Аутентификация на основе хэшированного пароля

- В большинстве используемого в настоящее время программного обеспечения применяются пароли не в чистом виде, а их хэш-значения, получаемые с помощью вычисления криптографической хэш-функции.
- **Однонаправленные хэш-функции (хэш-функции)** — это функции, которые принимают на входе строку переменной длины и преобразуют ее в выходную строку фиксированной (обычно меньшей) длины, называемую значением хэш-функции (хэш-значением).
- Пример прохождения пользователем процедуры аутентификации на основе хэшированного пароля:

  1. Пользователь вводит свои имя «Пользователь», и пароль «qwerty» на рабочей станции.

  2. Рабочая станция вычисляет хэш-значение N4a#@JD от введенного пароля. Имя пользователя и хэш-значение передаются по сети серверу аутентификации.

  3. Сервер аутентификаци сравнивает результат вычисления хэш-значения (N4a#@JD) от введенного пользователем пароля с хэш-значением, хранящимся в учетной записи пользователя (N4a#@JD).

  4. В случае совпадения аутентификация признается успешной

- Однонаправленные хэш-функции не позволяют восстановить исходную информацию. Поэтому, если посторонний человек получит доступ к базе данных аутентификации, он не сможет восстановить пароль из хранящегося в базе хэш-значения.

Пример парольной идентификации и авторизации в Российской Федерации через портал ГосУслуги

Постановление Правительства РФ от 10 ноября 2020 года №1802
https://storage.strategy24.ru/files/news/202011/c431626e0008bd36853565e665288e07.pdf

Аутентификация на основе PIN-кода

- **PIN-код (Personal Identification Number)** — это разновидность пароля, обычно используемого для аутентификации на локальном устройстве.
- Несмотря на слова identification (идентификационное) и number (число), послужившие основой для аббревиатуры, PIN-код редко служит в качестве идентификатора пользователя, а символы, входящие в PIN-код, необязательно являются цифрами. В торговых автоматах и банкоматах применяется карта с магнитной полосой или смарт-карта. PIN-коды часто используются с другими видами устройств аутентификации, например смарт-картами.
- Обычно PIN-код торгового автомата или банкомата состоит из четырех цифр. Таким образом, один из каждых 10000 клиентов имеют один и тот же PIN-код PIN-код похож на простой «пароль».

Аутентификация на основе PIN-кода

- Разница между PIN-кодом и паролем состоит в области и условиях их использования.
- Обычно для решений, в которых используется PIN-код, характерно следующее:
  - в локальном устройстве, в котором осуществляется аутентификация с помощью PIN-кода, имеется интерфейс для пользователя, а не для программ. Никто не может ввести PIN-код, не используя клавиатуру данного устройства.
  - PIN-код не передается по сети и не может быть перехвачен.

- Иногда термин PIN-код используют неправильно, применяя его для обозначения коротких и простых паролей. Между этими терминами есть функциональная разница

Парольные политики

- В связи с тем что парольная аутентификация основана на запоминании некоторой информации, многие пользователи информационных систем с парольной аутентификацией выбирают в качестве секрета не произвольную и трудно угадываемую информацию, а легко запоминаемые выражения или свои личные данные. Это могут быть имена, имена членов семьи, названия компьютеров, даты рождения и другие очевидные комбинации.
- Для повышения стойкости парольной защиты к перебору, во многих информационных системах реализуется проверка пароля на соответствие определенным требованиям и блокирование выбора простых паролей.
- Обычно термины «правила формата пароля», «опции автоматического блокирования», «политика смены паролей» не различаются и называются одним общим термином — **парольные политики**. **Парольные политики необходимы для повышения стойкости парольной защиты.**

Политика паролей

- **Политика паролей** - это набор правил, направленных на повышение безопасности компьютера путем поощрения пользователей к использованию надежных паролей и их правильному использованию.

- **Типичные компоненты политики паролей:**
  - Длина и формирование пароля;
  - Черные списки паролей;
  - Срок действия пароля.

Требования к паролям Рекомендации NIST (США) и ФСБ (РФ)

- В июне 2017 года Национальный институт стандартов и технологий США (NIST) выпустил новый пересмотр своих руководящих принципов цифровой аутентификации, NIST SP 800-63B-3.
- Сравним эти принципы с правилами по обеспечению защиты от НСД Федеральной службы безопасности Российской Федерации (ФСБ).

NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines
https://pages.nist.gov/800-63-3/
https://pages.nist.gov/800-63-3/sp800-63-3.html
NIST Special Publication 800-63A. Digital Identity Guidelines. Enrollment and Identity Proofing Requirements
https://pages.nist.gov/800-63-3/sp800-63a.html
NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management
https://pages.nist.gov/800-63-3/sp800-63b.html

Приказ Федеральной службы по интеллектуальной собственности от 14 июля 2015 г. N 97 "Об утверждении Положения по организации парольной защиты в Федеральной службе по интеллектуальной собственности“
https://www.garant.ru/products/ipo/prime/doc/71066002/
Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи https://roskazna.gov.ru/upload/iblock/9fc/rukovodstvo.pdf

NIST	ФСБ
•Пароли должны быть длиной не менее 8 символов, если они выбраны подписчиком •Системы проверки паролей должны позволять использовать пароли, выбранные подписчиком, длиной не менее 64 символов •Верификаторы могут заменить несколько последовательных пробелов одним пробелом до начала верификации, при условии, что результат будет иметь длину не менее 8 символов, но усечение пароля не производится	Длина пароля должна быть не менее 8 символов
•Все печатные символы ASCII, а также пробел должны быть допустимы в паролях. Допускается также использование символов Юникода •Проверяющие не должны навязывать другие правила составления паролей (например, требовать смешения различных типов символов или запрещать последовательно повторяющиеся символы) •Верификаторы должны предлагать подписчику рекомендации, например измеритель надежности пароля, чтобы помочь пользователю выбрать надежный пароль. Это особенно важно после отказа от пароля в приведенном выше списке, поскольку это препятствует тривиальной модификации занесенных в черный список (и, вероятно, очень слабых) паролей	В числе символов пароля обязательно должны присутствовать буквы в верхнем инижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.)
•При обработке запросов на установление или изменение паролей проверяющие сравнивают предполагаемые пароли со списком, содержащим значения, известные как часто используемые, ожидаемые или скомпрометированные. Если выбранный пароль найден в списке, верификатор сообщает подписчику, что необходимо выбрать другой пароль, и указывает причину отказа. Список может включать, но не ограничивается:Пароли, полученные от предыдущих нарушений [например, Облачных баз данных, взломанные коллекции] •Словарные слова •Пароли, состоящие из повторяющихся или последовательных символов (например, ‘aaaaaa’, ‘1234abcd’). •Контекстно-зависимые слова, такие как имя службы, имя пользователя и производные от него	Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.)
•Верификаторы должны реализовать механизм ограничения скорости, который эффективно ограничивает количество неудачных попыток аутентификации, которые могут быть сделаны на счете абонента •Проверяющие должны хранить пароли в форме, устойчивой к атакам в автономном режиме. Пароли должны быть засолены и хешированы с использованием подходящей односторонней функции формирования ключа. Функции формирования ключа принимают пароль, соль и коэффициент затрат в качестве входных данных, а затем генерируют хеш пароля	При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях
Верификаторы не должны позволять абоненту хранить "подсказку“, доступную неаутентифицированному заявителю, и верификаторы не должны побуждать абонентов использовать определенные типы информации (например," как звали вашего первого питомца?”) при выборе паролей	Личный пароль пользователь не имеет права сообщать никому
Верификаторы не должны требовать произвольного изменения паролей (например, периодически). Тем не менее, верификаторы должны принудить изменить, если есть доказательства компрометации пароля	Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев

Недостатки методов аутентификации с запоминаемым паролем

- **Атаки на пароли:**
  - Кража парольного файла
  - Атака со словарем
  - Подбор пароля
  - Социотехника
  - Принуждение
  - Подглядывание из-за плеча
  - Троянский конь
  - Аппаратный сниффер клавиатуры
  - Трассировка памяти
  - Отслеживание нажатия клавиш программными средствами
  - Регистрация излучения (перехват Ван Эка или фрикинг Ван Эка)
  - Анализ сетевого трафика
  - Атака на «золотой пароль»
  - Атака методом воспроизведения

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
КРАЖА ПАРОЛЬНОГО ФАЙЛА	
Злоумышленник может прочитать пароли пользователя из парольного файла или резервном копии	Хэширование пароля Каждая организация, разрабатывающая парольную аутентификацию, должна снабжать свои приложения этой защитой.
АТАКА СО СЛОВАРЕМ	
Злоумышленник, перебирая пароли, производит в файле паролей или его копии поиск, используя слова из большого заранее подготовленного им словаря. Злоумышленник вычисляет хэш-значение для каждого пробного пароля с помощью того же алгоритма, что и программа аутентификации.	Безопасность файла Доступ на чтение к файлу паролей должен быть предоставлен лишь небольшому числу доверенных пользователей. Хэшированные с шумами (помехами) пароли Генерирование хэш-значения различным способом для каждого пользователя намного усложняет атаку со словарем: злоумышленник должен при подборе пароля каждого пользователя еще и подбирать способ хэширования пароля. Это достигается в системах с помощью использования меняющегося значения, называемого шумом. Правила формата пароля Такие правила могут требовать, чтобы пароль содержал как минимум одну цифру, как минимум один «специальный» символ, комбинации заглавных и строчных букв, и т.д.

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
ПОДБОР ПАРОЛЯ	
Исходя из знаний личных данных пользователя, злоумышленник пытается войти в систему с помощью имени пользователя и одного или нескольких паролей, которые он мог бы использовать (в том числе пароля, установленного по умолчанию).	Правила формата пароля Как для «атаки со словарем» выше. Изменение пароля, установленного по умолчанию Пароль, установленный по умолчанию, должен изменяться сразу после первого использования. По возможности следует вовсе исключить практику использования общеизвестных паролей. Автоматическое блокирование После нескольких безуспешных попыток входа система или блокирует учетную запись пользователя на некоторое время, или вовсе аннулирует ее.
СОЦИОТЕХНИКА	
На пользователей Злоумышленник представляется администратором и вынуждает пользователя или открыть свой пароль, или сменить его на указанный им пароль. **На администраторов:** Злоумышленник представляется законным пользователем и просит администратора заменить пароль для данного пользователя.	**Политика нераскрытая паролей** В организации должны быть разработаны административные процедуры, запрещающие сообщать пароли другим лицам при любых обстоятельствах. Организация должна также извещать пользователей о том, что администратор никогда не обратится к пользователю с таким требованием. **Политика смены паролей** В организации должна действовать политика, согласно которой администратор меняет пароль пользователя только при условии, что он может установить его личность и передать новый пароль пользователю безопасным способом. Средства самостоятельного управления паролями могут удовлетворять обоим критериям.

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
ПРИНУЖДЕНИЕ	
Для того чтобы заставить пользователя открыть свой пароль, злоумышленник использует угрозы или физическое принуждение.	Сигнал о принуждении В некоторых системах предусматривается возможность для пользователя подавать сигнал о том, что вход осуществляется под принуждением Обычно это реализуется с помощью специального пароля при входе в систему — пароль «вход под принуждением»
ПОДГЛЯДЫВАНИЕ ИЗ-ЗА ПЛЕЧА	
Расположенный рядом злоумышленник или видеокамера следит за тем, как пользователь вводит свой пароль.	Неотображение пароля В большинстве систем пароли либо не отображаются на экране либо отображаются незначащими символами. В некоторых системах отображается количество таких символов, отличное от введенного. Вопреки этой технологии, злоумышленник может видеть, на какие непосредственно клавиши нажимает пользователь. Также применяются технологии, которые дают пользователю строго ограниченное время для ввода пароля, тем самым заставляя его вводить пароль максимально быстро. Таким образом, уменьшается вероятность его подсматривания, а также усложняется его подбор злоумышленником.

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
ТРОЯНСКИЙ КОНЬ	
Злоумышленник скрытно устанавливает программное обеспечение, имитирующее обычный механизм аутентификации, но собирающее имена пользователей и пароли при попытках пользователей войти в систему.	Особый режим интерактивного взаимодействия для механизма аутентификации В некоторых системах механизм аутентификации вызывается специально выделенным для этого сочетанием клавиш, недоступным для других программ. В ОС Microsoft Windows в качестве такого сочетания клавиш используется [Ctrl]—[Alt]—[Delete] Антивирусное программное обеспечение Организация может обнаруживать программы типа «троянский конь» с помощью антивирусного программного обеспечения. Средства обеспечения контроля целостности файлов В организации может использоваться система обнаружения вторжений (intrusion detection system) для определения модификации важных файлов, например, программы регистрации.

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
АППАРАТНЫЙ СНИФФЕР КЛАВИАТУРЫ	
Злоумышленник скрыто устанавливает в компьютер пользователя аппаратное средство, собирающее информацию, которую вводит пользователь при входе в систему, например, Keykeriki для беспроводных клавиатур, KeyCarbon, Key Devil или KeyGhost для проводных клавиатур.	Безопасность рабочих помещений Служба безопасности компании должна предоставлять доступ в помещения, в которых располагаются компоненты информационной системы предприятия, только тем, кому он разрешен. Безопасность рабочих мест Служба безопасности компании должна обеспечить возможность контроля компонентов информационной системы предприятия для защиты от возможности установки в них незаконных аппаратных средств. Контроль над соответствующими компонентами информационной системы предприятия возлагается на сотрудников компании, службу ИТ или службу безопасности компании
ТРАССИРОВКА ПАМЯТИ	
Злоумышленник использует программу для копирования пароля пользователя из буфера клавиатуры.	Защита памяти Некоторые ОС используют аппаратную защиту буферов клавиатуры от возможности ее трассировки.

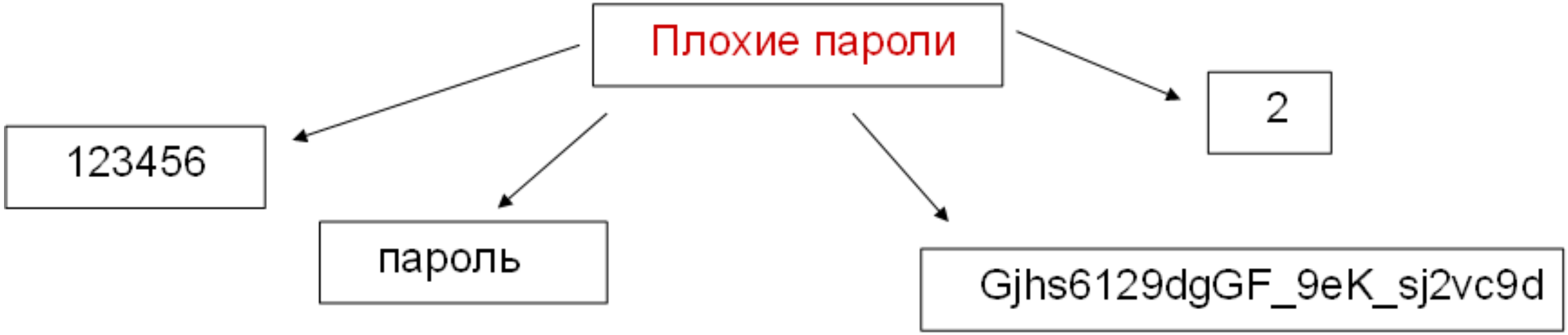
Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
ОТСЛЕЖИВАНИЕ НАЖАТИЯ КЛАВИШ ПРОГРАММНЫМИ СРЕДСТВАМИ	
Для предотвращения использования компьютеров не по назначению некоторые организации используют программное обеспечение, следящее за нажатием клавиш. Злоумышленник может для получения паролей просматривать журналы соответствующей программы.	Безопасность файлов Доступ на чтение к журналам должен быть предоставлен лишь узкому кругу доверенных пользователей (администраторов) с по мощью собственной или резидентной службы контроля доступа
РЕГИСТРАЦИЯ ИЗЛУЧЕНИЯ (ПЕРЕХВАТ ВАН ЭКА ИЛИ ФРИКИНГ ВАН ЭКА)	
Вим Ван Эк описал метод, которым злоумышленник может перехватывать информацию с монитора путем регистрации его излучения. Вин Швартау высказал идею приемников Ван Эка, регистрирующих не только видеосигналы.	Неотображение пароля Как для «подглядывания из-за плеча» выше Безопасность излучений Модернизация устройств для уменьшения излучения с помощью использования современных микрокомпонент, специально разработанных с учетом необходимости уменьшения излучения. Проектирование помещении и планирование расположения оборудования в нем с учетом предотвращения возможности утечки информации через паразитное излучение оборудования.

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
АНАЛИЗ СЕТЕВОГО ТРАФИКА	
Злоумышленник анализирует сетевой трафик, передаваемый от клиента к серверу, для восстановления из него имен пользователей и их паролей.	Шифрование Весь сетевой трафик или только пароли могут шифроваться для передачи по сети (использование протокола SSL или VPN-соединений). Одноразовые пароли Использование методов аутентификации, в которых «пароли» пользователей изменяются каждый раз при входе в систему.
АТАКА НА «ЗОЛОТОЙ ПАРОЛЬ»	
Злоумышленник ищет пароли пользователя, применяемые им в различных системах — домашняя почта, игровые серверы и т. п. Есть большая вероятность того, что пользователь применяет один и тот же пароль во всех системах.	Шифрование Как для «анализа сетевого трафика» (см. выше). Одноразовые пароли Как для «анализа сетевого трафика» (см. выше).
АТАКА МЕТОДОМ ВОСПРОИЗВЕДЕНИЯ	
Злоумышленнк записывает последовательность передаваемых и получаемых субъектом доступа в процессе аутентификации данных. Позднее он осуществляет попытку аутентификации, передавая и получая записанные данные в той же последовательности.	Использование надежных протоколов аутентификации Надежные протоколы аутентификации предполагают использование при обмене данными с субьъектом доступа криптографически защищенных меток времени. Одноразовые пароли Как для «анализа сетевого трафика» (см. выше).

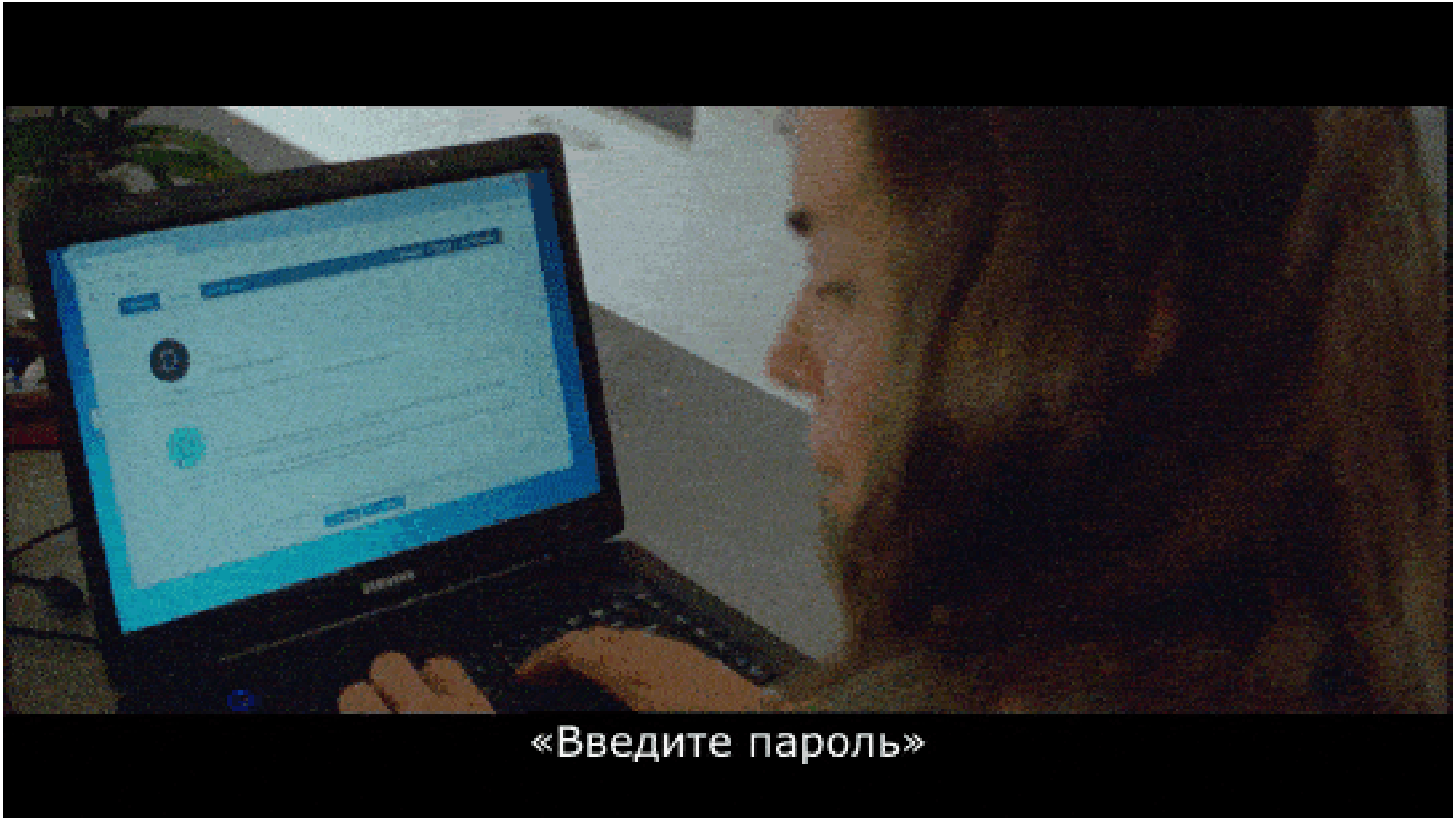
Решение проблемы "паролей"



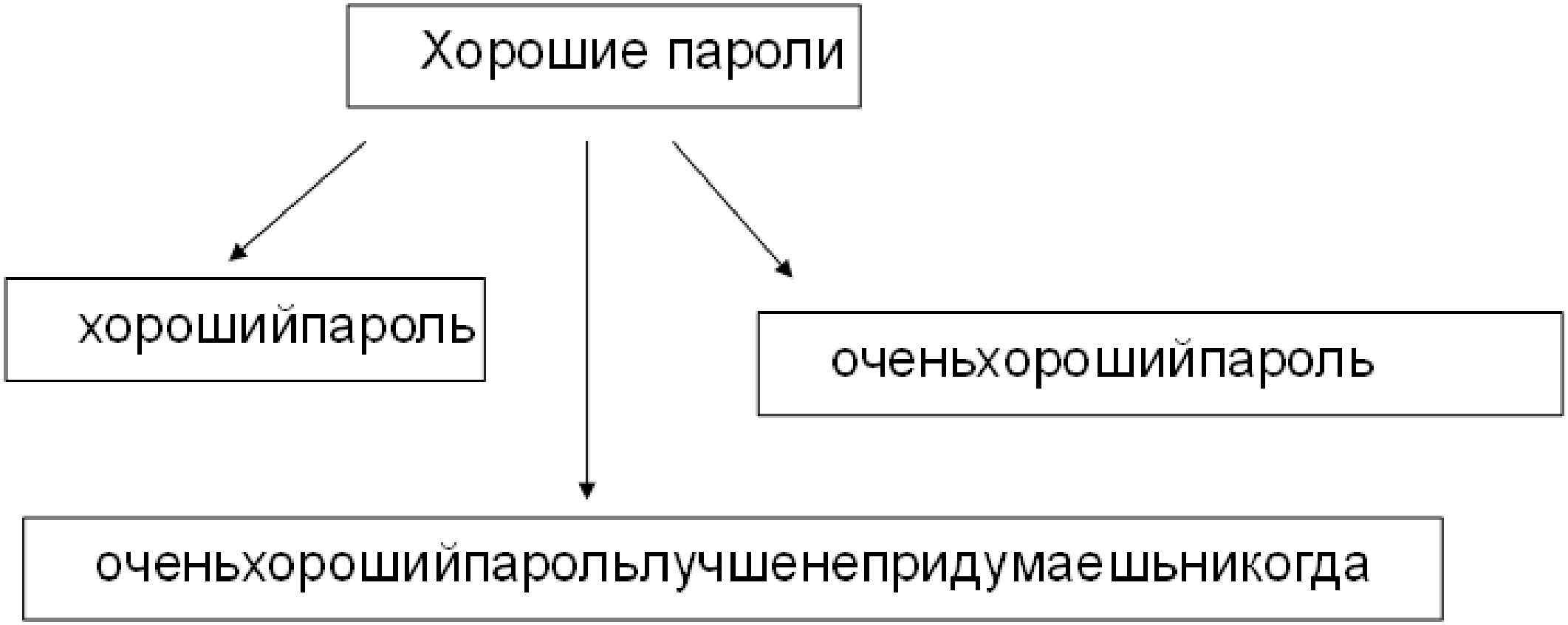
Почему эти пароли плохие:

- **"2"** - один символ, легко перебрать.
- **"123456"** - один из популярных паролей (еще примеры - 123; 111; qwerty; qazwsx; qazwsxedc; password; "ваш логин"; "номер телефона"; "дата рождения" и т.д.).
- **"пароль"** - словарное слово, после перебора популярных паролей, перебирают слова из словаря.
- **"Gjhs6129dgGF_9eK_sj2vc9d"** - пароль очень сложный, его не запомнят, а запишут и приклеят к монитору, пароль должен быть только в голове (или в сейфе).

Решение проблемы "паролей"



Решение проблемы "паролей"

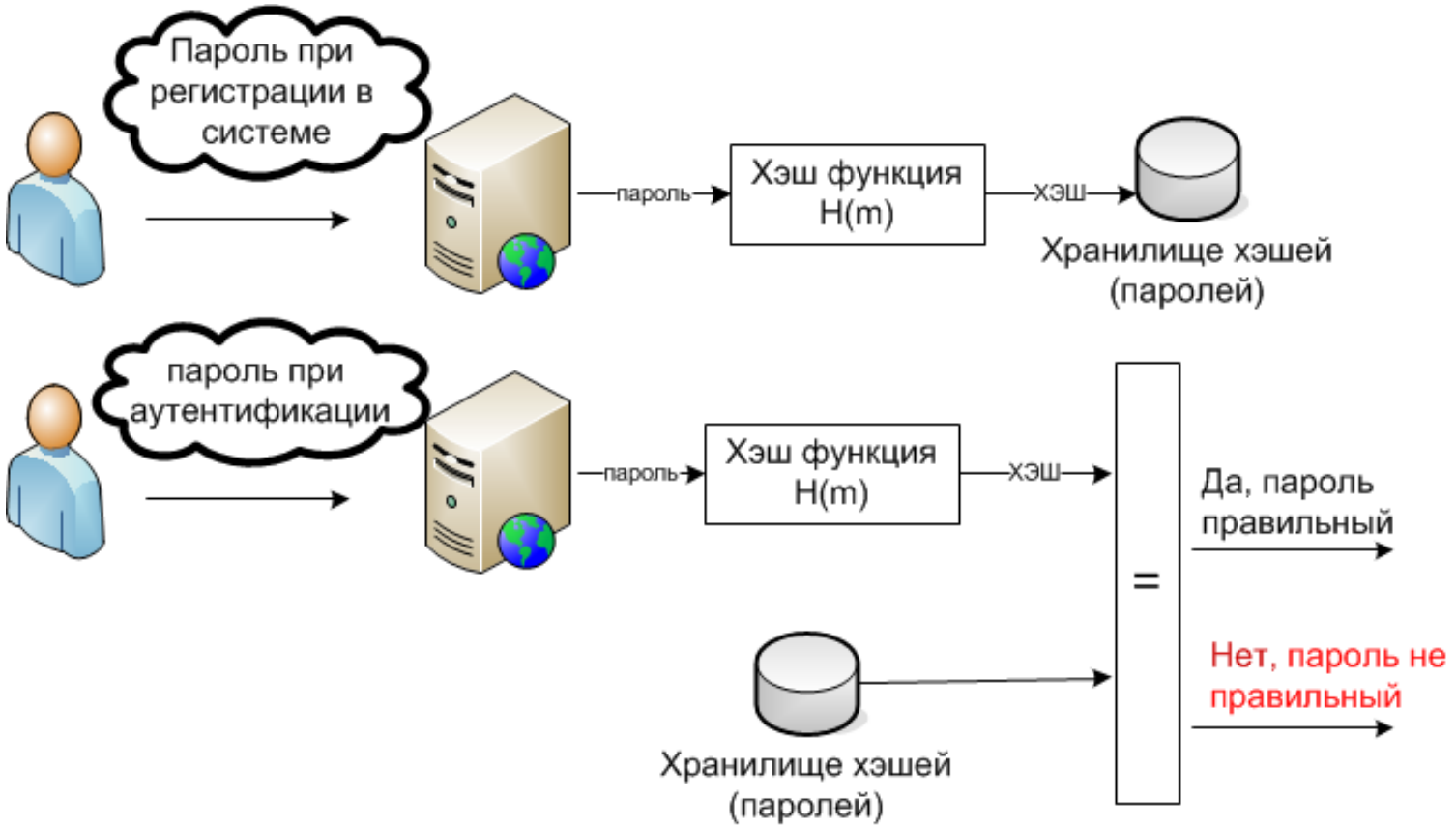


Наиболее хорошим вариантом являются пароли построенные на фразах:

- хорошо запоминаются
- достаточно длинные
- словарные атаки не проходят

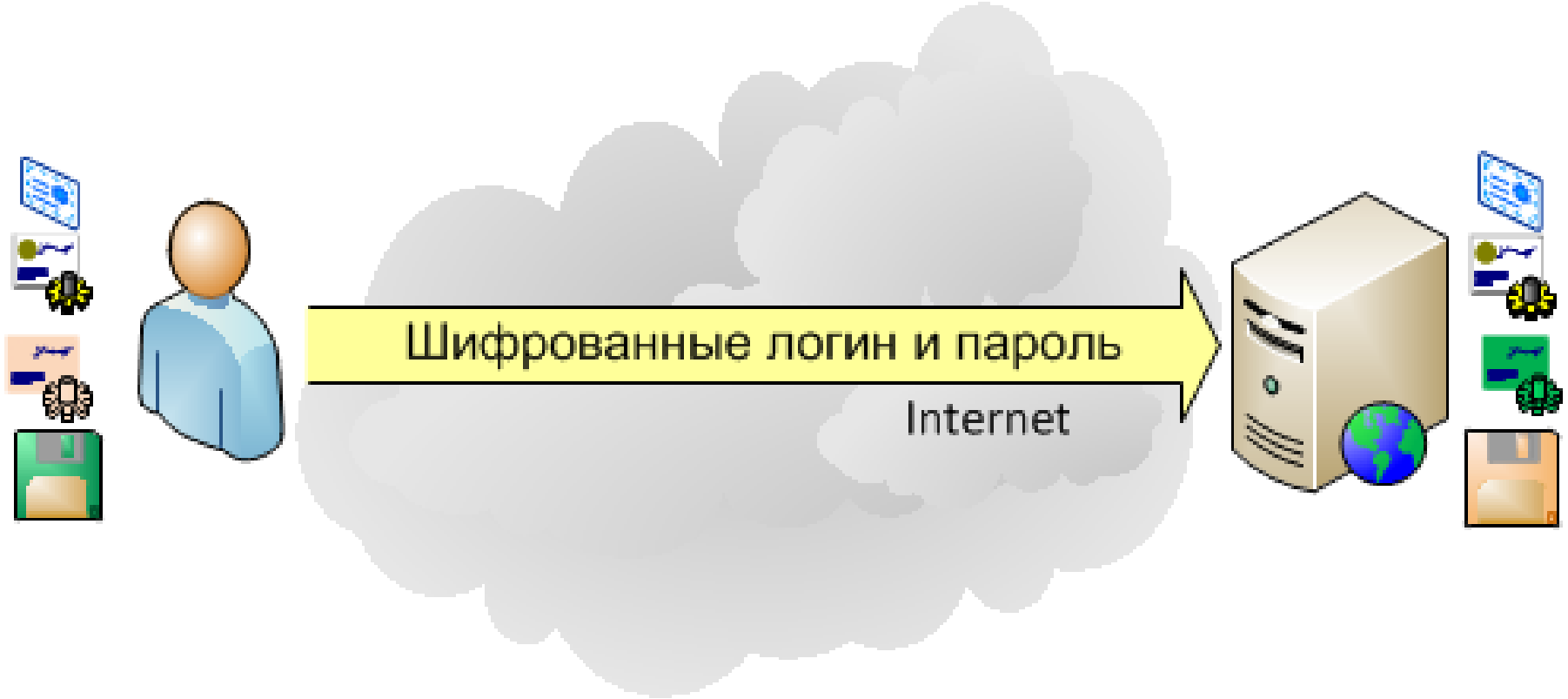
Решение проблемы "паролей"

- **Решение проблемы "просмотра паролей в системе"** :
  - шифрование (для расшифровывания нужно будет при себе носить ключ шифрования, при хранении на диске не защищенного ключа шифрования шифрование пароля не имеет смысла).
  - не хранить пароль в системе, а хранить его контрольную сумму или хэш.
- Пароли в системе не хранятся, при этом пользователь проходит аутентификацию по паролю.
- В большинстве современных систем именно так и сделано. Не только в ОС, но и в СУБД, форумах, сайтах и т.д.



Решение проблемы "паролей"

- **Решение проблемы "перехвата паролей при передачи":**
  - шифровать передаваемые пароли
  - использовать алгоритмы без передачи паролей (например по протоколу CHAP).
- В настоящее время чаще всего для шифрования паролей используется протокол SSL (Secure Sockets Layer — уровень защищённых сокетов)



Классификация протоколов аутентификации

Строгая аутентификация

Строгая аутентификация

- **В соответствии с рекомендациями стандарта X.509** различают процедуры строгой аутентификации следующих типов.
  - а) односторонняя аутентификация;
  - б) двусторонняя аутентификация;
  - в) трехсторонняя аутентификация.

X.509 — стандарт ITU-T для инфраструктуры открытого ключа (англ. Public key infrastructure, PKI) и инфраструктуры управления привилегиями (англ. Privilege Management Infrastructure).

X.509 определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями.
Эти сертификаты предоставляются удостоверяющими центрами (англ. Certificate Authority).
Кроме того, X.509 определяет формат списка аннулированных сертификатов, формат сертификатов атрибутов и алгоритм проверки подписи путём построения пути сертификации.
X.509 предполагает наличие иерархической системы удостоверяющих центров для выдачи сертификатов.
Сертификат X.509 используется для **проверка личности одноранговой** при использовании протокола HTTPS (HTTP по SSL)

Строгая аутентификация. Односторонняя

- **Односторонняя аутентификация** предусматривает обмен информацией только в одном направлении.

- Данный тип аутентификации **позволяет**:
  - **подтвердить** подлинность только одной стороны информационного обмена;
  - **обнаружить** нарушение целостности передаваемой информации;
  - **обнаружить** проведение атаки типа «повтор передачи»;
  - **гарантировать**, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона.

Строгая аутентификация. Двусторонняя и Трехсторонняя

- **Двусторонняя аутентификация** по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с той стороны, которой были предназначены аутентификационные данные.

- **Трехсторонняя аутентификация** содержит дополнительную передачу данных от доказывающей стороны проверяющей. Этот подход позволяет отказаться от использования меток времени при проведении аутентификации.

Строгая аутентификация

- **При использовании строгой аутентификации для проверки подлинности пользователя используется несколько методов или факторов**:
  - **Фактор знания:** общий секрет между пользователем и субъектом проверки подлинности пользователя (например, пароли, ответы на секретные вопросы и т. д.)
  - **Фактор владения:** устройство, которым обладает только пользователь (например, мобильное устройство, криптографический ключ и т. д.)
  - **Фактор неотъемлемости:** физические (часто биометрические) характеристики пользователя (например, отпечаток пальца, рисунок радужки глаза, голос, поведение и т. д.)

Строгая аутентификация

- Необходимость взломать несколько факторов значительно увеличивает вероятность неудачи для злоумышленников, поскольку обход или обман различных факторов требует использования нескольких типов тактик взлома, для каждого фактора отдельно.
- **Важно отметить, что по крайней мере один из факторов аутентификации, применяемый при строгой аутентификации, должен использовать криптографию на основе открытого ключа.**

Классификация протоколов строгой аутентификации

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы.

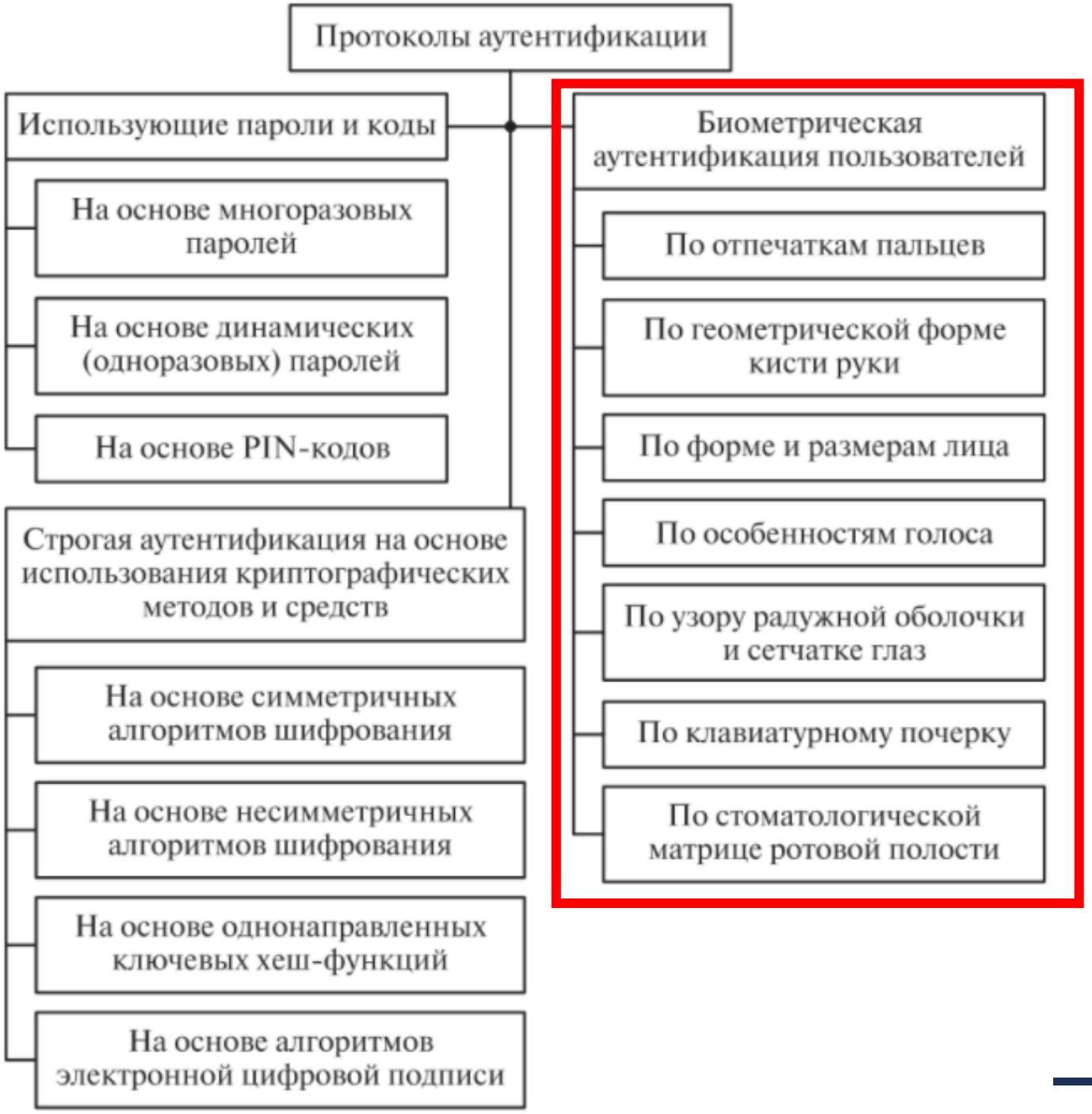
Строгая аутентификация

отчет Javelin «Состояние строгой аутентификации»
The State of Strong Authentication 2019 Report

Строгая аутентификация

отчет Javelin «Состояние строгой аутентификации»
The State of Strong Authentication 2019 Report

Классификация протоколов аутентификации



Биометрическая аутентификация

Биометрическая аутентификация

- Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.).
- Привычные системы аутентификации не всегда удовлетворяют современным требованиям в области информационной безопасности, особенно если речь идет об ответственных приложениях (онлайновые финансовые приложения, доступ к удаленным базам данных и т.п.).
- В последнее время все большее распространение получает **биометрическая аутентификация** пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Биометрическая аутентификация

- **Биометрическая характеристика** — это измеримая физиологическая или поведенческая черта живого человека, которую можно использовать для установления личности или проверки декларируемых личных данных.

- **Биометрические характеристики делятся на физиологические и поведенческие.**

Биометрическая аутентификация

- **Биометрические характеристики делятся на физиологические и поведенческие.**

- **Физиологические биометрические характеристики** (физические биометрические характеристики, статические биометрические характеристики) — биометрические характеристики на основе данных, полученных путем измерения анатомических характеристик человека.

- К физиологическим биометрическим характеристикам можно отнести:
  - радужную оболочку глаза;
  - отпечаток пальца;
  - лицо;
  - кисть;
  - сетчатку.

Биометрическая аутентификация

- **Биометрические характеристики делятся на физиологические и поведенческие.**

- **Поведенческие биометрические характеристики** (динамические биометрические характеристики) — биометрические характеристики на основе данных, полученных путем измерения действий человека.

- Характерной чертой для поведенческих параметров является их протяженность во времени — измеряемое действие имеет начало, середину и конец.

- К поведенческим биометрическим характеристикам можно отнести:
  - голос;
  - подпись;
  - ритм работы сердца;
  - ходьбу.

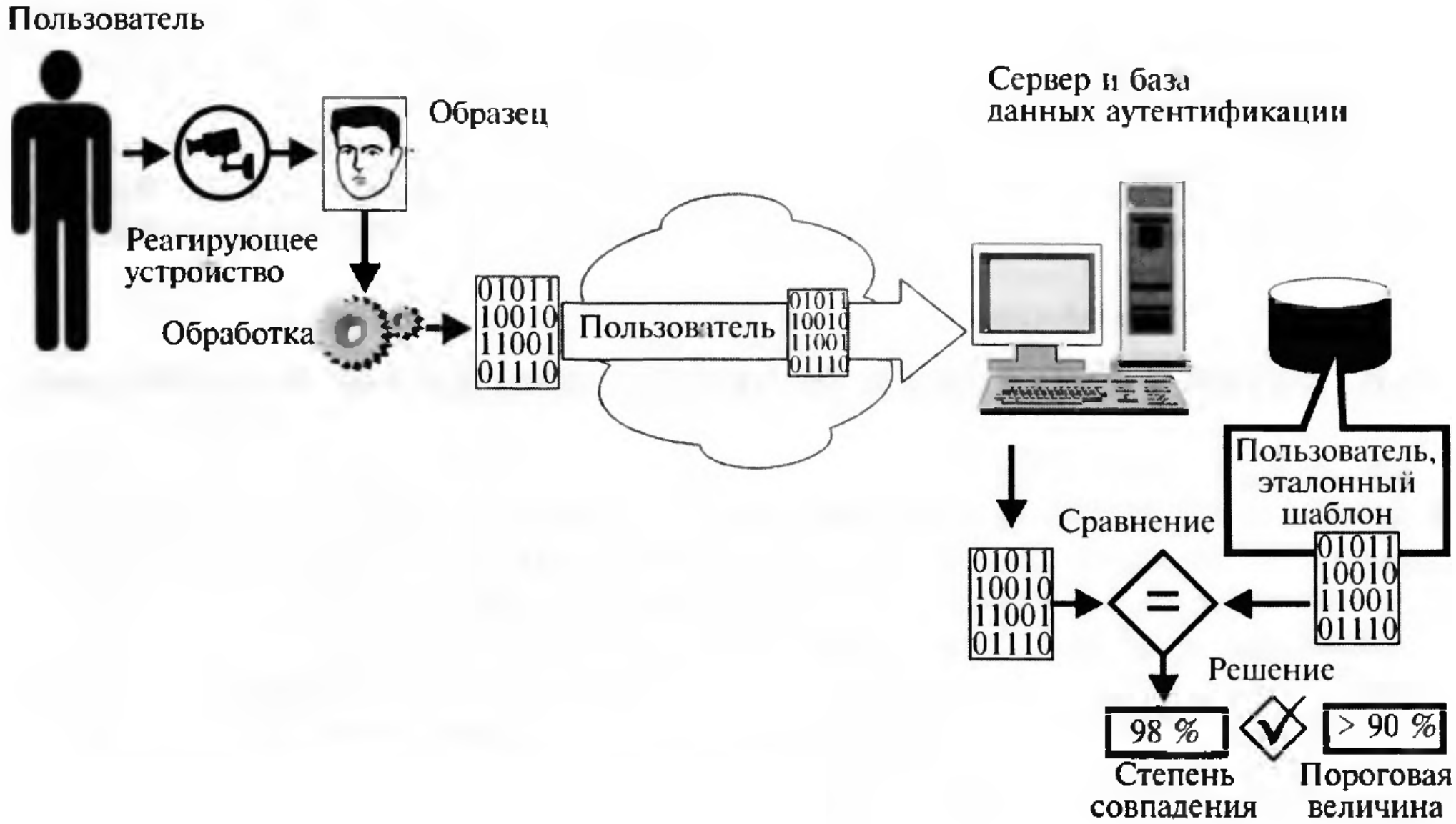
Биометрическая аутентификация

- **Биометрические характеристики делятся на физиологические и поведенческие.**
- **Поведенческие** биометрические параметры достаточно зависимы от физиологии.
- **Физиологические** биометрические характеристики обычно неизменны в течение жизни человека и не могут быть изменены без существенного воздействия на человека.

Биометрическая аутентификация

- **Все биометрические системы работают одинаково**: пользователь предоставляет образец, с помощью регистрирующего устройства этот биометрический образец обрабатывается, в результате чего получается контрольный шаблон.

Схема работы биометрических систем



Биометрические системы могут ошибаться

- **Биометрические системы могут ошибаться**, контрольный шаблон может быть ошибочно признан:
  - соответствующим эталонному шаблону другого лица;
  - несоответствующим эталонному шаблону данного пользователя, несмотря на то что этот пользователь зарегистрирован в биометрической системе.

- **Точность биометрической системы** измеряется двумя параметрами:
  - **коэффициентом неверных совпадений (FMR)**, также известным под названием ошибка типа I или вероятность южного допуска (FAR);
  - **коэффициентом неверных несовпадений (FNMR)**, также известным под названием ошибка типа II или вероятность ложного отказа в доступе (FRR).

Реализация физиологических биометрических характеристик

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Радужная оболочка глаза	Видеокамера, способная работать в инфракрасном диапазоне, камера для ПК	Черно-белое (или цветное) изображение радужной оболочки глаза	Полоски и бороздки в радужной оболочке глаза
Отпечаток пальца	Периферийное устройство настольного компьютера, карта стандарта PC card, мышь, микросхема или считыватель, встроенный в клавиатуру	Изображение отпечатка пальцев (оптическое, на кремниевом фото-приемнике, ультразвуковое, или бесконтактное)	Расположение и направление гребешковых выступов и разветвлений на отпечатке пальцев, мелкие детали
Лицо	Видеокамера, камера для ПК, цифровой фотоаппарат	Изображение лица (оптическое, двумерное (2D-фото) или трехмерное (3D-фото))	Форма черепа, относительное расположение и форма носа, расположение скул
Кисть	Настенное устройство	Трехмерное изображение верха и боков кисти	Высота и ширина костей и суставов кисти и пальцев
Сетчатка	Настольное или настенное устройство	Изображение сетчатки	Расположение кровеносных сосудов на сетчатке

Реализация поведенческих биометрических характеристик

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Голос	Микрофон телефон	Запись голоса	Частота, модуляция и продолжительность голосового образа
Подпись	Планшет для подписи, перо для ввода данных	Изображение подписи и показания соответствующих динамических измерении	Скорость, порядок линий, давление и внешний вид подписи
Динамика нажатия клавиш	Клавиатура	Ритм машинописи	Время задержки (промежуток времени, в течение которого пользователь удерживает конкретную клавишу) время «полета» (промежуток времени, который требуется пользователю для перехода с одной клавиши на другую)

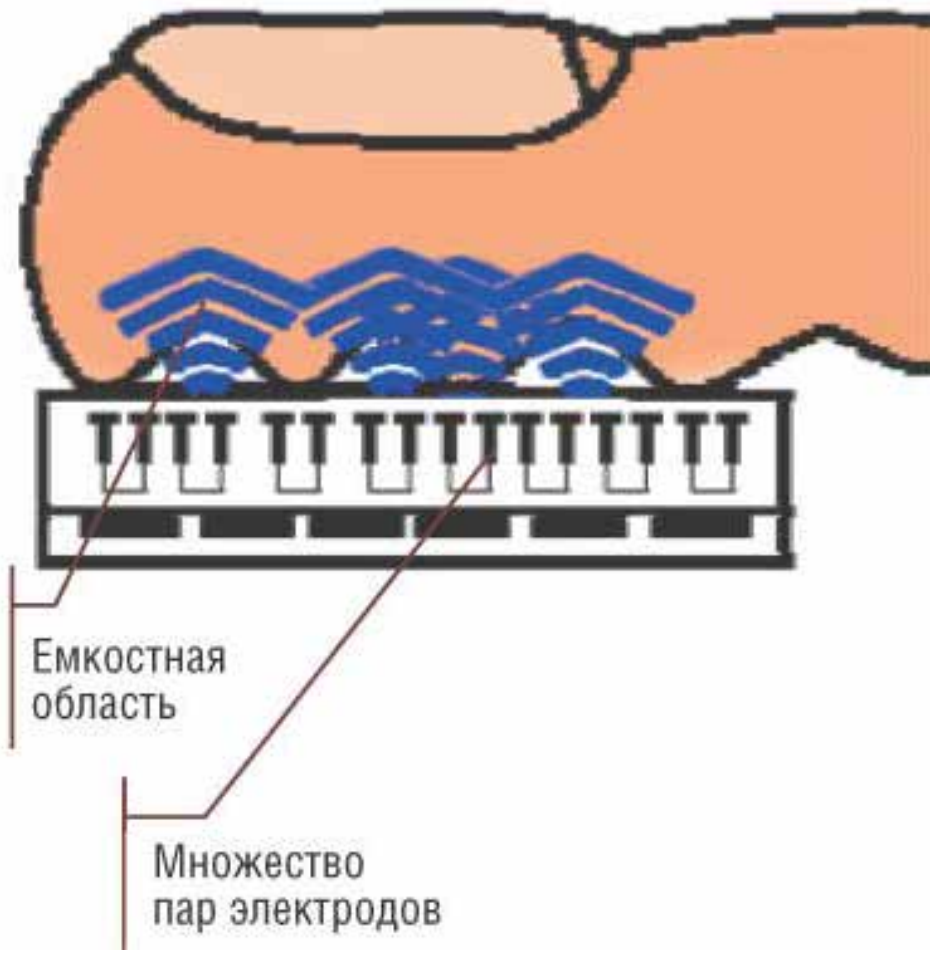
Биометрическая аутентификация. Аутентификация по отпечаткам пальцев

- **Аутентификация по отпечаткам пальцев.** Большинство систем используют отпечаток одного пальца, который пользователь предоставляет системе.
- Дактилоскопическая система работает следующим образом. Сначала производится регистрация пользователя. Как правило, производится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образны будут немного отличаться и требуется сформировать некоторый обобщенный образец, «паспорт». Результаты сохраняются в базе данных аутентификации. При аутентификации производится сравнение отсканированного отпечатка пальца с «паспортами», хранящимися в базе данных.

Биометрическая аутентификация. Аутентификация по отпечаткам пальцев

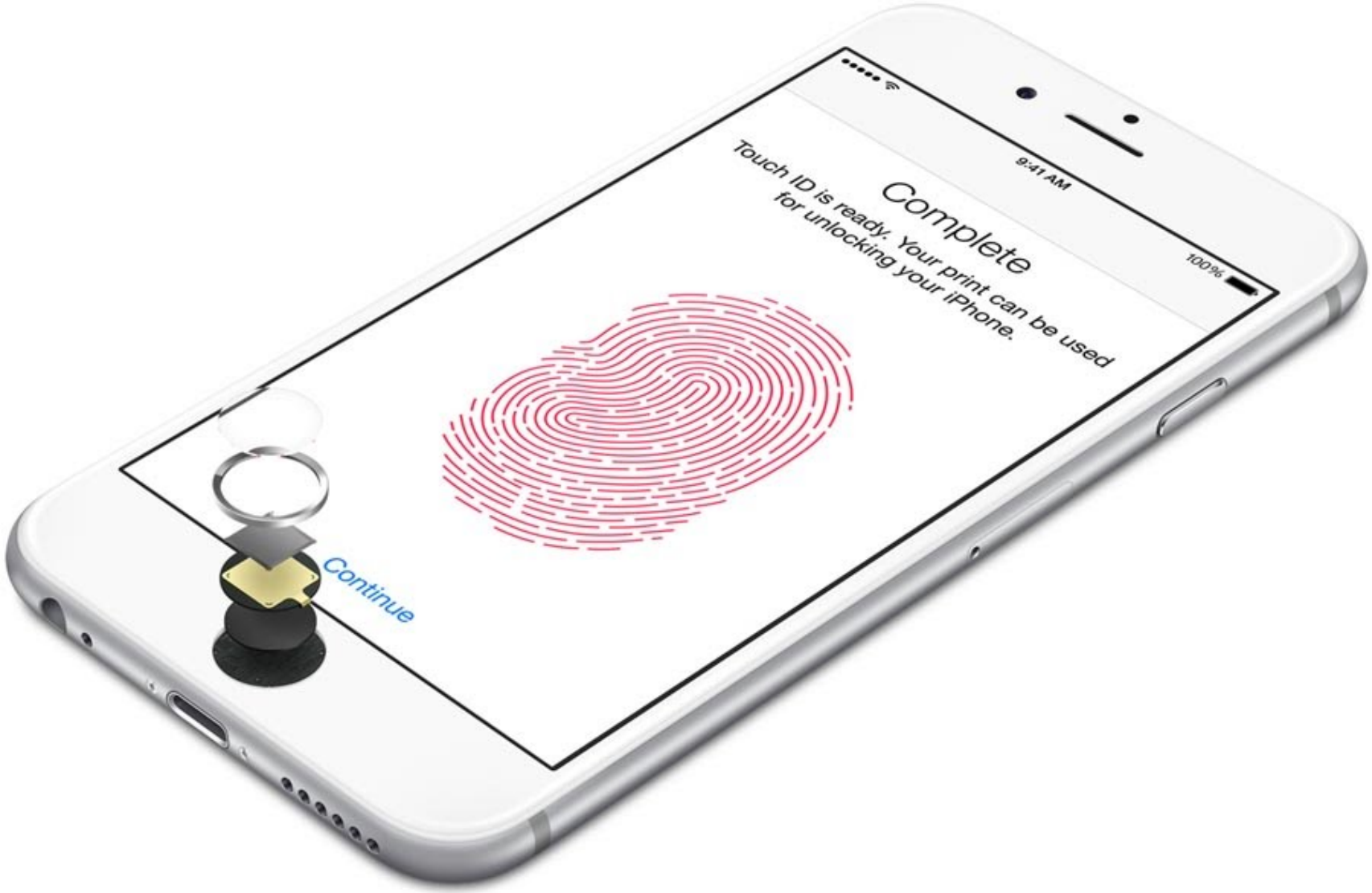
Как работают ёмкостные сканеры отпечатков Ультразвуку не страшна грязь на поверхности кожи, он создаёт наиболее чёткую карту узора. Дактилоскопия — довольно достоверный метод установления личности с помощью полупроводниковых ёмкостных сканеров, но и у него есть недостатки. Пальцы травмируются, кожа бывает сухой и стареет — во всех этих случаях узор отпечатка бледнеет или «портится». Работа сканеров строится на изменении ёмкости электронно-дырочного перехода полупроводника при соприкосновении гребня папиллярного узора с элементом полупроводниковой матрицы.

Биометрическая аутентификация. Аутентификация по отпечаткам пальцев



Биометрическая аутентификация. Аутентификация по отпечаткам пальцев

Биометрическая аутентификация. Аутентификация по отпечаткам пальцев



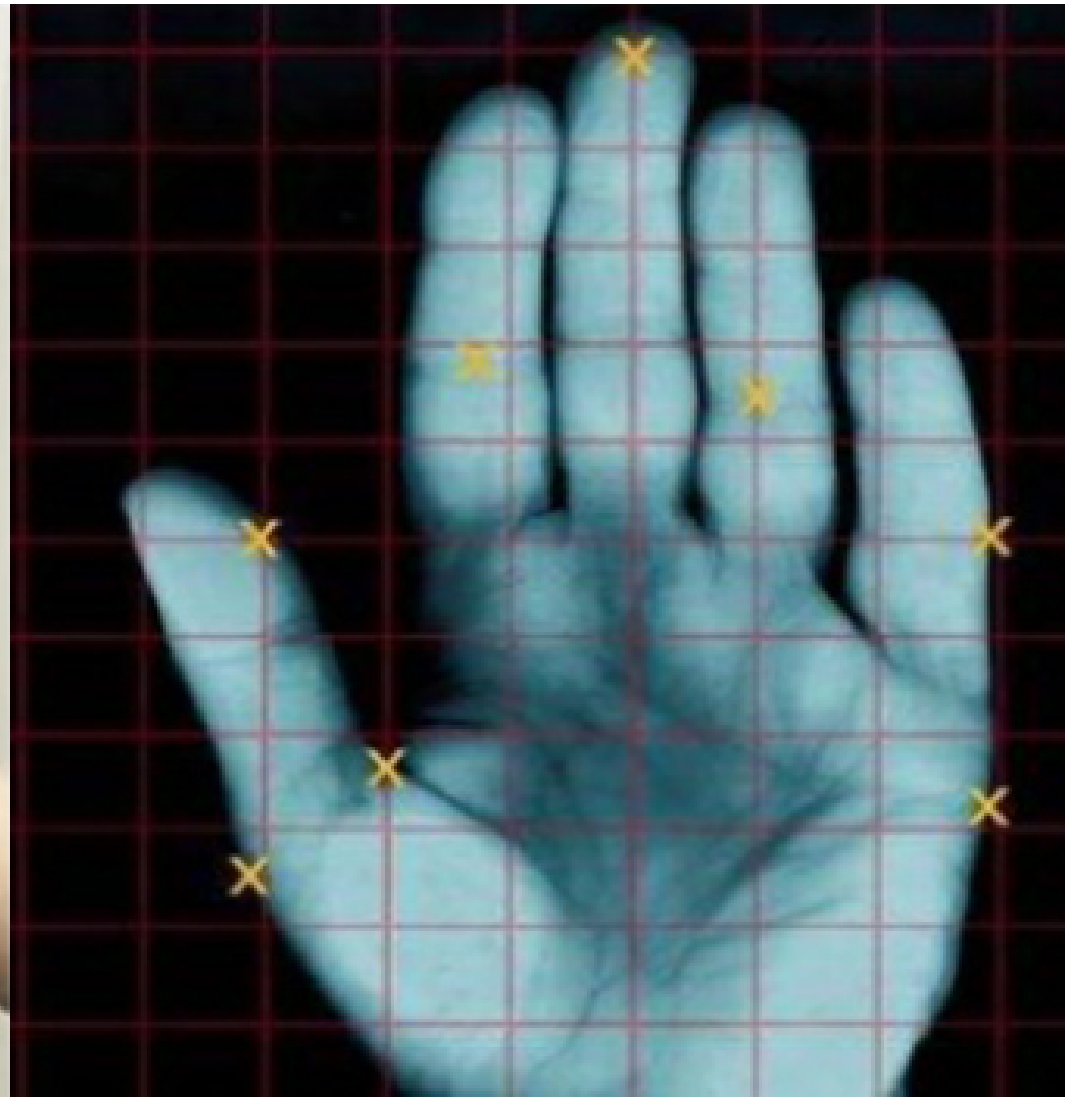
Биометрическая аутентификация. Аутентификация по отпечаткам пальцев

Биометрическая аутентификация. Аутентификация по отпечаткам пальцев

Биометрическая аутентификация. Аутентификация по форме ладони.

- **Аутентификация по форме ладони.**
- Данная аутентификация проводится сканерами формы ладони, обычно устанавливаемыми на стенах.
- Устройства считывания формы ладони создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони.
- Всего может выполняться до 100 измерений, которые преобразуются в двоичный код — образец для дальнейших сравнений. Этот образец может сохраняться в базе данных или в сканере ладони.

Биометрическая аутентификация. Аутентификация по форме ладони.

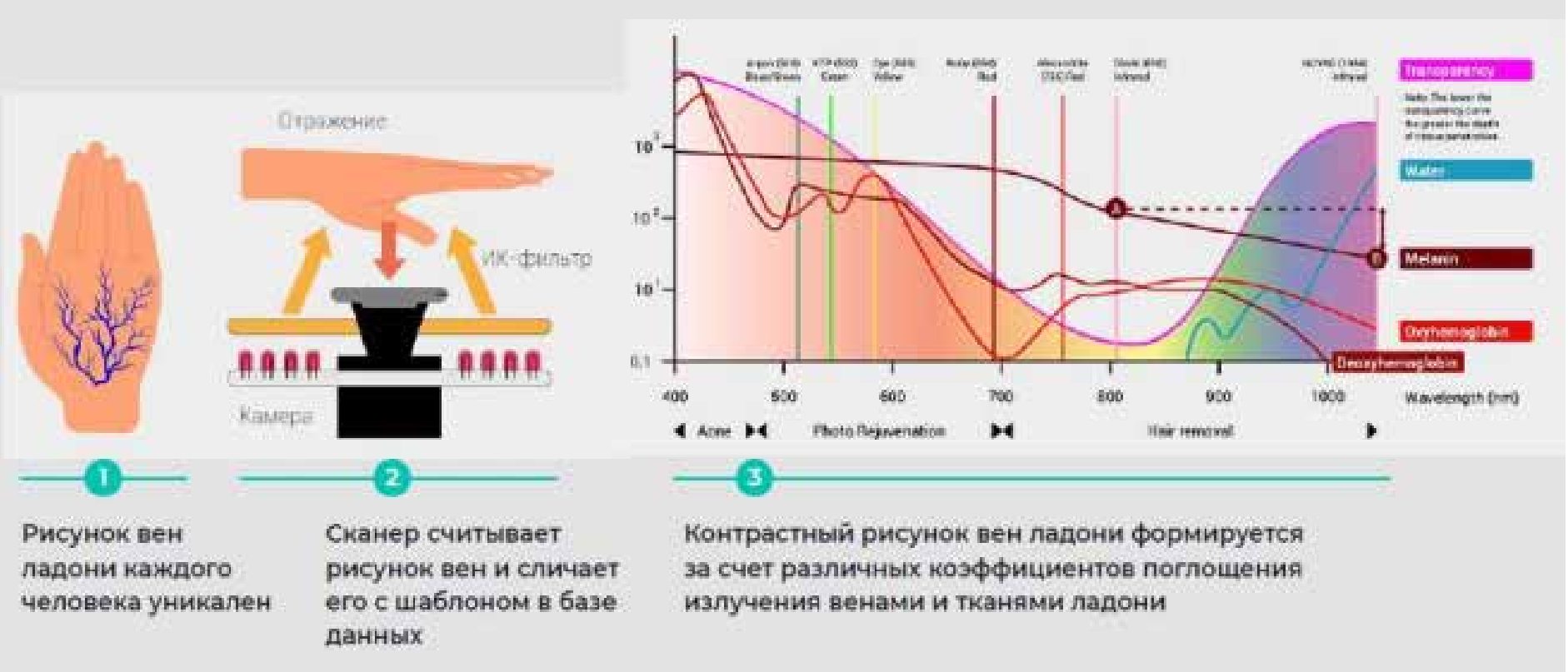


Биометрическая аутентификация. Аутентификация по форме ладони.

Биометрическая аутентификация. Аутентификация по форме ладони.

Биометрическая аутентификация. Аутентификация по рисунку вен ладони.

Биометрическая аутентификация. Аутентификация по рисунку вен ладони.



- Биометрический сканер идентифицирует человека по уникальному рисунку кровеносных сосудов под кожей руки.
- Рисунок вен невозможно украсть, потерять, передать другому лицу, невозможно подделать, поскольку вены ладони не видны в оптическом спектре.

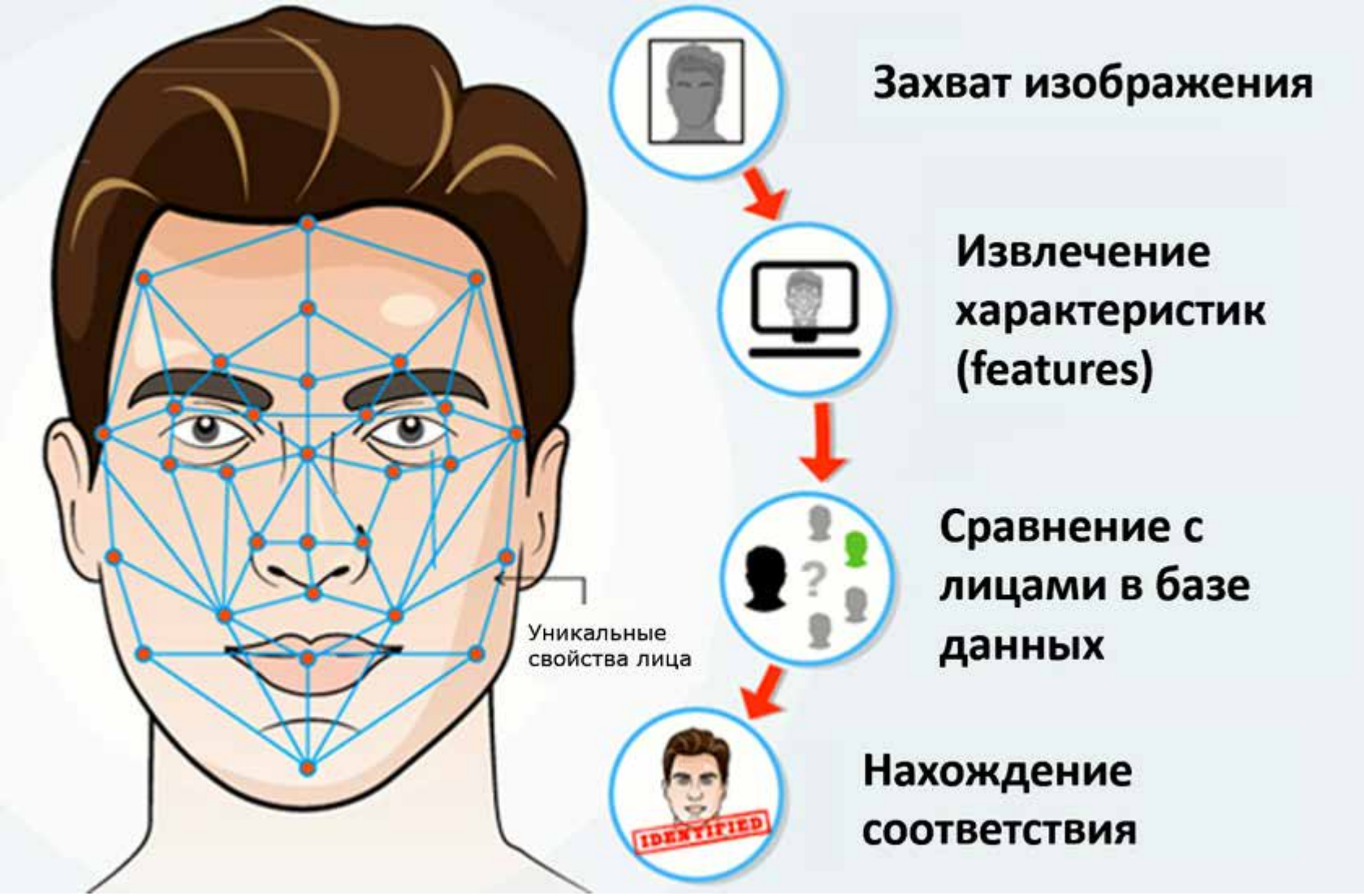
Биометрическая аутентификация. Аутентификация по лицу и голосу

- **Аутентификация по лицу и голосу.**
- Данные системы являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства.
- Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Биометрическая аутентификация. Аутентификация по лицу

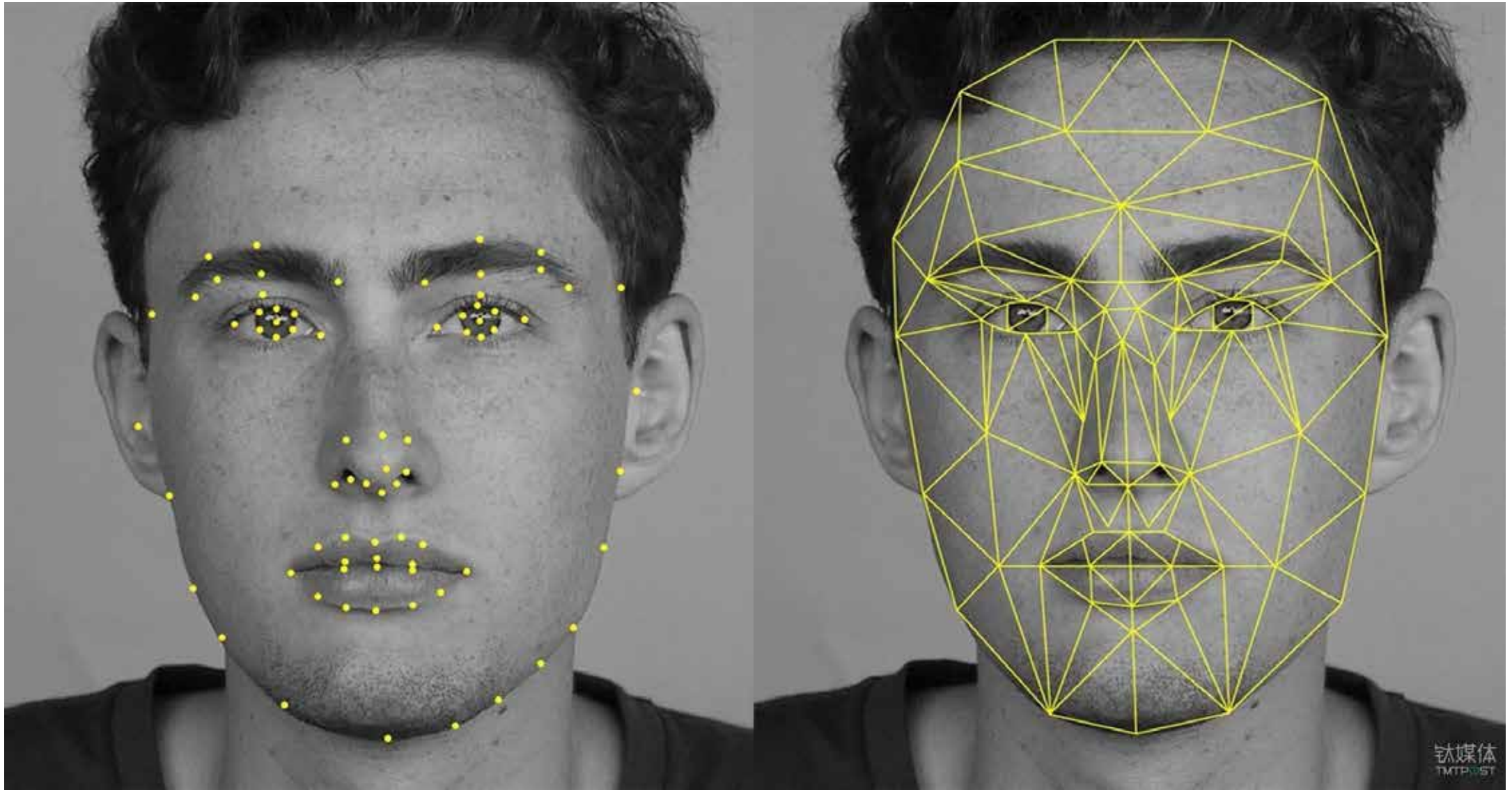
Биометрическая аутентификация. Аутентификация по лицу

Биометрическая аутентификация. Аутентификация по лицу

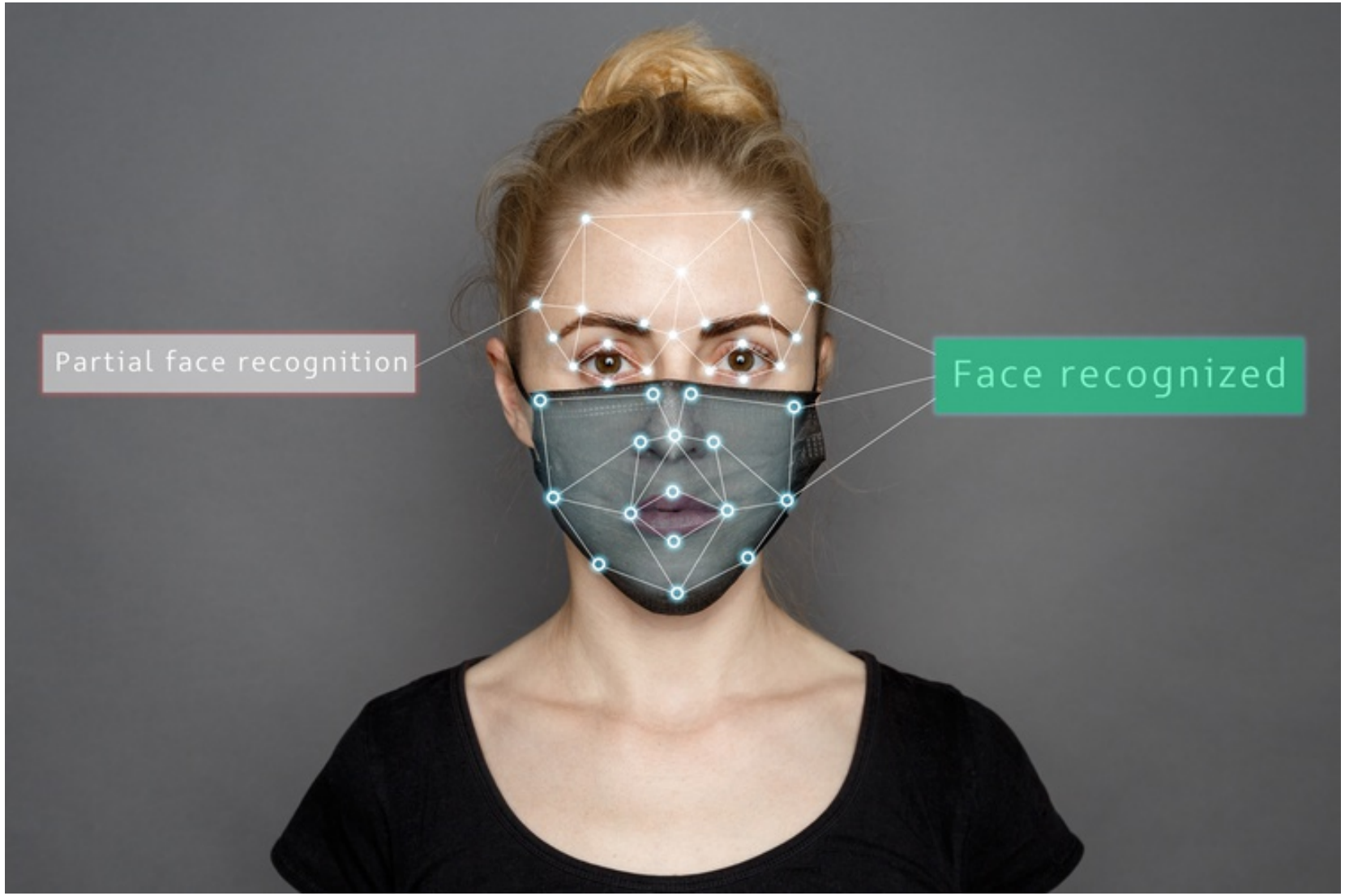


Биометрическая аутентификация. Аутентификация по лицу

Биометрическая аутентификация. Аутентификация по лицу



Биометрическая аутентификация. Аутентификация по лицу



Биометрическая аутентификация. Аутентификация по лицу

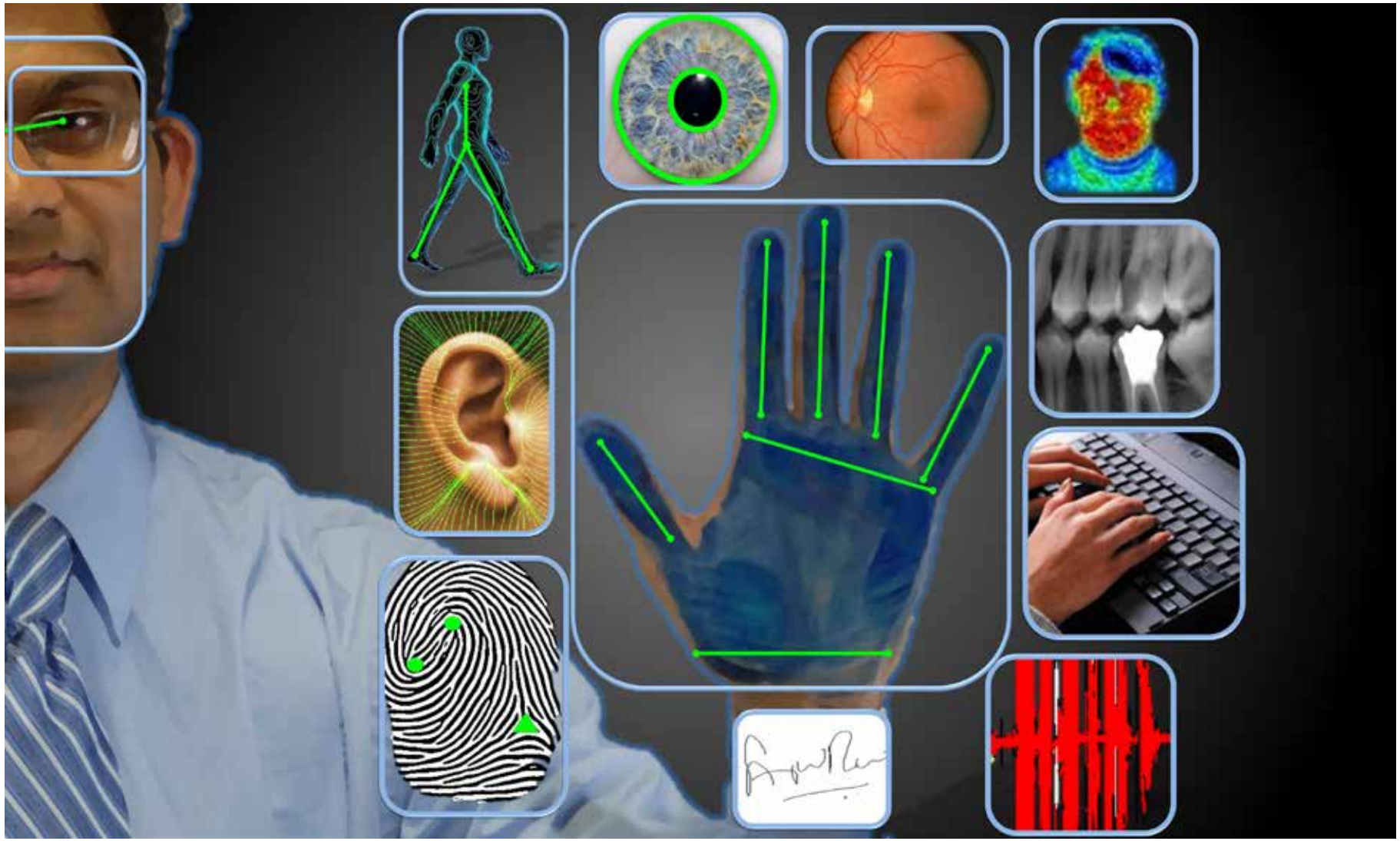
Биометрическая аутентификация. Аутентификация по лицу

Биометрическая аутентификация. Аутентификация по изображению глаза

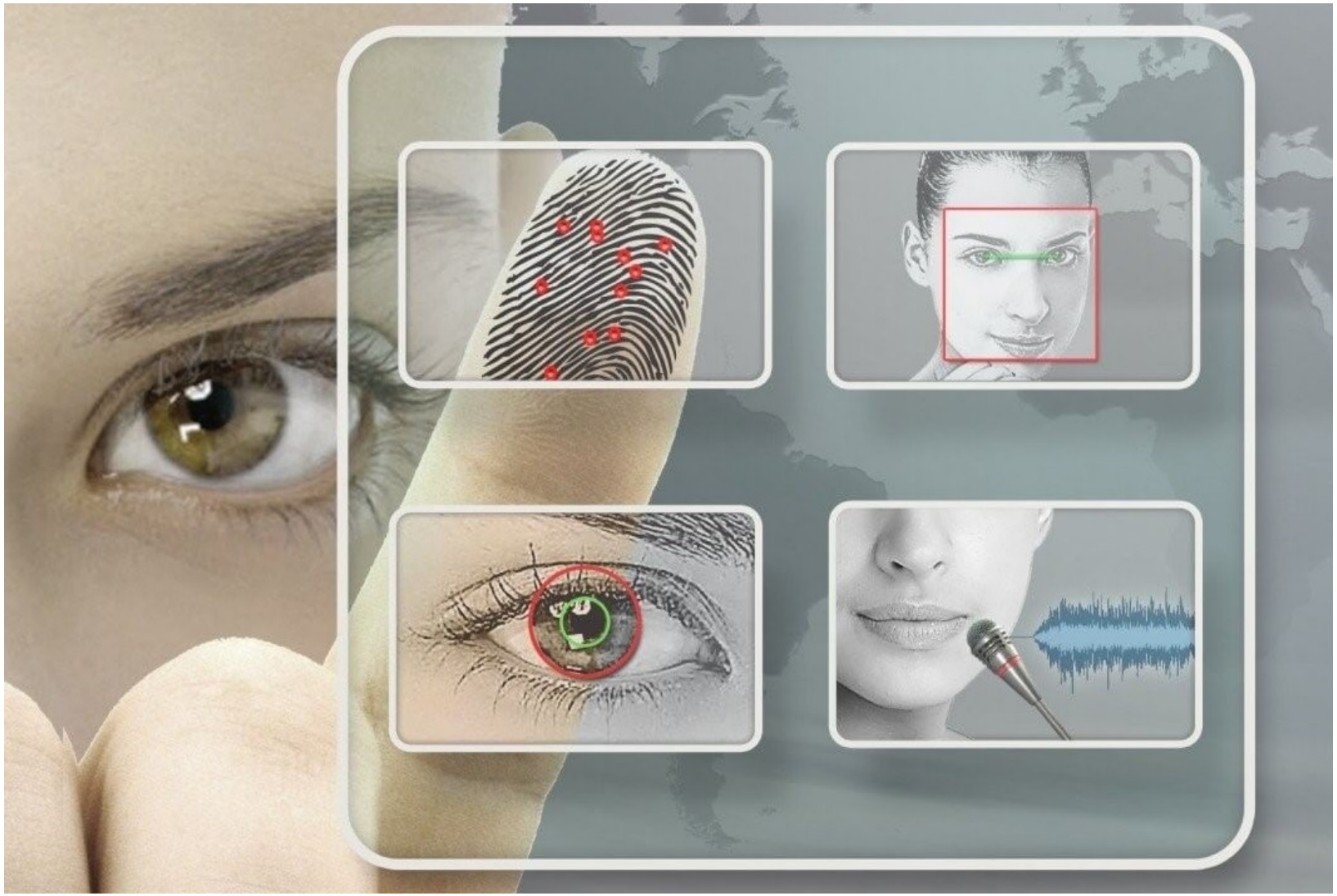
Биометрическая аутентификация. Аутентификация по голосу

Биометрическая аутентификация. Аутентификация по голосу

Комплексная аутентификация по нескольким признакам



Комплексная аутентификация по нескольким признакам



Комплексная аутентификация по нескольким признакам

Атаки на биометрические системы и защита от них

Атаки на биометрические системы и защита от них

Описание атаки	Защита от данной атаки
ПОДДЕЛКА ОТЛИЧИТЕЛЬНОЙ ЧЕРТЫ	
Злоумышленник изготавливает копию физической отличительной черты законного пользователя и предъявляет эту копию биометрическому датчику.	Снятие показателей с высоким уровнем детализации При изготовлении эталонного шаблона с законного пользователя снимают дополнительные биометрические показатели, так что простая копия физической отличительной черты законного пользователя не будет отражать все ее параметры.
ВОСПРОИЗВЕДЕНИЕ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ	
Злоумышленник записывает поведенческую отличительную черту пользователя и воспроизводит на биометрическом датчике.	Изменяемое поведение При каждой попытке аутентификации система требует от пользователя различного проявления его поведенческой биометрической характеристики, так что просто ее запись и воспроизведение не будут приниматься.

Атаки на биометрические системы и защита от них

Описание атаки	Защита от данной атаки
ПЕРЕХВАТ БИОМЕТРИЧЕСКИХ ПОКАЗАТЕЛЕЙ	
Злоумышленник перехватывает биометрические показатели законного пользователя в момент их передачи между устройствами.	Шифрование биометрических данных Биометрические данные шифруются сразу после их получения от пользователя устройством считывания, их передача между устройствами осуществляется только в шифрованном виде.
ВОСПРОИЗВЕДЕНИЕ БИОМЕТРИЧЕСКОЙ «ПОДПИСИ»	
Злоумышленник воспроизводит показатель биометрического датчика — «подпись», которая далее обрабатывается системой так, словно была получена от реального человека.	Аутентификация биометрической «подписи» Меры аутентификации принимаются в отношении биометрических данных, чем гарантируется их поступление только из заслуживающих доверия источников. Использование электронной цифровой подписи для обеспечения целостности биометрическом «подписи».

Биометрические документы


Биометрические
документы
Республики
Беларусь
ПАШПАРТ
ПАСПОРТ
PASSPORT

ID-КАРТА БЕЛОРУСА

ID-карта - документ, удостоверяющий личность, для пользования внутри страны.

Цифровой аналог паспорта будут выдавать с 1 сентября 2021 года.

Всего появится 8 новых видов документов, содержащих биометрические данные, в том числе идентификационная карта гражданина и биометрический паспорт.

Карта содержит

ПРЕИМУЩЕСТВА

- защита от подделок,
- удобство пользования,
- сокращение времени на административные процедуры,
- в перспективе с помощью ID-карты можно будет оплачивать услуги или платить налоги.

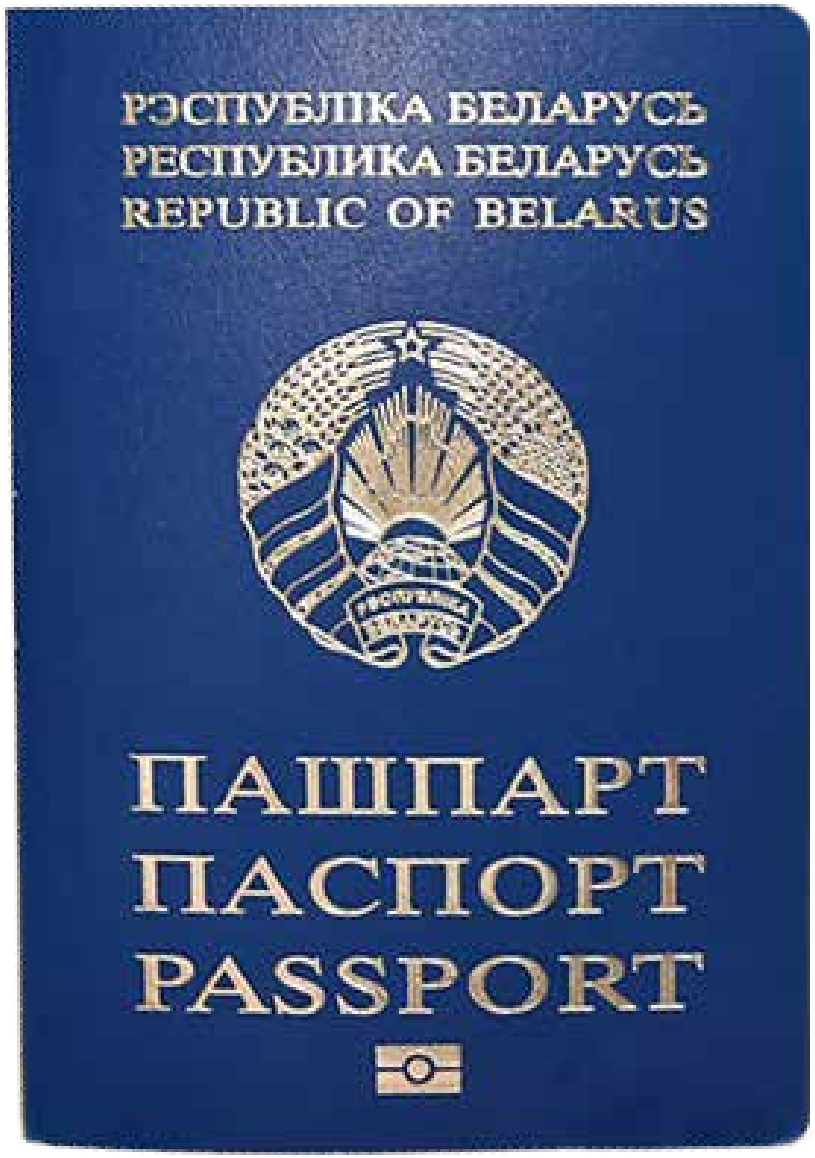
Биометрические документы
Образец идентификационной карты гражданина (ID-карта)

- **ID-карта будет содержать:**
- фотоизображение (цифровой фотопортрет) владельца;
- фамилию, собственное имя, отчество (если таковое имеется) владельца;
- число, месяц, год рождения владельца;
- пол владельца;
- место рождения владельца;
- гражданство (подданство) владельца (при наличии);
- идентификационный номер;
- вид документа;
- номер документа;
- код Республики Беларусь;
- число, месяц, год выдачи документа;
- код органа, выдавшего документ;
- число, месяц, год окончания срока действия документа;
- машиносчитываемую зону;
- изображение подписи владельца, достигшего четырнадцатилетнего возраста, либо иностранца, приобретшего дееспособность в полном объеме в соответствии с законодательством Республики Беларусь (за исключением случаев, когда отобрать образец подписи физически невозможно);
- двухмерный штрих-код (QR-код), содержащий закодированную информацию о владельце документа (фамилию, собственное имя, отчество (если таковое имеется), число, месяц, год рождения), информацию о документе (номер, число, месяц, год выдачи, число, месяц, год окончания срока действия) и идентификационный номер;
- интегральную микросхему, содержащую электронное средство биометрической идентификации с персональными данными владельца биометрического документа в соответствии с требованиями международной организации по гражданской авиации (ICAO) и криптографический токен аутентификации.

Биометрические документы
Образец идентификационной карты гражданина (ID-карта)

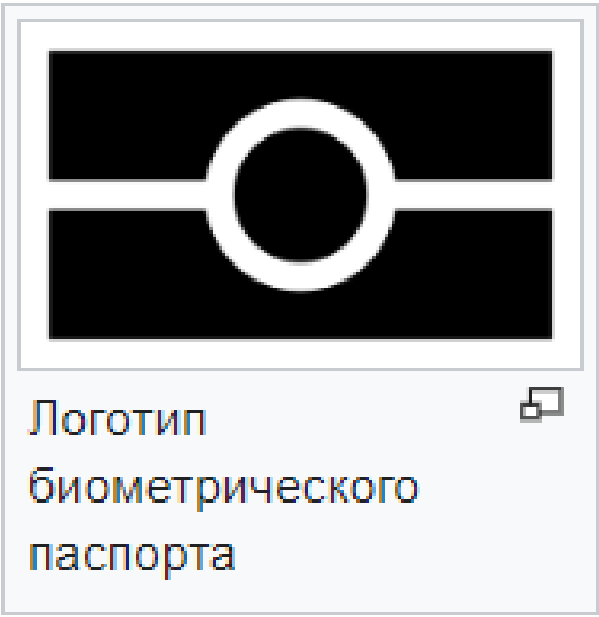
- **Интегральная микросхема (чип) ID-карты будет содержать:**
- 1. Криптографический токен аутентификации (КТА) – программное обеспечение с информацией о владельце (в соответствии с белорусскими стандартами) и для выработки электронно-цифровой подписи.
- КТА содержит следующие группы данных:
- a. DG1 идентификационный номер
- b. DG2- код страны, тип документа, номер ID-карты, дата выпуска, срок действия, код органа выдавшего документ, гражданство, место рождения.
- c. DG3- ФИО
- d. DG4- дата рождения
- e. DG5-пол
- 2. Программное обеспечение (ПО) ICAO – ПО с информацией о владельце в международном формате.

Образец биометрического паспорта



Образец биометрического паспорта

- Биометрический паспорт гражданина Республики Беларусь (далее – биометрический паспорт) – документ, подтверждающий гражданство и удостоверяющий личность владельца в целях выезда из Республики Беларусь и въезда в Республику Беларусь, а также пребывания и проживания за пределами Республики Беларусь;
  - фотоизображение владельца;
  - фамилию и собственное имя владельца;
  - число, месяц, год рождения владельца;
  - пол владельца;
  - место рождения владельца;
  - гражданство владельца (при наличии);
  - идентификационный номер;
  - номер документа;
  - вид документа;
  - код Республики Беларусь;
  - число, месяц, год выдачи документа;
  - код органа, выдавшего документ;
  - число, месяц, год окончания срока действия документа;
  - машиносчитываемую зону;



- В биометрический паспорт встроена интегральная микросхема (чип), содержащая электронное средство биометрической идентификации с персональными данными владельца биометрического документа в соответствии с требованиями международной организации по гражданской авиации (ICAO).

Официально о биометрических документах в Республике Беларусь

https://mpt.gov.by/ru/biometricheskie-dokumenty-respubliki-belarus

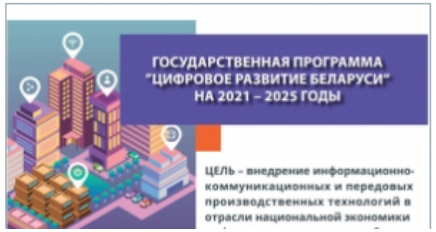
Министерство связи и информатизации Республики Беларусь

220050, г.Минск, пр-т Независимости, 10
Тел.: +375 (17) 287 87 06
Факс: +375 (17) 327 21 57

Рус Бел Eng

Главная | Новости | Министерство | Деятельность | Вниманию инвесторов | Статистика | Версия для слабовидящих

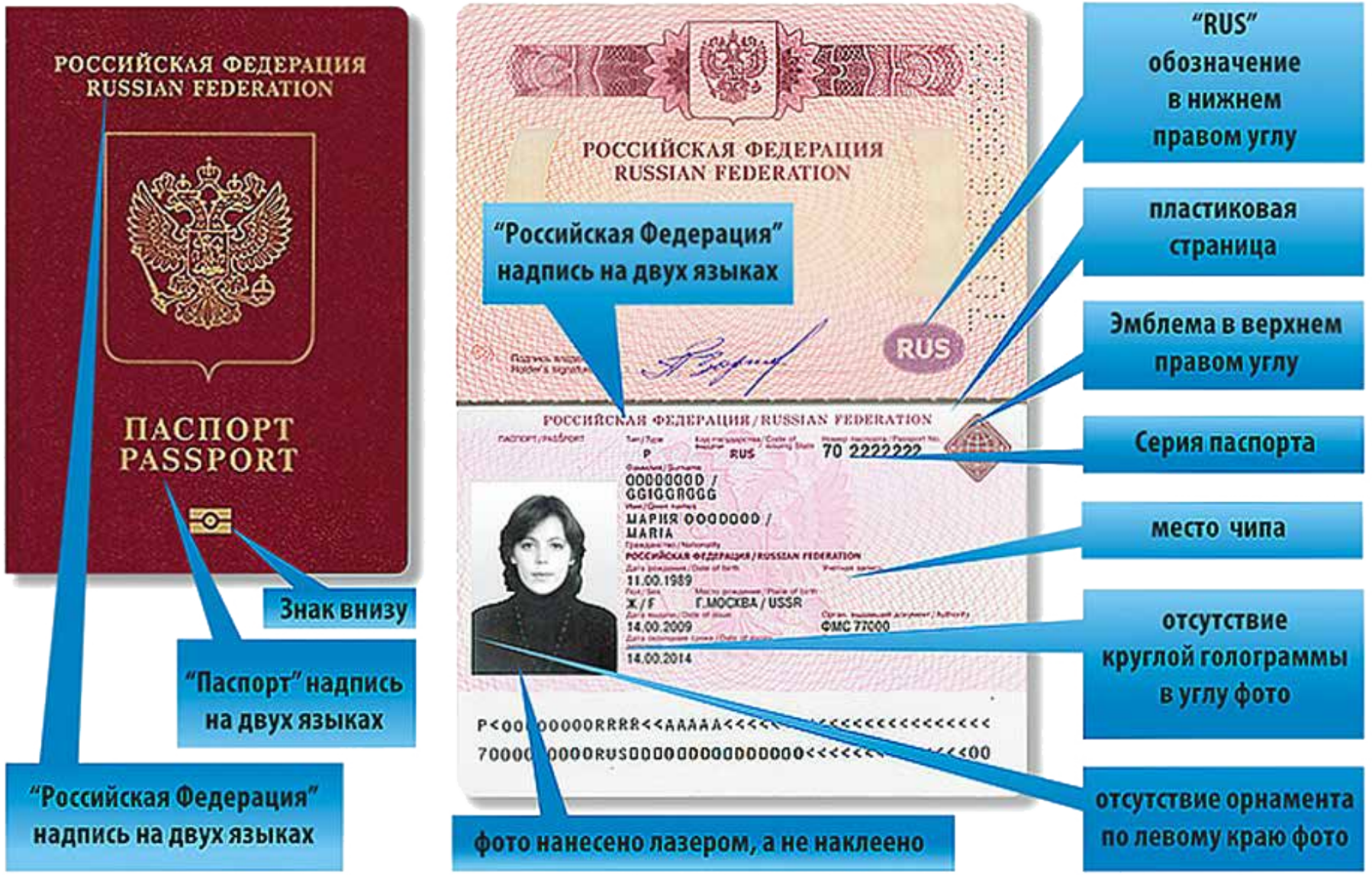
- График приема
- «Прямая телефонная линия»
- Электронные обращения
- Часто задаваемые вопросы
- Одно окно
- Пресс-центр



Белорусская интегрированная сервисно-расчетная система

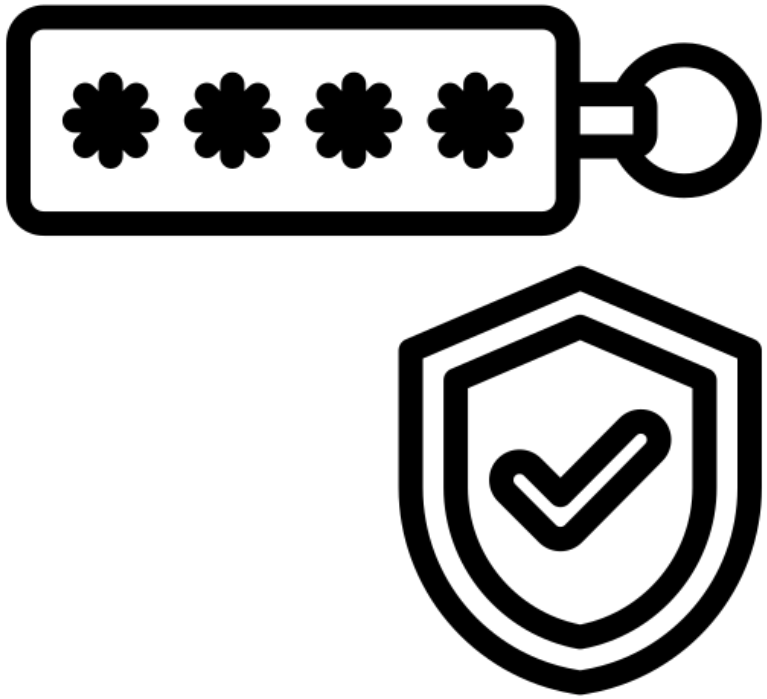
- О БИСРС
- Биометрические документы
- В соответствии с Указом Президента Республики Беларуси А.Г.Лукашенко №107 от 16 марта 2021 года биометрические документы в стране вводятся с 1 сентября 2021 года.
- Инфографика: ID-карта Белоруса
- Видеоролик об Идентификационной карте
- Алгоритмы организации рабочих мест к взаимодействию с идентификационными картами граждан
- Технические требования к считывателям ID-карт
- Потенциальные поставщики считывателей ID-карт
- Программное обеспечение для взаимодействия с системой идентификации (ЕС ИФЮЛ)
- Тестовые образцы ID-карт
- Семинар по вопросам внедрения и функционирования БИСРС, 9 сентября 2020 г. (Презентации)
- КОНТАКТНАЯ ИНФОРМАЦИЯ
- Видеоролик о получении биометрических документов
- Видеосюжет: Белорусские ID-карты: что это такое, зачем они нужны и когда их начнут выдавать
  - Видеосюжет «ID-карты и биометрические паспорта» из еженедельной программы Время высоких технологий на «ЯСНАе TV»

Биометрический паспорт Российской Федерации



Универсальная электронная карта в РФ

** - в случае выдачи универсальной электронной карты по заявлению гражданина*



Аутентификация с помощью одноразовых паролей

Аутентификация с использованием токенов

Одноразовые пароли (OTP, One-Time Passwords)

- **Одноразовые пароли (OTP, One-Time Passwords)** — динамическая аутентификационная информация, генерируемая для единичного использования с помощью аутентификационных устройств (программных или аппаратных).

- Одноразовый пароль действителен один раз в течение ограниченного времени и при перехвате такого пароля злоумышленник имеет ограниченную возможность представиться пользователем.

Одноразовые пароли (OTP, One-Time Passwords)

- **Преимущество одноразового пароля по сравнению со статическим состоит в том, что пароль невозможно использовать повторно.** Таким образом, злоумышленник, перехвативший данные из успешной сессии аутентификации, не может использовать скопированный пароль для получения доступа к защищаемой информационной системе.
- Использование одноразовых паролей само по себе не защищает от атак, основанных на активном вмешательстве в канал связи, используемый для аутентификации (например, от атак типа «человек посередине»).
- **Человек не в состоянии запомнить одноразовые пароли. Поэтому требуются дополнительные технологии для их корректной работы.**

Характеристика различных типов персональных идентификаторов

Продукт	Основные преимущества	Основные недостатки
OTP-токены	Мобильность. Легкость в использовании. Не требуется установка ПО пользователя	Ограниченный круг поддерживаемых приложений. Требуется сервер аутентификации. Ограниченное время эксплуатации в связи с использованием батарейки
USB-токены	Мобильность — токен можно использовать на любом компьютере, где есть USB-порт. Поддержка большого числа приложений ИТ-безопасности. Очевидная принадлежность токена пользователю	Требуется установка ПО пользователя
Смарт-карты	Высокий уровень безопасности. Компактность. Поддержка большого числа приложений	Требуется установка ПО пользователя. Требуется считывающее устройство
USB-токены со встроенным чипом	Высокий уровень безопасности. Мобильность. Поддержка большого числа приложений. Очевидная принадлежность токена пользователю	Требуется установка ПО пользователя
Гибридные токены	Мобильность. Поддержка большого числа приложений. Не требуется установка ПО пользователя для применения одноразовых паролей (OTP). Очевидная принадлежность токена пользователю	Ограниченное время эксплуатации в связи с использованием батарейки (кроме тех случаев, когда пользователь может заменить батарейку самостоятельно)
Программные токены	Не требуется аппаратное устройство	Секретный ключ слабо защищен. Ограниченный круг поддерживаемых приложений. Требуется сервер аутентификации

Одноразовые пароли (OTP, One-Time Passwords)

- **Чаще всего в качестве возможных устройств для генерации одноразовых паролей обычно используются OTP-токены.**
- **OTP-токен** — мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли, используемые для аутентификации данного пользователя.

- Таким образом, **аутентификация с помощью одноразовых паролей**, по сравнению с аутентификацией на основе пароля, является аутентификацией с помощью другого фактора аутентификации — **аутентификацией «на основе обладания чем-либо»**

Аппаратно-программные OTP-токены

- **OTP-токены имеют небольшой размер и выпускаются в виде:**
  - карманного калькулятора;
  - брелока;
  - смарт-карты;
  - устройства, комбинированного с USB-ключом;
  - специального программного обеспечения для карманных компьютеров, смартфонов, настольных компьютеров.

Аппаратный eToken **от компании** Aladdin Knowledge Systems

Токен

- **Токен (также аппаратный токен, USB-ключ, криптографический токен)** — компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т.д.
- **Как правило, это физическое устройство, используемое для упрощения аутентификации.**
- Также этот термин **может относиться и к программным токенам**, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам. Часто используется для несанкционированного доступа к аккаунту злоумышленниками.

Токены

- **Токены предназначены для электронного удостоверения личности (например, клиента, получающего доступ к банковскому счёту), при этом они могут использоваться как вместо пароля, так и вместе с ним. В некотором смысле токен — это электронный ключ для доступа к чему-либо.**
- Обычно аппаратные токены обладают небольшими размерами, что позволяет носить их в кармане или кошельке, часто они оформлены в виде брелоков. Некоторые предназначены для хранения криптографических ключей, таких как электронная подпись или биометрические данные (например, детали дактилоскопического узора). В одни встроена защита от взлома, в другие — мини-клавиатура для ввода PIN-кода или же просто кнопка вызова процедуры генерации и дисплей для вывода сгенерированного ключа. Токены обладают разъёмом USB, функциями RFID или беспроводным интерфейсом Bluetooth для передачи сгенерированной последовательности ключей на клиентскую систему.

Токен - JaCarta **ГОСТ**
Компания "Аладдин Р.Д."

Пример: Сценарий работы совместно со средством электронной подписи

https://www.aladdin-rd.ru/catalog/antifraud

Типы паролей

- Все токены содержат некоторые секретные сведения, которые используются для подтверждения личности. Есть четыре различных способа, в которых эта информация может быть использована:
- **Токен со статическим паролем.**
  - Устройство содержит пароль, который физически скрыт (не виден обладателю), но который передаётся для каждой аутентификации. Этот тип уязвим для атак повторного воспроизведения.
- **Токен с синхронно динамическим паролем.**
  - Устройство генерирует новый уникальный пароль с определённым интервалом времени. Токен и сервер должны быть синхронизированы, чтобы пароль был успешно принят.
- **Токен с асинхронным паролем.**
  - Одноразовый пароль генерируется без использования часов, с помощью шифра Вернама или другого криптографического алгоритма.
- **Токен вызов-ответ.**
  - Используя криптографию с открытым ключом, можно доказать владение частным ключом, не раскрывая его. Сервер аутентификации шифрует вызов (обычно случайное число или по крайней мере, данные с некоторыми случайными частями) с помощью открытого ключа. Устройство доказывает, что обладает копией соответствующего частного ключа, путём предоставления расшифрованного вызова.

Типы паролей

- **Одноразовые пароли, синхронизированные по времени**
  - Синхронизированные по времени одноразовые пароли постоянно меняются в установленное время, например, раз в минуту. Для этого должна существовать синхронизация между токеном клиента и сервером аутентификации. Для устройств, не подключённых к сети, эта синхронизация сделана до того, как клиент приобрёл токен. Другие типы токенов синхронизируются, когда токен вставляется в устройство ввода. Главная проблема с синхронизированными токенами состоит в том, что они могут рассинхронизоваться спустя какой-то большой период времени. Тем не менее, некоторые системы, такие как SecurID компании RSA, позволяют пользователю синхронизировать сервер с токеном путём ввода нескольких последовательных кодов доступа. Большинство из них не может иметь сменных батарей, следовательно, они имеют ограниченный срок службы.
- **Одноразовые пароли на основе математического алгоритма**
  - Другой тип одноразовых паролей использует сложный математический алгоритм, например, хеш-цепи, для создания серии одноразовых паролей из секретного ключа. Ни один из паролей нельзя отгадать, даже тогда, когда предыдущие пароли известны. Существует общедоступный, стандартизированный алгоритм OATH; другие алгоритмы покрыты американскими патентами. Каждый новый пароль должен быть уникальным, поэтому неавторизованный пользователь по ранее использованным паролям не сможет догадаться, каким может быть новый пароль.

Типы токенов авторизации

- Токены авторизации различаются по типам. Рассмотрим их:
  - **Устройства, которые необходимо подключить физически.** Например: ключи, диски и тому подобные. Тот, кто когда-либо использовал USB-устройство или смарт-карту для входа в систему, сталкивался с подключенным токеном.
  - **Устройства, которые находятся достаточно близко к серверу**, чтобы установить с ним соединение, но оно не подключаются физически. Примером такого типа токенов может служить "magic ring" от компании Microsoft.
  - **устройства, которые могут взаимодействовать с сервером на больших расстояниях.**
- Во всех трех случаях пользователь должен что-то сделать, чтобы запустить процесс. Например, ввести пароль или ответить на вопрос. Но даже когда эти шаги совершаются без ошибок, доступ без токена получить невозможно.

Пример процесса токен авторизации

- **Авторизация с помощью токена происходит следующим образом.**

1. Сначала человек запрашивает доступ к серверу или защищенному ресурсу. Запрос обычно включает в себя ввод логина и пароля.
2. Затем сервер определяет, может ли пользователь получить доступ.
3. После этого сервер взаимодействует с устройством: ключ, телефон, USB или что-то ещё.
4. После проверки сервер выдает токен и отправляет пользователю. Токен находится в браузере, пока работа продолжается.
5. Если пользователь попытается посетить другую часть сервера, токен опять связывается с ним. Доступ предоставляется или, наоборот, запрещается на основе выданного токена.

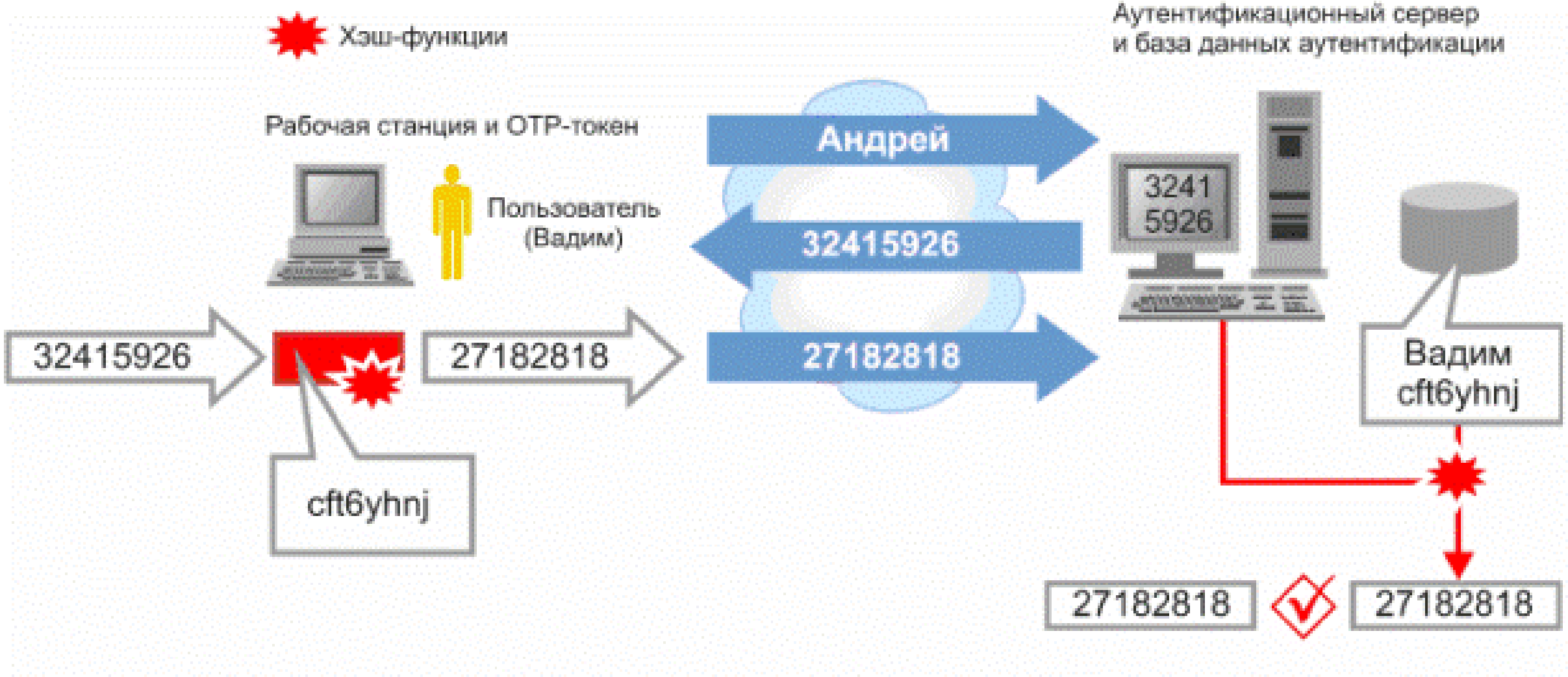
- Администраторы устанавливают ограничения на токены. Можно разрешить одноразовый токен, который немедленно уничтожается, когда человек выходит из системы. Иногда устанавливается маркер на самоуничтожение в конце определенного периода времени.

Методы аутентификации с помощью токенов

- **OTP-токены**, использующие симметричную криптографию, могут работать в асинхронном или синхронном режиме.

- Соответственно методы, используемые токенами можно разделить на две группы, работающие:
  - **в асинхронном режиме** («запрос-ответ»)
  - **в синхронном режиме** («только ответ», «синхронизация по времени», «синхронизация по событию»).

Метод «Запрос—ответ»

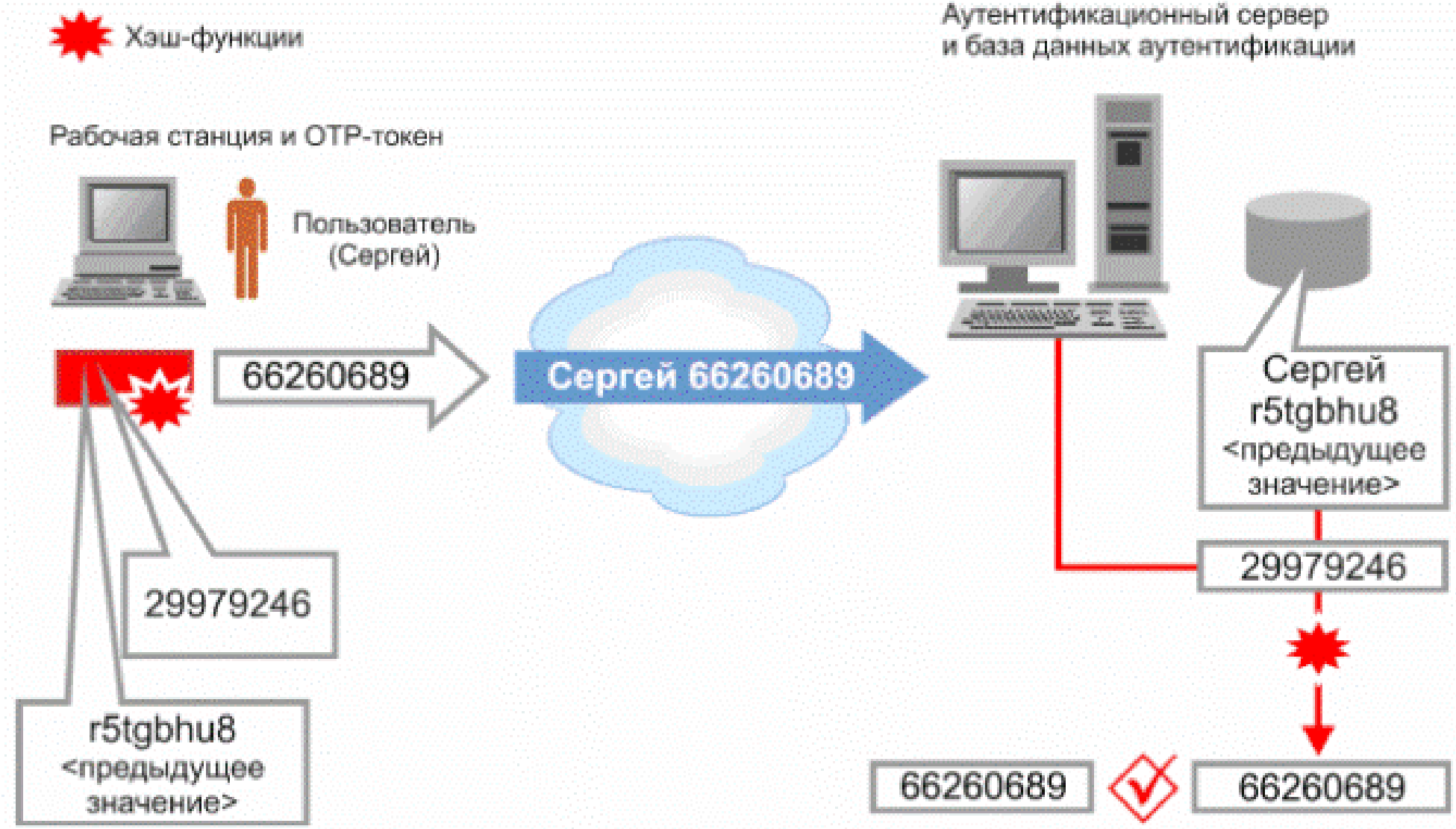


В методе «запрос—ответ» OTP является ответом пользователя на случайный запрос от сервера аутентификации

Метод «Запрос—ответ»

- Пример аутентификации пользователя при использовании OTP-токеном метода «запрос-ответ»:
  1. Пользователь вводит свое имя пользователя на рабочей станции.
  2. Имя пользователя передается по сети в открытом виде.
  3. Сервер аутентификации генерирует случайный запрос («31415926»)
  4. Запрос передается по сети в открытом виде.
  5. Пользователь вводит запрос в свой OTP-токен.
  6. OTP-токен шифрует запрос с помощью секретного ключа пользователя («cft6yhnj»), в результате получается ответ («27182818»), который отображается на экране OTP-токена.
  7. Пользователь вводит этот ответ на рабочей станции.
  8. Ответ передается по сети в открытом виде.
  9. Аутентификационный сервер находит запись пользователя в аутентификационной базе данных и с помощью хранимого им секретного ключа пользователя зашифровывает тот же запрос.
  10. Сервер сравнивает представленный ответ от пользователя («27182818») с вычисленным им самим ответом («27182818»).
  11. При совпадении значений аутентификация считается успешной.

Метод «только ответ» (Response only)



Метод «только ответ» (Response only)

- В методе «только ответ» аутентификационное устройство и сервер аутентификации генерируют «скрытый» запрос, используя значения предыдущего запроса Для начальной инициализации данного процесса используется уникальное случайное начальное значение, генерируемое при инициализации OTP-токена.
- Пример аутентификации пользователя при использовании OTP-токеном метода «только ответ»:
  1. Пользователь активизирует свой OTP-токен, который вычисляет и отображает ответ на «скрытый» запрос.
  2. Пользователь вводит свое «имя пользователя» и этот ответ («66260689») на рабочей станции.
  3. Имя пользователя и ответ («66260689») передаются по сети в открытом виде
  4. Сервер находит запись пользователя, генерирует такой же скрытый запрос и шифрует его с помощью секретного ключа пользователя, получая ответ на свои запрос
  5. Сервер сравнивает представленный ответ от пользователя («66260689») с вычисленным им самим ответом («66260689»).
  6. При совпадении значений аутентификация считается успешной.

Метод «Синхронизация по времени» (Time synchronous)

Метод «Синхронизация по времени» (Time synchronous)

- В режиме «синхронизация по времени» аутентификационное устройство и аутентификационный сервер генерируют OTP на основе значения внутренних часов. OTP-токен может использовать не стандартные интервалы времени, измеряемые в минутах, а специальные интервалы времени обычно равные 30 с.
- Пример аутентификации пользователя при использовании OTP-токеном метода «синхронизация по времени»:

1 Пользователь активизирует свой OTP-токен, который генерирует OTP («96823030»), зашифровывая показания часов с помощью своего секретного ключа.

2. Пользователь вводит свое «имя пользователя» и этот OTP на рабочей станции

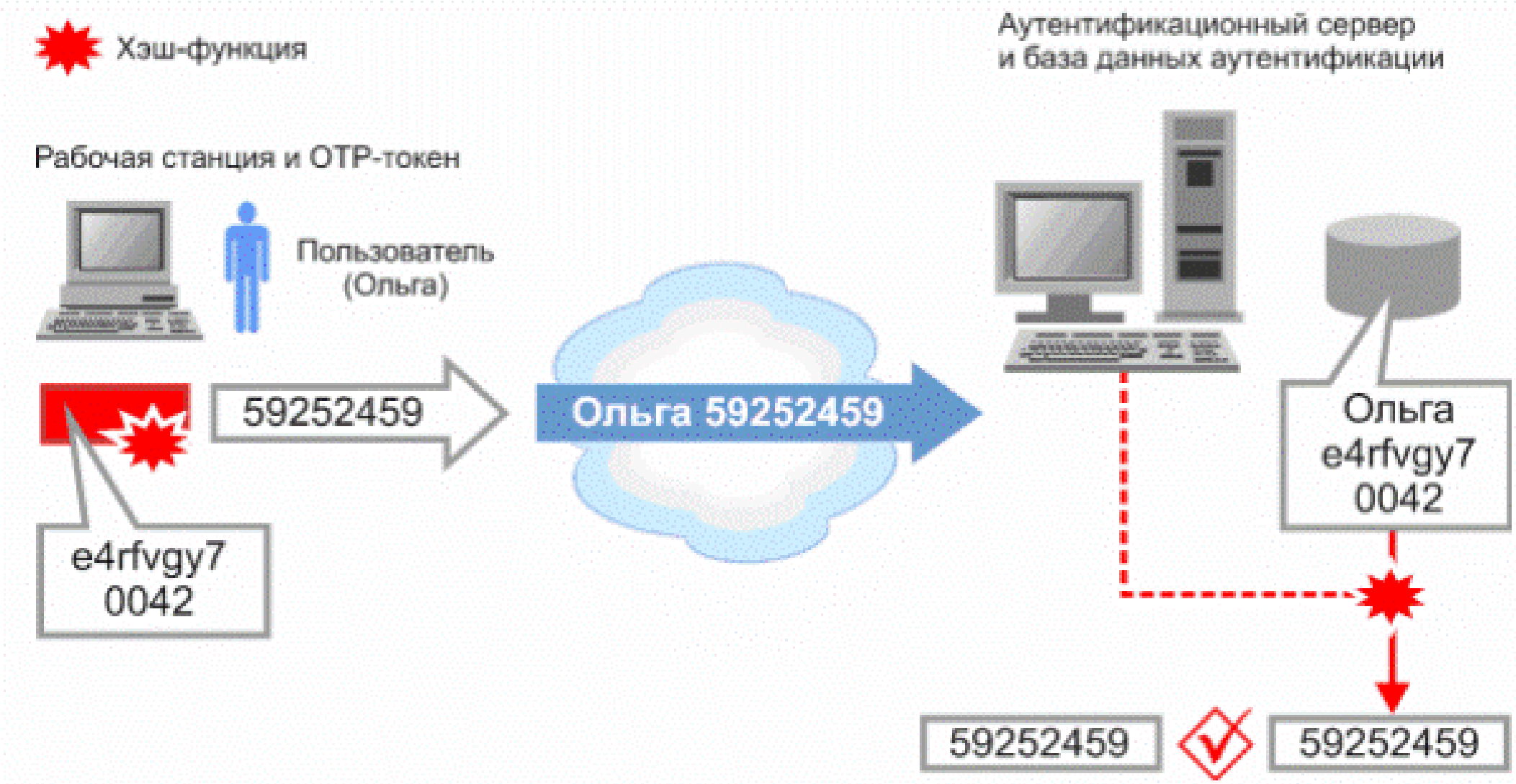
3. Имя пользователя и OTP передаются по сети в открытом виде.

4. Аутентификационный сервер находит запись пользователя и шифрует показание своих часов с помощью хранимого им секретного ключа пользователя, получая в результате OTP.

5. Сервер сравнивает OTP, представленный пользователем, и OTP, вычисленный им самим.

6. При совпадении значений аутентификация считается успешной.

Метод «синхронизация по событию» (Event synchronous)



Метод «синхронизация по событию» (Event synchronous)

- В режиме «синхронизация по событию» OTP-токен и сервер аутентификации ведут количественный учет прохождения аутентификации данным пользователем, и на основе этого числа генерируют OTP.
- Пример аутентификации пользователя при использовании OTP-токеном метода «синхронизация по событию»:

1. Пользователь активизирует свой OTP-токен, который генерирует OTP («59252459») зашифровывая число раз прохождения аутентификации данного пользователя с помощью своего секретного ключа.
2. Пользователь вводит свое «имя пользователя» и этот OTP на рабочей станции.
3. Имя пользователя и OTP передаются по сети в открытом виде
4. Аутентификационный сервер находит запись пользователя и шифрует значение числа раз прохождения аутентификации данного пользователя с помощью хранимого им секретного ключа пользователя, получая в результате OTP.
5. Сервер сравнивает OTP, представленный пользователем, и OTP, вычисленный им самим.
6. При совпадении значений аутентификация считается успешной

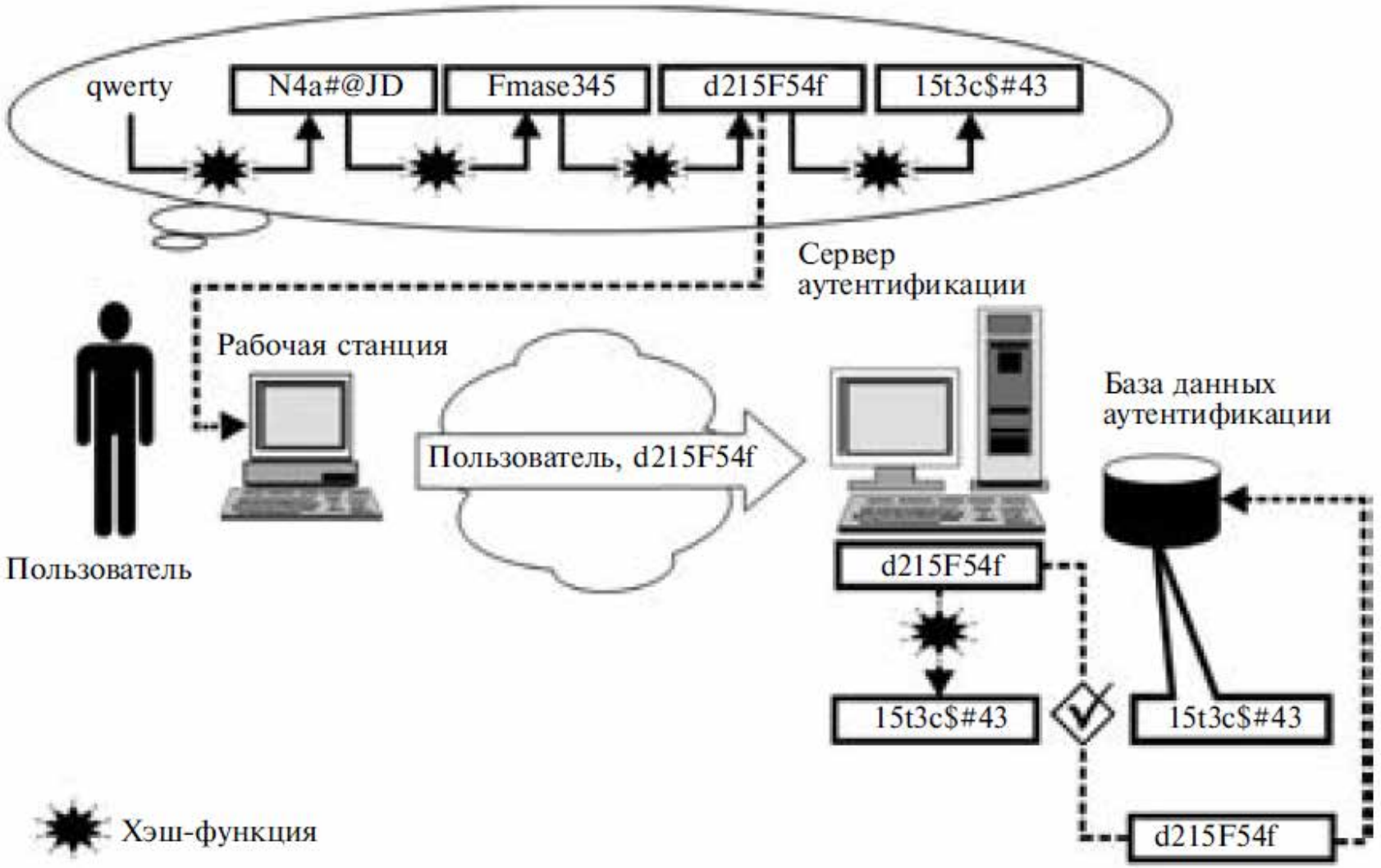
Сравнение методов OTP-аутентификации

- Метод «запрос—ответ», работающий в асинхронном режиме, предполагает большее количество шагов, совершаемых пользователем, чем любой из синхронных режимов.
- **Потенциальная проблема всех методов реализации аутентификации с помощью OTP, работающих в синхронном режиме, — возможность рассинхронизации OTP-токена и сервера**, например:
  - в режимах «только ответ» или «синхронизации по событию» сбой при аутентификации может привести к «отставанию» сервера от аутентификационного устройства;
  - в режиме «синхронизации по времени» часы аутентификационного устройства могут уйти вперед или отстать от часов сервера.
- При аутентификации с помощью OTP-токенов, как правило, предусматривается вариант решения проблемы рассинхронизации: сервер генерирует несколько возможных вариантов OTP — «ответов» от пользователя за некоторый короткий промежуток времени (для нескольких событий или единиц измерения времени).

Системы одноразовых паролей
Система S/Key

- **Система S/Key**— система одноразовых паролей, разработанная в Беллкоре (Bell Communication Research Labs, Bellcore Labs) в начале 1990-х гг. в качестве метода регистрации для UNIX-систем.
- Техническая концепция была впервые предложена Лесли Лэмпортом (Leslie Lamport) и опубликована в 1981 г. **Основное отличие подхода Лэмпорта от других методик на основе принципа «запрос—ответ» состояло в том, что не было базы данных секретных ключей**, поэтому взломщики не могли поставить под угрозу работу системы, украв эту базу данных.
- В схеме Лэмпорта **используется последовательность значений односторонних хэш-функций, вычисляемых из базового секрета.** Как и в случае традиционной парольной аутентификации в UNIX-системах, в схеме Лэмпорта использован тот факт, что вычисление хэшированного значения пароля не представляет сложности, а вот обратное получение пароля по значению хэша невозможно. В схеме Лэмпорта используется последовательность значений хэш-функции, каждое из которых вычисляется из предыдущего члена последовательности. Сервер хранит последнее значение хэш-функции в последовательности.

Системы одноразовых паролей Система S/Key (схема Лэмпорта)



Системы одноразовых паролей Система S/Key (схема Лэмпорта)

- Схему Лэмпорта можно представить в виде последовательности следующих шагов:

  1. Четыре раза последовательно вычисляется значение хэш-функции базового секрета пользователя. Конечный результат этих вычислений сохраняется в базе данных аутентификации, а промежуточные выдаются пользователю либо повторно вычисляются им при каждом акте аутентификации.

  2. Пользователь в качестве одноразового пароля предоставляет предпоследнее в последовательности значение хэш-функции.

  3. Сервер принимает одноразовый пароль, вычисляет значение хэш-функции и сравнивает со значением хэш-функции, хранящимся в базе данных аутентификации. Эти значения должны совпасть.

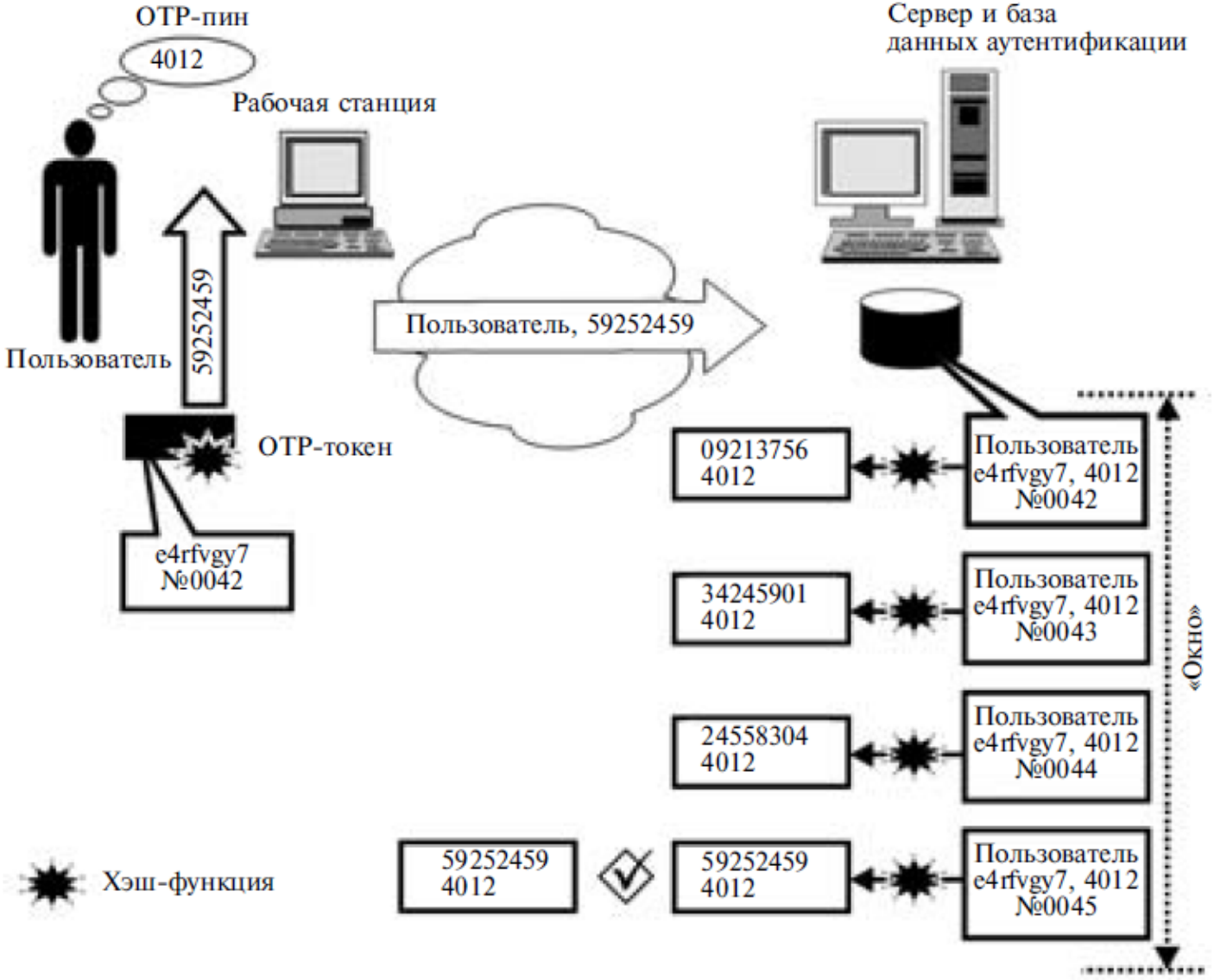
  4. При совпадении (успешной аутентификации) сервер заменяет значение хэш-функции в учетной записи пользователя (четвертое значение хэш-функции) значением пароля, только что принятым от пользователя (третьим значением хэш-функции). При следующем входе пользователя в систему он должен предоставить второе значение хэш-функции, а при последнем входе — первое значение.

- Схема Лэмпорга реализована в системе S/Key.
- Как правило, пользователи системы S/Key используют для генерации одноразовых паролей программно реализованные OTP-токены.

Системы одноразовых паролей Группа OATH и система HOTP

- **Система HOTP (HMAC-basest One-Time Password System)** была разработана в 2005 г. в рамках инициативы группы открытой аутентификации **OATH** (Open AuTHentification) и описана в документе RFC 4226. **Данная система основана на концепции OTP-аутентификации с синхронизацией по событию.** Для генерации одноразового пароля используется алгоритм HMAC (Hashed Message Authentication Code).
- Система HOTP предусматривает возможность задания «окна» попыток аутентификации и синхронизацию сервера аутентификации с OTP-токеном после успешного про хождения аутентификации.

Системы одноразовых паролей Группа OATH и система HOTP

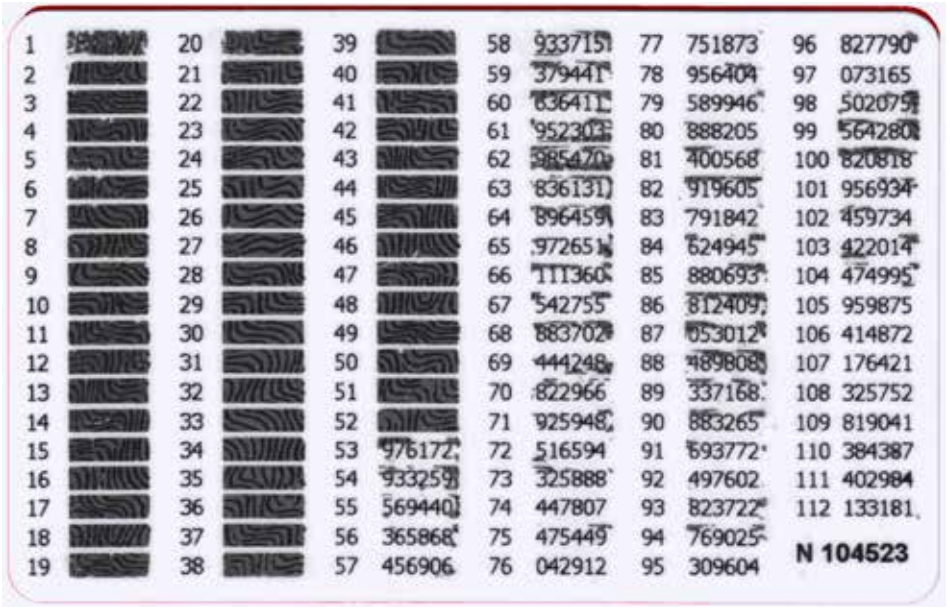


Системы одноразовых паролей Группа OATH и система HOTP

- Пример аутентификации пользователя с помощью HOTP:
  - 1. Пользователь генерирует значение HOTP с использованием хранимого на OTP-токене значения числа раз прохождения аутентификации и секретного ключа (592524594012).
  - 2. Пользователь вводит свое «имя пользователя» и OTP на рабочей станции.
  - 3. Имя пользователя и OTP (592524594012) передаются по сети в открытом виде.
  - 4. Аутентификационный сервер находит запись пользователя и генерирует OTP, используя хранимые на сервере значения числа раз прохождения аутентификации данного пользователя и секретного ключа пользователя и получая в результате OTP (592524594012).
  - 5. Сервер сравнивает OTP, представленный от пользователя, и OTP, вычисленный им самим.
    - a. Если значения не совпадают, сервер увеличивает значение числа раз прохождения аутентификации пользователя на единицу и повторяет попытку.
    - b. Если значения совпадают — на сервере сохраняется новое значение числа раз прохождения аутентификации пользователя.
    - Аутентификация считается успешной.
    - c. Если достигнуто максимальное число неуспешных повторов процедуры аутентификации (задаваемое шириной «окна»), аутентификация считается неуспешной.

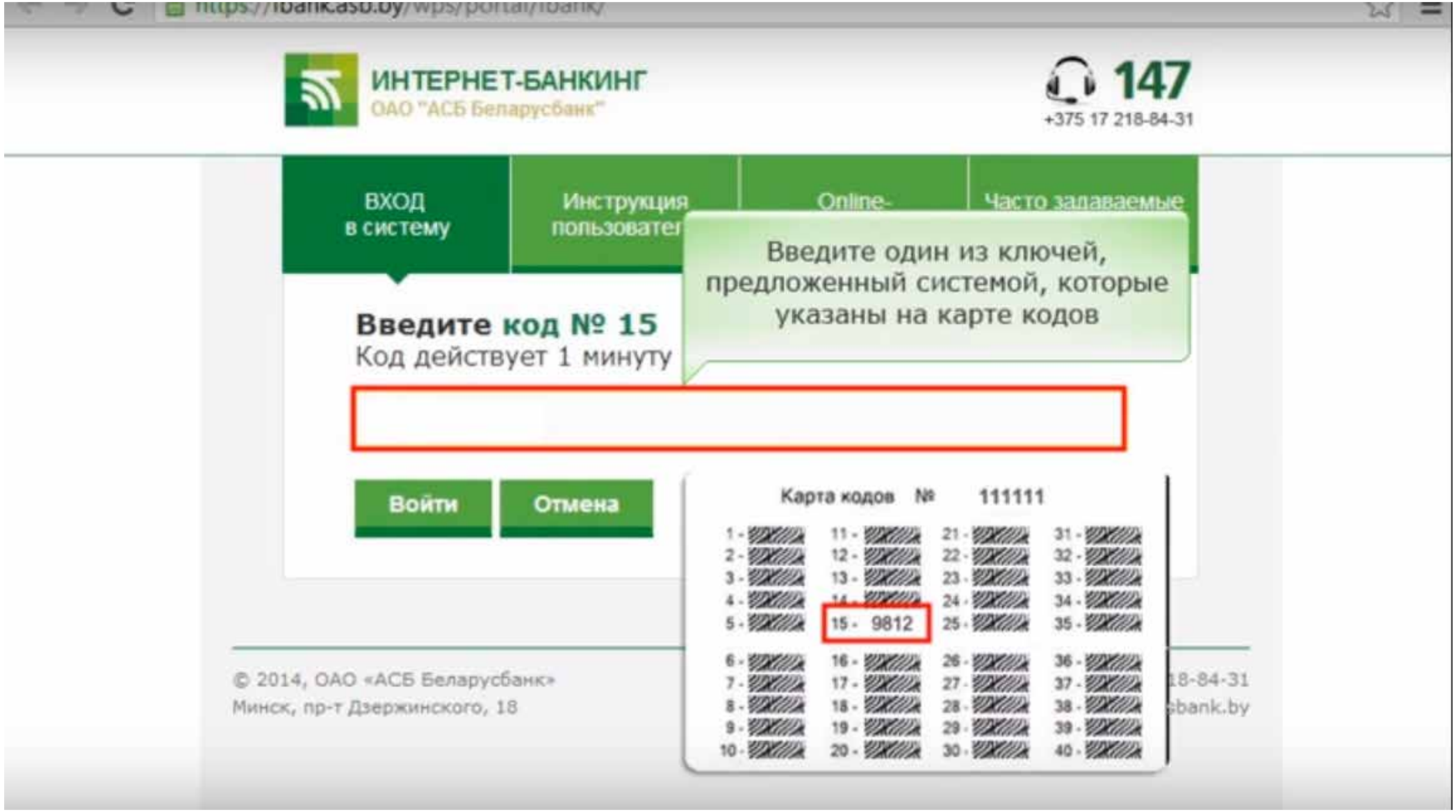
OTP в рамках банковского дела

- В некоторых странах одноразовые пароли используются для удалённого использования банков.
- **В некоторых из этих систем банк посылает пользователю пронумерованный список одноразовых паролей, напечатанный на бумаге или в виде пластиковой карты с одноразовыми паролями.**
- Для каждой удалённой транзакции пользователь должен ввести соответствующий одноразовый пароль из этого списка.
- В Германии эти пароли обычно называют TAN-кодом (от «transaction authentication numbers»). Некоторые банки отправляют TAN-коды пользователю с помощью SMS, и в этом случае они называются mTAN-коды (от «mobile TANs»).



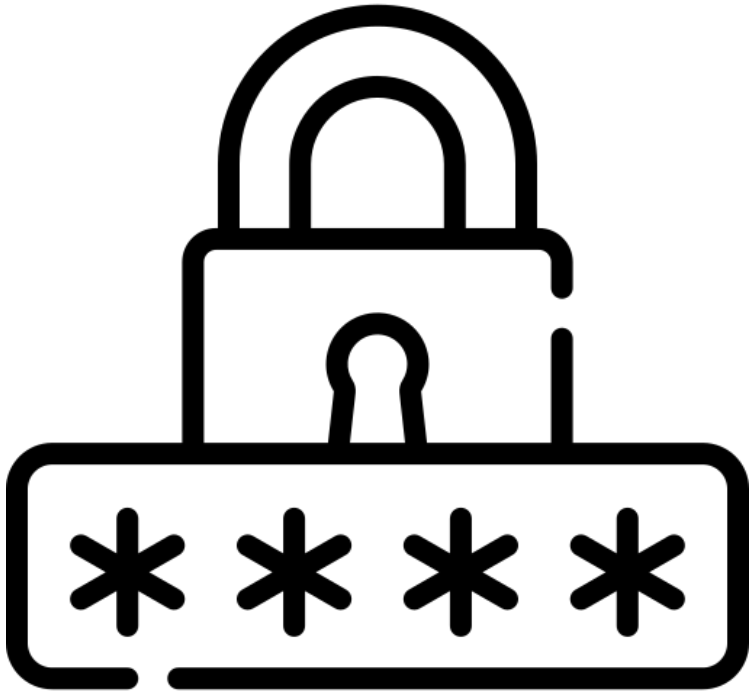
Скретч-карта банка ВТБ24
с одноразовыми паролями

OTP в рамках банковского дела



OTP в рамках интернет платежей

- **Чаще всего одноразовые пароли являются олицетворением двухфакторной аутентификации**, например при онлайн покупках когда при осуществлении платежа банк дополнительно проверяет подлинность владельца карты при помощи **одноразового пароля через SMS.**
- SMS — это повсеместный канал связи, который имеется во всех телефонах и используется большим количеством клиентов, SMS-сообщения имеют наибольший потенциал для всех потребителей, обладающие низкой себестоимостью.



Недостатки методов аутентификации с помощью OTP (One-Time Passwords). Возможные атаки

Атаки на одноразовые пароли и защита от них

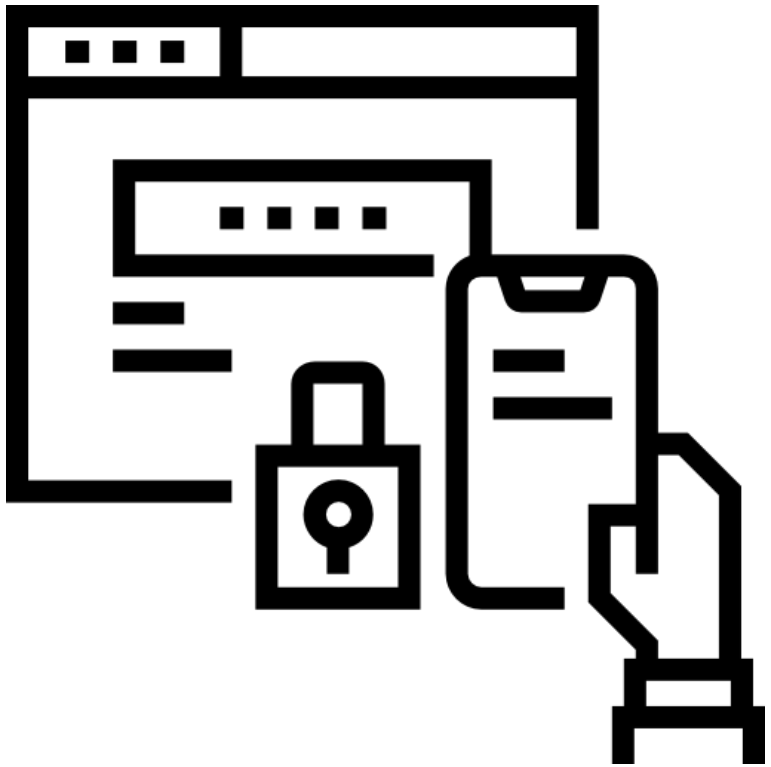
Описание атаки	Защита от данной атаки
Атака «Человек посередине»	
Злоумышленник перехватывает одноразовый пароль, посланный законным пользователем при аутентификации, блокирует законного пользователя и использует перехваченный пароль для входа в систему.	Использование метода «запрос—ответ» Использование вместо синхронных одноразовых паролей, имеющих легитимность «в продолжительном» периоде времени, одноразовых паролей, работающих по принципу «запрос-ответ». Каждое повое соединение требует выполнения аутентификании заново.
Кража аутентификационного токена	
Злоумышленник похищает аутентификационный токен законного пользователя и использует его для входа в систему.	PIN-коды в аутентификационных токенах Использование аутентификационных токенов, требующих от владельца ввода PIN-кода перед началом генерации OTP.
Подбор PIN-кода аутентификационного токена	
Злоумышленник вручную производит перебор всех возможных значений PIN-кода похищенного им аутентификационного токена законного пользователя.	Блокирование после ввода неправильного PIN-кода Аутентификационный токен отключается после того, как пользователь вводит неправильное значение PIN-кода подряд более заданного количества раз. Увеличение задержки для каждого ввода неправильного PIN-кода Если вводится неправильное значение PIN-кода, то следующая попытка ввода PIN-кода возможна только через определенный промежуток времени, с каждым неправильным вводом эта задержка увеличивается.

Атаки на одноразовые пароли и защита от них

Описание атаки	Защита от данной атаки
Извинение значения секретного ключа из программного аутентификационного токена	
Злоумышленник копирует программный аутентификационный токен (программное обеспечение), пытается найти в нем хранимый секретный ключ, чтобы потом его использовать для аутентификации под видом законного пользователя	PIN-код является частью секретного ключа Частью секретного ключа аутентификационного токена является PIN-код, без его знания нельзя сгенерировать правильный OTP, даже зная часть секретного ключа, который хранится в программном аутентификационном токене.
Подбор PIN-кода аутентификационного токена с помощью известных OTP	
Злоумышленник перехватывает несколько правильных OTP, использованных для входа в систему, копирует программный аутентификационный токен (программное обеспечение), затем он пытается подобрать PIN-код путем перебора его возможных значений, для тестирования пробного значения PIN-кода используются перехваченные OTP.	Использование «аппаратных» аутентификационных токенов В этом случае достаточно сложно произвести «вреальные сроки» перебор возможных значений PIN-кода до момента обнаружения владельцем пропажи токена и «информирования аутентификационного сервера» о том, что данный токен может быть использован злоумышленником.

Атаки на одноразовые пароли и защита от них

Описание атаки	Защита от данной атаки
Нечестный администратор аутентификационных токенов	
Злоумышленник является доверенным лицом либо является посредником доверенного лица, производящего инициализацию аутентификационного устройства до передачи его владельцу. Он может создать дубликат токена и, используя его, выдавать себя за владельца.	Разделение ответственности при инициализации аутентификационных токенов. В процессе программирования и активирования токена должны участвовать двое или более людей, каждый из которых выполняет строго ограниченный набор операций.



Применение криптографических алгоритмов при идентификации и аутентификации

Общие сведения о криптографии с открытым ключом

- В криптографии с открытым ключом (асимметричная криптография) алгоритмы используют связанные между собой пары ключей, состоящие из открытого и закрытого ключа.
- Для каждого человека или объекта генерируется **ключевая пара**:
  - **открытый ключ**, доступный для всех;
  - **закрытый ключ** известный только человеку, которому он выдан, и никому другому не раскрывается и никуда не передается.

- Информация зашифрованная с помощью одного ключа из ключевой пары, может быть расшифрована только с помощью другого ключа из этой же пары. Ключи математически связаны между собой так, что, зная открытый ключ, практически невозможно вычислить закрытый. Пользователь может повсеместно распространять свой открытый ключ, но он должен обязательно защищать свой закрытый ключ.

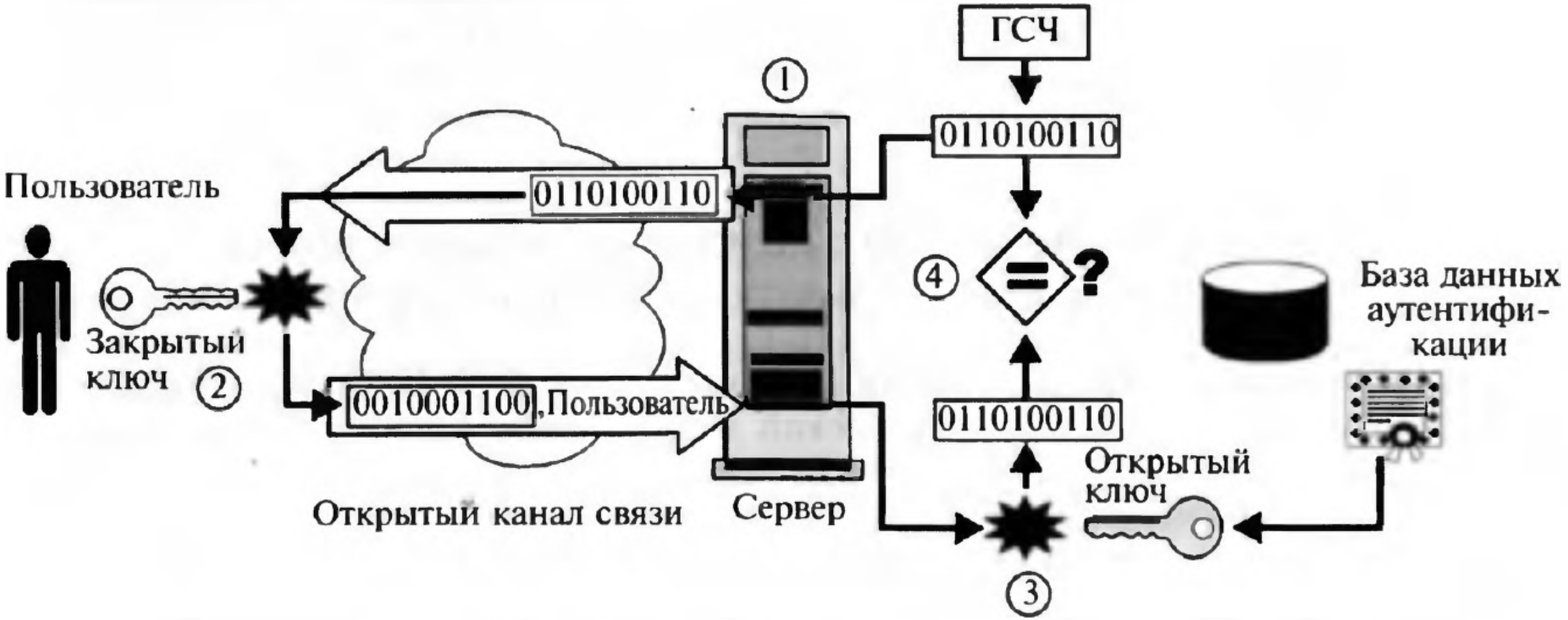
Общие сведения о криптографии с открытым ключом

- Криптографические методы защиты используют операцию преобразования информации. которая может выполняться одним или несколькими пользователями, обладающими некоторым секретом, без знания которого (с вероятностью, близкой к единице за разумное время) невозможно осуществить эту операцию
- **К криптографическим методам защиты в общем случае относятся:**
  - **шифрование информации** (термин шифрование объединяет в себе два процесса: зашифровывание и расшифровывание информации);
  - формирование и проверка **цифровой подписи** электронных документов.

Пример использования криптографии с открытым ключом для электронной цифровой подписи

Электронная цифровая подпись (ЭЦП) — это реквизит электронного документа, который предназначен для зашиты данного электронного документа от подделки, получен в результате криптографического преобразования информации с помощью закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Аутентификация с помощью открытого ключа (упрощенный вариант)

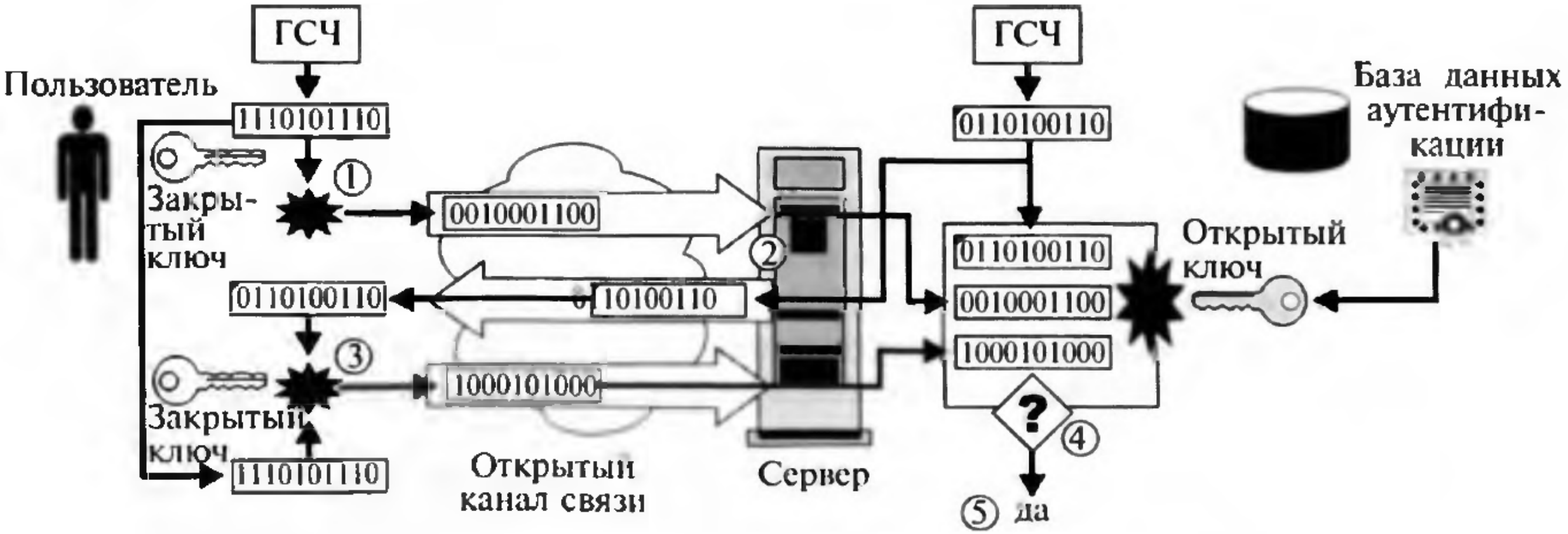


Аутентификация с помощью открытого ключа (упрощенный вариант)

- Аутентификационный сервер хранит файл открытых ключей всех пользователей, а все пользователи хранят свои закрытые ключи.
- **Пример аутентификации пользователя с помощью открытых ключей (упрощенный вариант):**
  - 1. **Сервер** посылает пользователю случайную строку, созданную генератором случайных чисел (ГСЧ).
  - 2. **Пользователь** шифрует эту строку своим закрытым ключом и посылает ее обратно серверу вместе со своим именем.
  - 3. **Сервер** находит в базе данных открытый ключ пользователя и расшифровывает сообщение, используя этот открытый ключ.
  - 4. Если отправленная и расшифрованная строки совпадают, **сервер** предоставляет пользователю доступ к системе.

- Никто другой не может воспользоваться закрытым ключом Пользователя следовательно, никто не сможет выдать себя за него. Что более важно, Пользователь никогда не посылает на компьютер свой закрытый ключ. Злоумышленник, перехватывая сообщения, не получит никаких сведений, которые позволили бы ему вычислить закрытый ключ Пользователя и выдать себя за него.
- В данной процедуре на шаге 1 производится шифрование «случайной строки, присланной от сервера», что служит потенциальной уязвимостью процедуры, так как этим может воспользоваться злоумышленник для взлома данного протокола с помощью подобранного шифртекста.

Аутентификация с помощью открытого ключа (сложный вариант)



Аутентификация с помощью открытого ключа (сложный вариант)

- Безопасные идентификационные протоколы имеют более сложную форму:
  - 1. **Пользователь** выполняет вычисление, основанное на некоторых случайных числах в своем закрытом ключе, и посылает результат серверу.
  - 2. **Сервер** посылает другое случайное число.
  - 3. **Пользователь** выполняет некоторое вычисление, основанное на случайных числах (как созданных им. так и полученных от сервера) в своем закрытом ключе, и посылает результат серверу.
  - 4. **Сервер** выполняет некоторое вычисление для различных чисел, полученных от Пользователя, и его открытого ключа, проверяя, что Пользователю известен его закрытый ключ.
  - 5. Если проверка завершается успешно, личность Пользователя подтверждается.
- В этом случае шаг 1 позволяет защитить протокол от вскрытия с помощью подобранного шифртекста.
- Данный протокол широко используется, если криптография с открытым ключом применяется в рамках одного небольшого предприятия, когда число пользователей невелико. Если же криптографию с открытым ключом используют для большого числа пользователей или нескольких предприятий, необходимо иметь инфраструктуру для управления ключами.

Инфраструктура открытых ключей (PKI)

- Для использования криптографии с открытым ключом необходимо гарантировать, что каждый закрытый и открытый ключ управляются корректным образом

- **Инфраструктура открытых ключей (Public Key Infrastructure — PKI)** предназначена для управления открытыми ключами и сертификатами с целью поддержки услуг аутентификации, шифрования, целостности и неотказуемости.

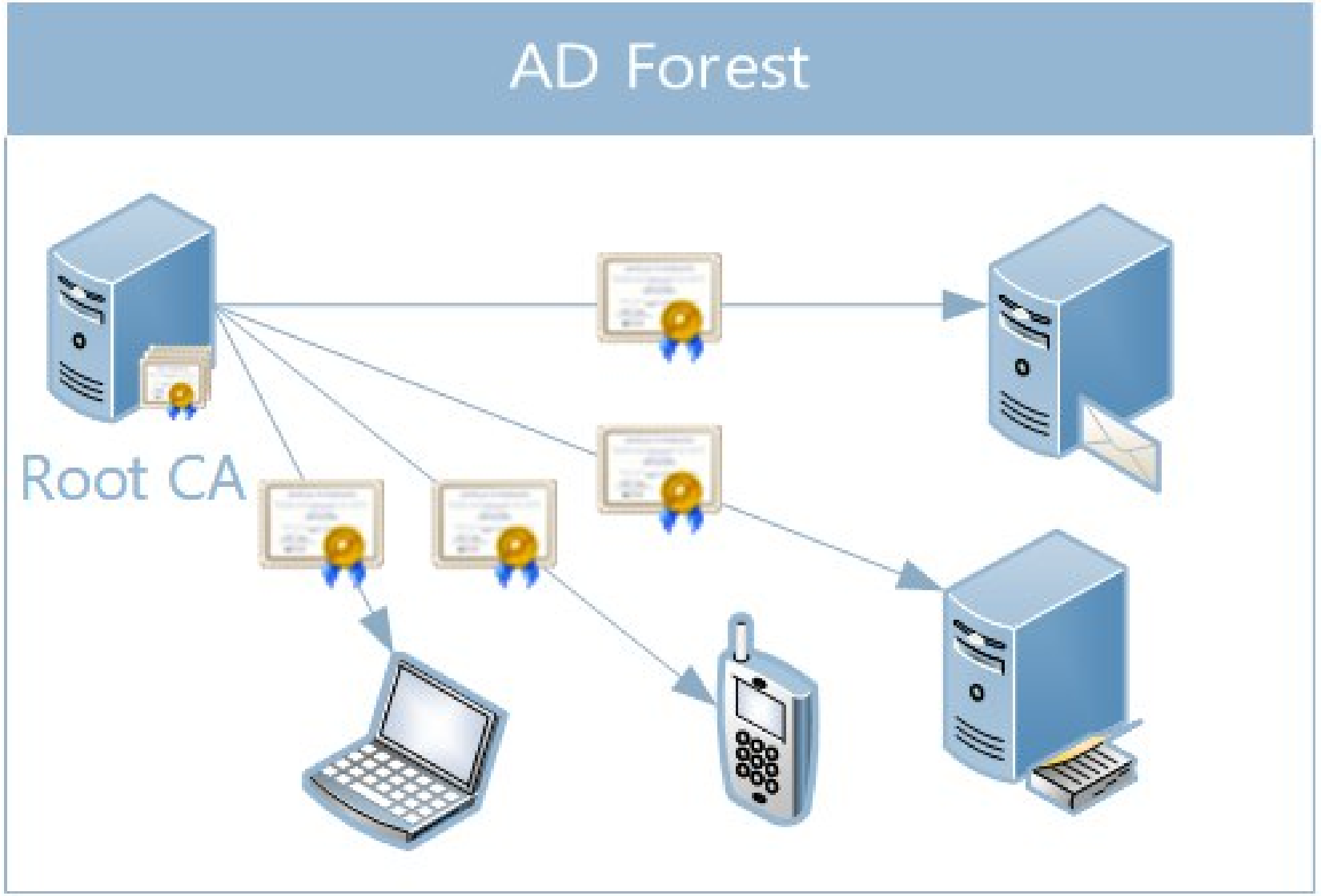
Инфраструктура открытых ключей (PKI)

- **Открытый ключ**, связанный с определенным пользователем, должен быть удостоверен сертификатом открытого ключа Более того, подлинность **сертификата открытого ключа** должна проверяться доверенным учреждением — **центром сертификации** (CA — certification autority).

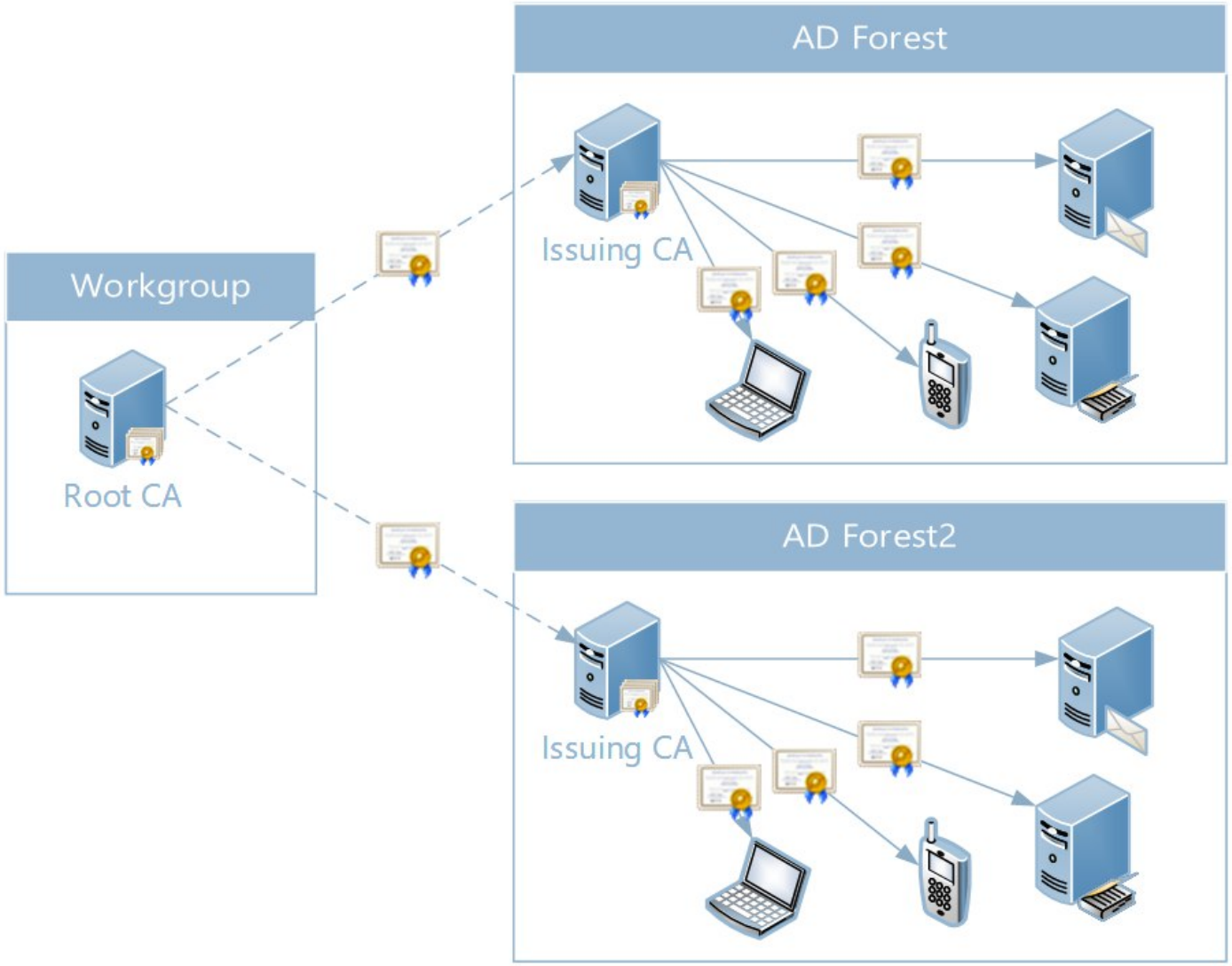
Инфраструктура открытых ключей (PKI)

- В основе PKI лежит использование криптографической системы с открытом ключом и несколько основных принципов:
  - закрытый ключ известен только его владельцу;
  - удостоверяющий центр создает сертификат открытого ключа, удостоверяя этот ключ;
  - никто не доверяет друг другу, но все доверяют удостоверяющему центру;
  - удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

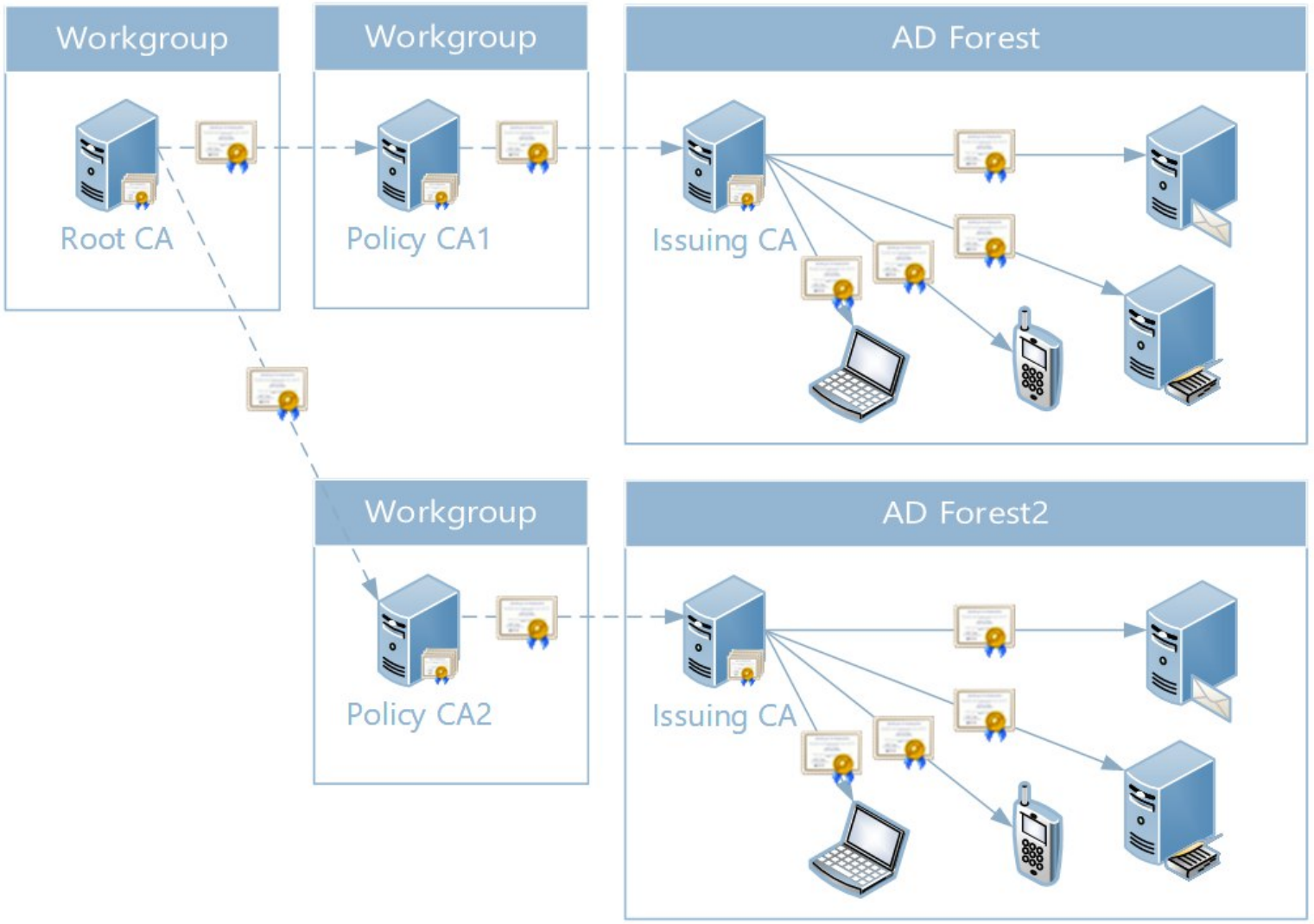
Типовые схемы развёртывания иерархии PKI **Одноуровневая иерархия**



Типовые схемы развёртывания иерархии PKI **Двухуровневая иерархия**



Типовые схемы развёртывания иерархии PKI Трёх- и более уровневые иерархии



Аутентификация с помощью открытого ключа на основе сертификата

- **Механизмы аутентификации на основе сертификатов обычно используют режим запрос-ответ.**
- Пользователь, или точнее программное обеспечение компьютера для генерирования ответа вырабатывает с помощью закрытого ключа пользователя цифровую подпись для случайного запроса от сервера аутентификации.
- Пользователь возвращает эту подпись серверу вместе с сертификатом открытого ключа.
- Сервер аутентификации проверяет подлинность сертификата открытого ключа, и, если она подтверждается он проверяет подлинность цифровой подписи, используя открытый ключ пользователя из сертификата, таким образом, удостоверяя подлинность пользователя.

Аутентификация с помощью открытого ключа на основе сертификата

- Общий процесс, с помощью которого аутентификационный сервер использует сертификат открытого ключа для получения подлинного открытого ключа пользователя, состоит из следующих этапов:
  1. Получение подлинного открытого ключа CA (одноразовый процесс).
  2. Получение идентификатора пользователя.
  3. Получение по незащищенному каналу от этого пользователя его сертификата открытого ключа (согласующегося с его идентификатором).
  4. Проверка текущей даты и времени относительно срока действия, указанного в сертификате (при проверке используются локальные доверенные часы):
  5. Проверка текущей действительности открытого ключа CA.
  6. Проверка подписи под сертификатом пользователя с помощью открытого ключа CA;
  7. Проверка того, что сертификат не был отозван.
  8. Если все проверки успешны, то сервер аутентификации принимает открытый ключ в сертификате как подлинным открытый ключ данного пользователя.

Организация хранения закрытого ключа

- Несмотря на то, что криптография с открытым ключом может обеспечивать надежную аутентификацию пользователя, сам по себе закрытый ключ никак с ним не связан. Поэтому необходимо хранить закрытый ключ, обеспечивая его защиту от компрометации.
- **Существует несколько способов хранения закрытого ключа:**
  - **Профиль пользователя/реестр** (ключи хранятся внутри локального хранилища операционной системы. Закрытый ключ связан с конкретным компьютером);
  - **Незащищенные носители** (карты памяти, USB-флеш и пр.);
  - **Touch Memory** (электронные ключи в виде так называемых «таблеток») и **Memory-карты**, выполненные в виде пластиковых карт;
  - **Смарт-карты и USB-ключи** с встроенной микросхемой защиты.

Протоколы аутентификации

В рамках операционных систем Windows компании Микрософт

Локальная аутентификация Windows

- **Локальная аутентификация в операционных системах Windows** выполняется в следующей последовательности:
  1. Пользователь вводит логин и пароль
  2. Данные передаются подсистеме локальной безопасности (LSA), которая сразу преобразует пароль в хэш. В открытом виде пароли нигде не хранятся.
  3. Служба LSA обращается к диспетчеру учетных записей безопасности (SAM) и сообщает ему имя пользователя
  4. Диспетчер обращается в базу SAM и извлекает оттуда хэш пароля указанного пользователя, сгенерированный при создании учетной записи (или в процессе смены пароля)
  5. Затем LSA сравнивает хэши, в случае их совпадения аутентификация считается успешной, а хэш введенного пароля помещается в хранилище службы LSA и до окончания сеанса пользователя

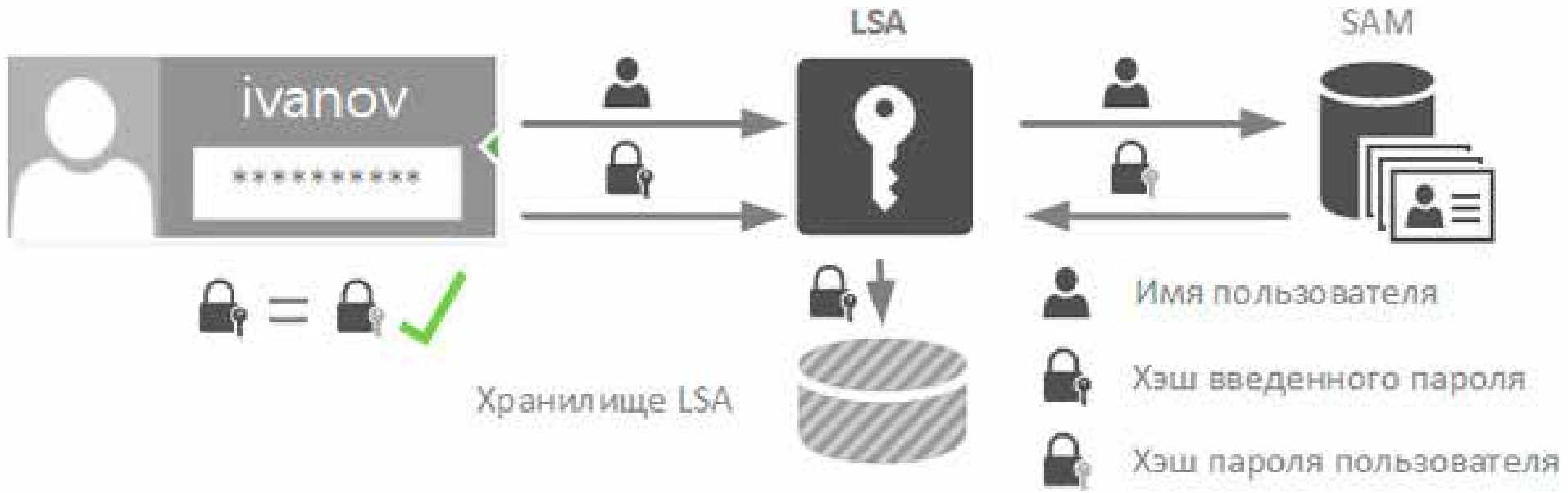


Схема работы локальной аутентификации Windows

Аутентификация в системах Windows

- **В системах Windows применяются следующие <u>СЕТЕВЫЕ ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ</u>:**
  - **LAN Manager (LM), LMv2** – до Windows XP включительно;
  - **NT LAN Manager (NTLM)** - появился в Windows NT, а до появления Kerberos в Windows 2000 был единственным протоколом аутентификации в домене NT. Начиная с Windows 7 / Server 2008 R2 использование протоколов NTLM и LM по умолчанию выключено.
  - **NT LAN Manager версии 2 (NTLM v2)** – начал использоваться с выходом Windows 2000;
  - **Kerberos** – используется после выхода Windows 2000 для управления доменом в Active Directory. Используется также в различных UNIX и UNIX подобных ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS и др.).

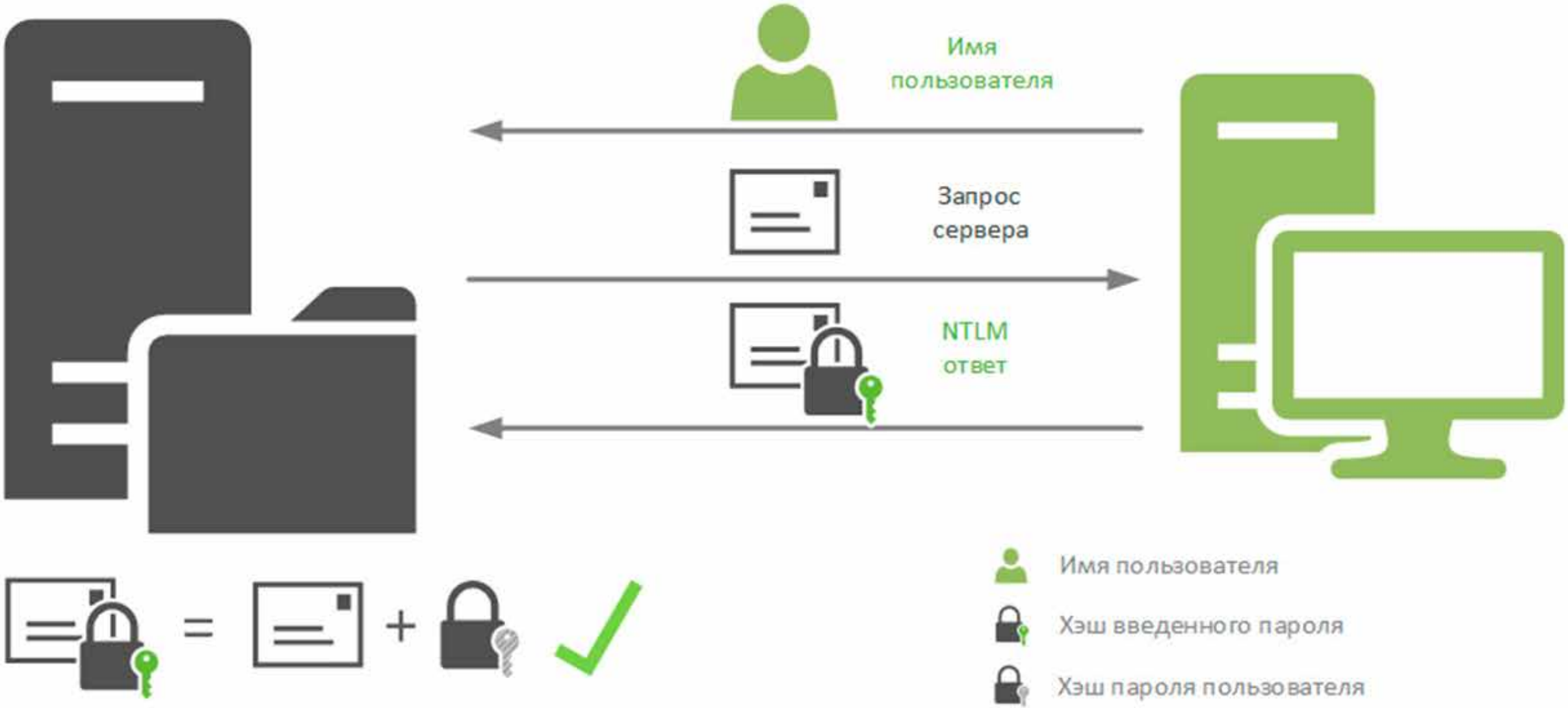
LAN Manager (LM)

- **Протокол LAN Manager возник на заре зарождения локальных сетей под управлением Windows и впервые был представлен в Windows 3.11 для рабочих групп, откуда перекочевал в семейство Windows 9.x.** Мы не будем рассматривать этот протокол, так как в естественной среде он уже давно не встречается, однако его поддержка, в целях совместимости, присутствует до сих пор. И если современной системе поступит запрос на аутентификацию по протоколу LM, то, при наличии соответствующих разрешений, он будет обработан.
- Что в этом плохого? Попробуем разобраться. Прежде всего разберемся, каким образом создается хэш пароля для работы с протоколом LM, не вдаваясь в подробности обратим ваше внимание на основные ограничения:
  - Пароль регистронезависимый и приводится к верхнему регистру.
  - Длина пароля - 14 символов, более короткие пароли дополняются при создании хэша нулями.
  - Пароль делится пополам и для каждой части создается свой хэш по алгоритму DES.
- Исходя из современных требований к безопасности можно сказать, что LM-хэш практически не защищен и будучи перехвачен очень быстро расшифровывается. Сразу оговоримся, прямое восстановление хэша невозможно, однако в силу простоты алгоритма шифрования возможен подбор соответствующей паролю комбинации за предельно короткое время.
- А теперь самое интересное, LM-хэш, в целях совместимости, создается при вводе пароля и хранится в системах по Windows XP включительно. Это делает возможной атаку, когда системе целенаправленно присылают LM-запрос и она его обрабатывает. Избежать создания LM-хэша можно изменив политику безопасности или используя пароли длиннее 14 символов. В системах, начиная с Windows Vista и Server 2008, LM-хэш по умолчанию не создается.

NT LAN Manager (NTLM)

- Сегодня протокол **NTLM**, точнее его более современная версия **NTLMv2, применяются для аутентификации компьютеров рабочих групп**, в **доменных сетях Active Directory по умолчанию применяется Kerberos**, однако если одна из сторон не может применить этот протокол, то по согласованию могут быть использованы NTLMv2, NTLM и даже LM (LAN Manager – использовался в системах до Windows XP включительно).
- **Принцип работы NTLM** имеет много общего с LM и эти протоколы обратно совместимы, но есть и существенные отличия. NT-хэш формируется на основе пароля длиной до 128 символов по алгоритму MD4, пароль регистрозависимый и может содержать не только ACSII символы, но и Unicode, что существенно повышает его стойкость по сравнению с LM.

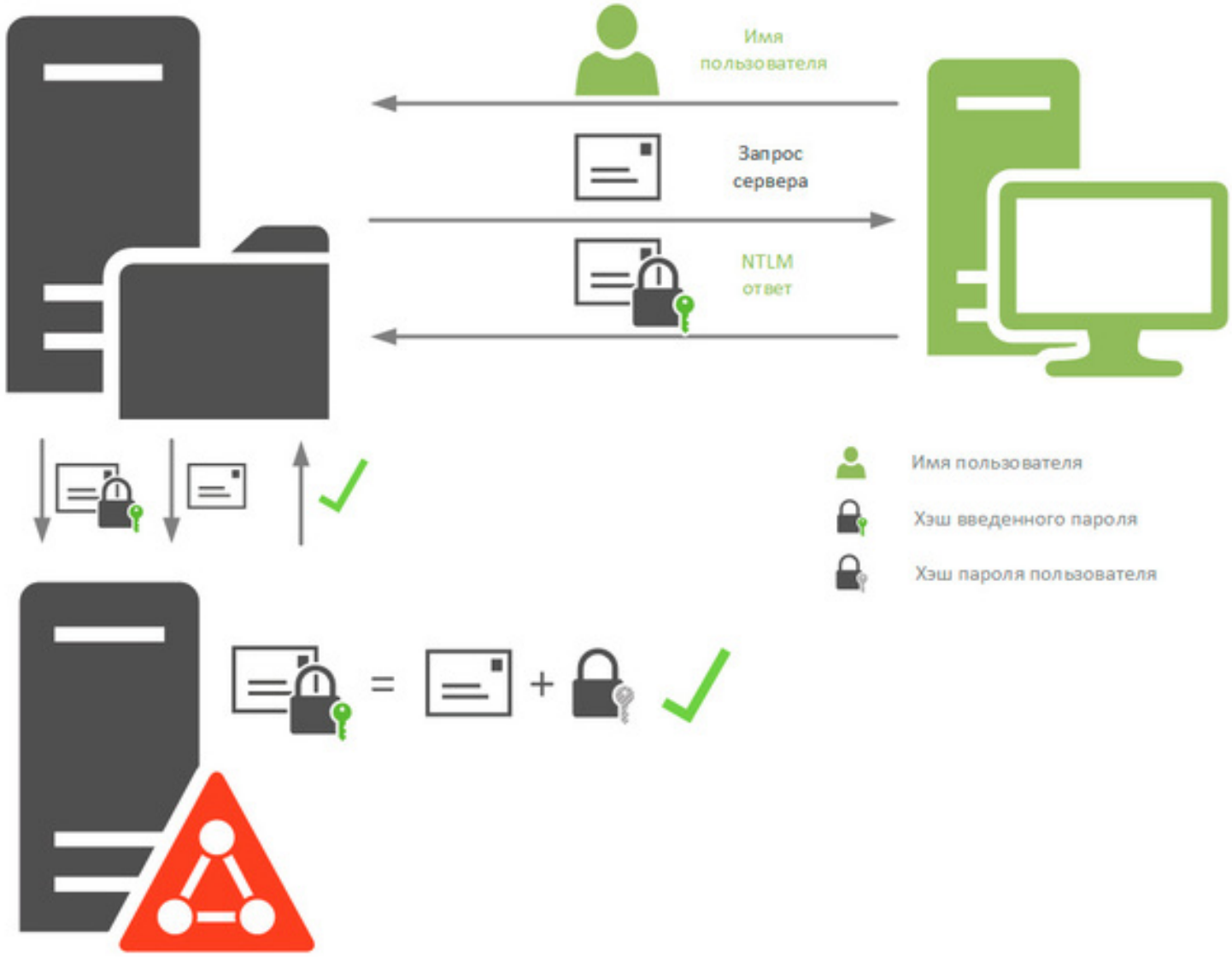
NT LAN Manager (NTLM). **Схема работы**



NT LAN Manager (NTLM). Схема работы

- Допустим локальный компьютер хочет получить доступ к некоторому файловому ресурсу на другом ПК, который мы будем считать сервером, при этом совсем не обязательно наличие на этом ПК северной ОС или серверных ролей. С точки зрения протокола NTLM клиент это тот, кто обращается, сервер - к кому обращаются.
- Чтобы получить доступ к ресурсу клиент направляет серверу запрос с именем пользователя. В ответ сервер передает ему случайное число, называемое **запросом сервера**. Клиент в свою очередь шифрует данный запрос по алгоритму DES, используя в качестве ключа NT-хэш пароля, однако, несмотря на то, что NT-хэш 128-битный, в силу технических ограничений используется 40 или 56 битный ключ (хеш делится на три части и каждая часть шифрует запрос сервера отдельно).
- Зашифрованный хэшем пароля запрос сервера называется ответом NTLM и передается обратно серверу, сервер извлекает из хранилища SAM хэш пароля того пользователя, чье имя было ему передано и выполняет аналогичные действия с запросом сервера, после чего сравнивает полученный результат с ответом NTLM. Если результаты совпадают, значит пользователь клиента действительно тот, за кого себя выдает, и аутентификация считается успешной.
- В случае доменной аутентификации процесс протекает несколько иначе. В отличие от локальных пользователей, хэши паролей которых хранятся в локальных базах SAM, хэши паролей доменных пользователей хранятся на контроллерах доменов. При входе в систему LSA отправляет доступному контроллеру домена запрос с указанием имени пользователя и имени домена и дальнейший процесс происходит как показано выше.

NT LAN Manager (NTLM). **Схема работы**
В случае получения доступа к третьим ресурсам



NT LAN Manager (NTLM). Схема работы В случае получения доступа к третьим ресурсам

- В случае получения доступа к третьим ресурсам схема также немного изменяется.
- Получив запрос от клиента, сервер точно также направит ему запрос сервера, но получив NTLM-ответ он не сможет вычислить значение для проверки на своей стороне, так как не располагает хэшем пароля доменного пользователя, поэтому он перенаправляет NTLM-ответ контроллеру домена и отправляет ему свой запрос сервера. Получив эти данные, контроллер домена извлекает хэш указанного пользователя и вычисляет на основе запроса сервера проверочную комбинацию, которую сравнивает с полученным NTLM-ответом, при совпадении серверу посылается сообщение, что аутентификация прошла успешно.
- Как видим, хэш пароля ни при каких обстоятельствах по сети не передается. Хэш введенного пароля хранит служба LSA, хэши паролей пользователей хранятся либо в локальных хранилищах SAM, либо в хранилищах контроллера домена.
- Но несмотря на это, протокол NTLM на сегодняшний день считаться защищенным не может. Слабое шифрование делает возможным достаточно быстро восстановить хэш пароля, а если использовался не только NTLM, а еще и LM-ответ, то и восстановить пароль.
- Но и перехваченного хэша может оказаться вполне достаточно, так как NTLM-ответ генерируется на базе пароля пользователя и подлинность клиента сервером никак не проверяется, то возможно использовать перехваченные данные для неавторизованного доступа к ресурсам сети. Отсутствие взаимной проверки подлинности также позволяет использовать атаки плана человек посередине, когда атакующий представляется клиенту сервером и наоборот, устанавливая при этом два канала и перехватывая передаваемые данные.

NTLMv2

- **NTLMv2 (NTLM версии 2) — встроенный в операционные системы семейства Microsoft Windows протокол сетевой аутентификации.**
- Широко применяется в различных сервисах на их базе. Изначально был предназначен для повышения безопасности аутентификации путём замены устаревших LM и NTLM v1. NTLMv2 был введён начиная с Windows NT 4.0 SP4 и используется версиями Microsoft Windows вплоть до Windows 10 включительно.

NTLMv2

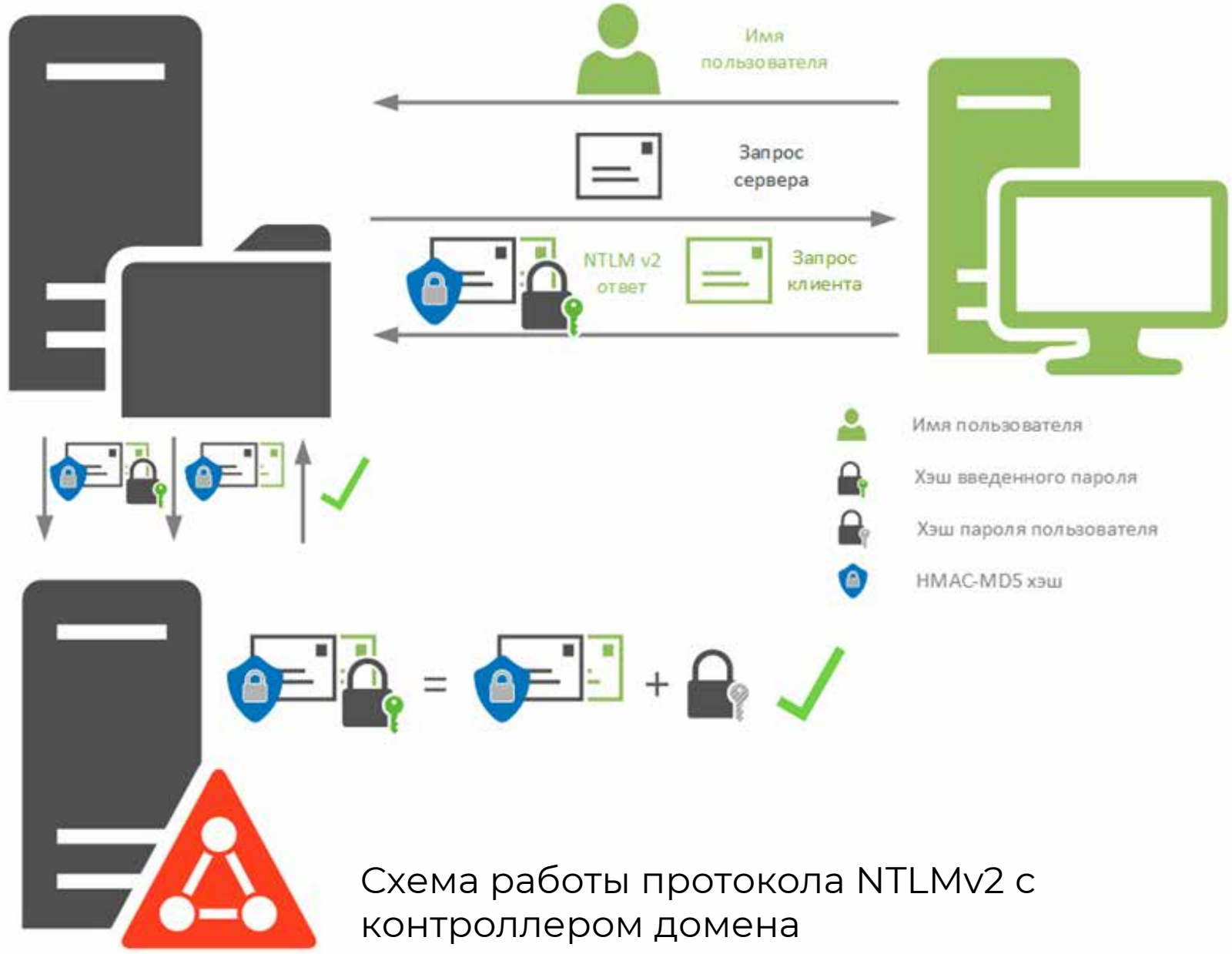
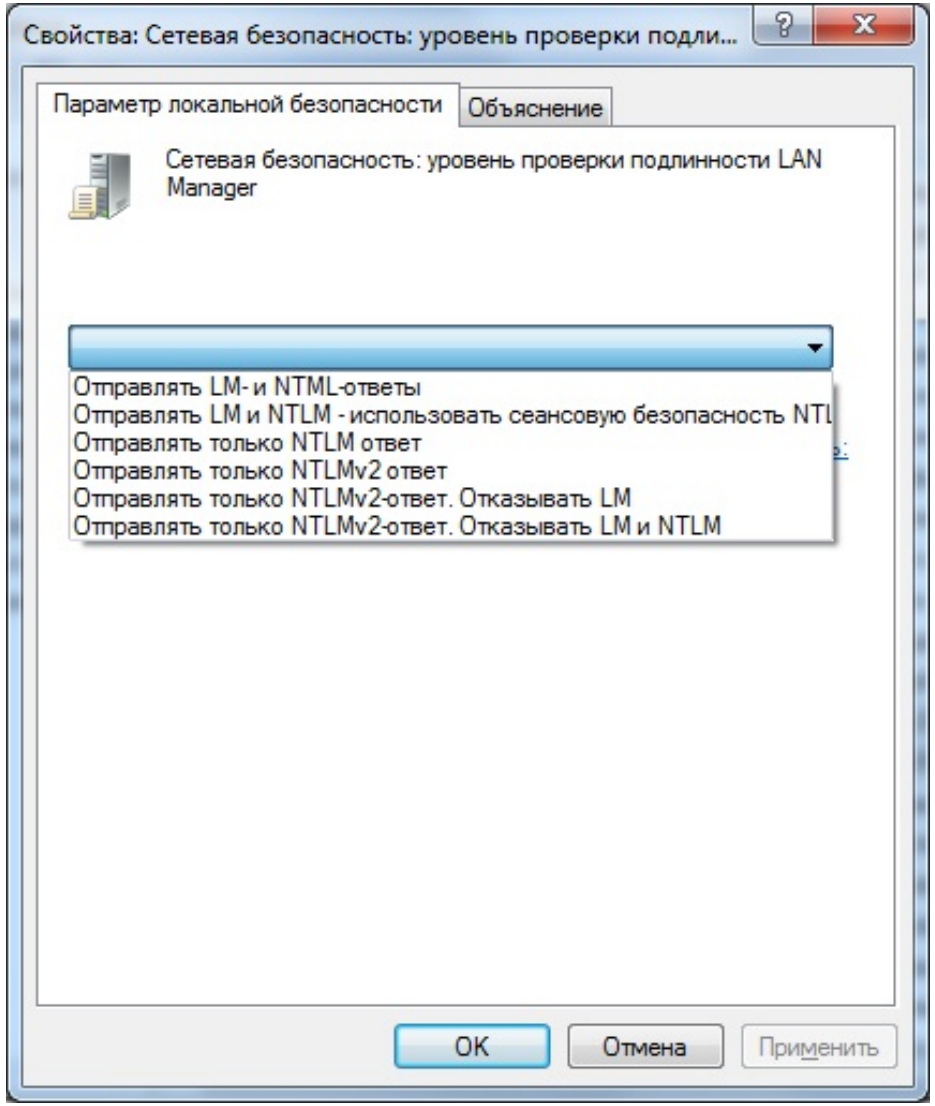


Схема работы протокола NTLMv2 с контроллером домена

NTLMv2

- Как и в NTLM, клиент при обращении к серверу сообщает ему имя пользователя и имя домена, в ответ сервер передает ему случайное число - запрос сервера. В ответ клиент генерирует также случайное число, куда, кроме прочего, добавляется метка времени, которое называется запрос клиента. Наличие метки времени позволяет избежать ситуации, когда атакующий первоначально накапливает перехваченные данные, а потом с их помощью осуществляет атаку.
- Запрос сервера объединяется с запросом клиента и от этой последовательности вычисляется HMAC-MD5 хэш. После чего от данного хэша берется еще один HMAC-MD5 хэш, ключом в котором выступает NT-хэш пароля пользователя. Получившийся результат называется NTLMv2-ответом и вместе с запросом клиента пересылается серверу.
- Криптостойкость данного алгоритма является актуальной и на сегодняшний день, известно только два случая взлома данного хэша, один из них произведен компанией Symantec в исследовательских целях. Можно с уверенностью сказать, что в настоящий момент нет массовых инструментов для атак на NTLMv2, в отличие от NTLM, взломать который может любой вдумчиво прочитавший инструкцию школьник.
- Сервер, получив NTLMv2-ответ и запрос клиента, объединяет последний с запросом сервера и также вычисляет HMAC-MD5 хэш, затем передает его вместе с ответом контроллеру домена. Тот извлекает из хранилища сохраненный хэш пароля пользователя и производит вычисления над HMAC-MD5 хешем запросов сервера и клиента, сравнивая получившийся результат с переданным ему NTLMv2-ответом. В случае совпадения серверу возвращается ответ об успешной аутентификации.

LM, NTLM, NTLMv2



Окно параметров безопасности Windows

Настройка политики безопасности Windows

Запустите «Панель управления» и откройте раздел «Администрирование → Локальная политика безопасности → Локальные политики → Параметры безопасности» (Administrative Tools → Local Security Policy → Local Policies → Security Options). В этом разделе найдите политику «Сетевая безопасность: уровень проверки подлинности LAN Manager». Из раскрывающегося списка необходимо выбрать параметр «Отправлять только NTLMv2-ответ. Отказывать LM и NTLM»

Недостатки протокола NTLM

- **Основным недостатком протокола NTLM служит то, что он не предусматривает взаимную аутентификацию клиента и сервера**, это во многом обусловлено тем, что протокол изначально разрабатывался для небольших сетей, где все узлы считаются легитимными. Несмотря на то, что в последних версиях протокола сделаны серьезные улучшения безопасности, но направлены они в основном на усиление криптографической стойкости, не устраняя принципиальных недостатков.
- **В доменных сетях протоколы NTLM вызывают повышенную нагрузку на контроллеры домена**, так как всегда обращаются к ним для аутентификации пользователя. При этом также отсутствует взаимная идентификация узлов и существует возможность накопления пакетов для последующего анализа и атаки с их помощью.

Kerberos

- Протокол Kerberos был разработан в Массачусетском технологическом институте (MIT) в рамках проекта «Афина» в 1983 году и долгое время использовался в качестве образовательного, пока версия 4 не была сделана общедоступной. В настоящий момент принята в качестве стандарта и широко используется следующая версия протокола **Kerberos 5**.
- **В отличии от NTLM Kerberos изначально разрабатывался с условием, что первичная передача информации будет производиться в открытых сетях**, где она может быть перехвачена и модифицирована.
- Также **протокол предусматривает обязательную взаимную аутентификацию клиента и сервера**, а взаимное доверие обеспечивает единый удостоверяющий центр, который обеспечивает централизованную выдачу ключей.

Kerberos

- Протокол Kerberos может использовать централизованное хранение аутентификационных данных и является основой для построения механизмов Single Sign-On (возможность одноразовой аутентификации в нескольких приложениях).
- **Протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними с учетом того, что начальный обмен информацией между клиентом и сервером может происходить в незащищённой среде**, а передаваемые пакеты - перехвачены и модифицированы.
- Одним из преимуществ протокола Kerberos, обеспечивающих очень высокий уровень сетевой безопасности, является то, что **во всех сетевых взаимодействиях в открытом виде не передаются ни пароли, ни хэши паролей**. Все удостоверения являются зашифрованными пакетами данных.

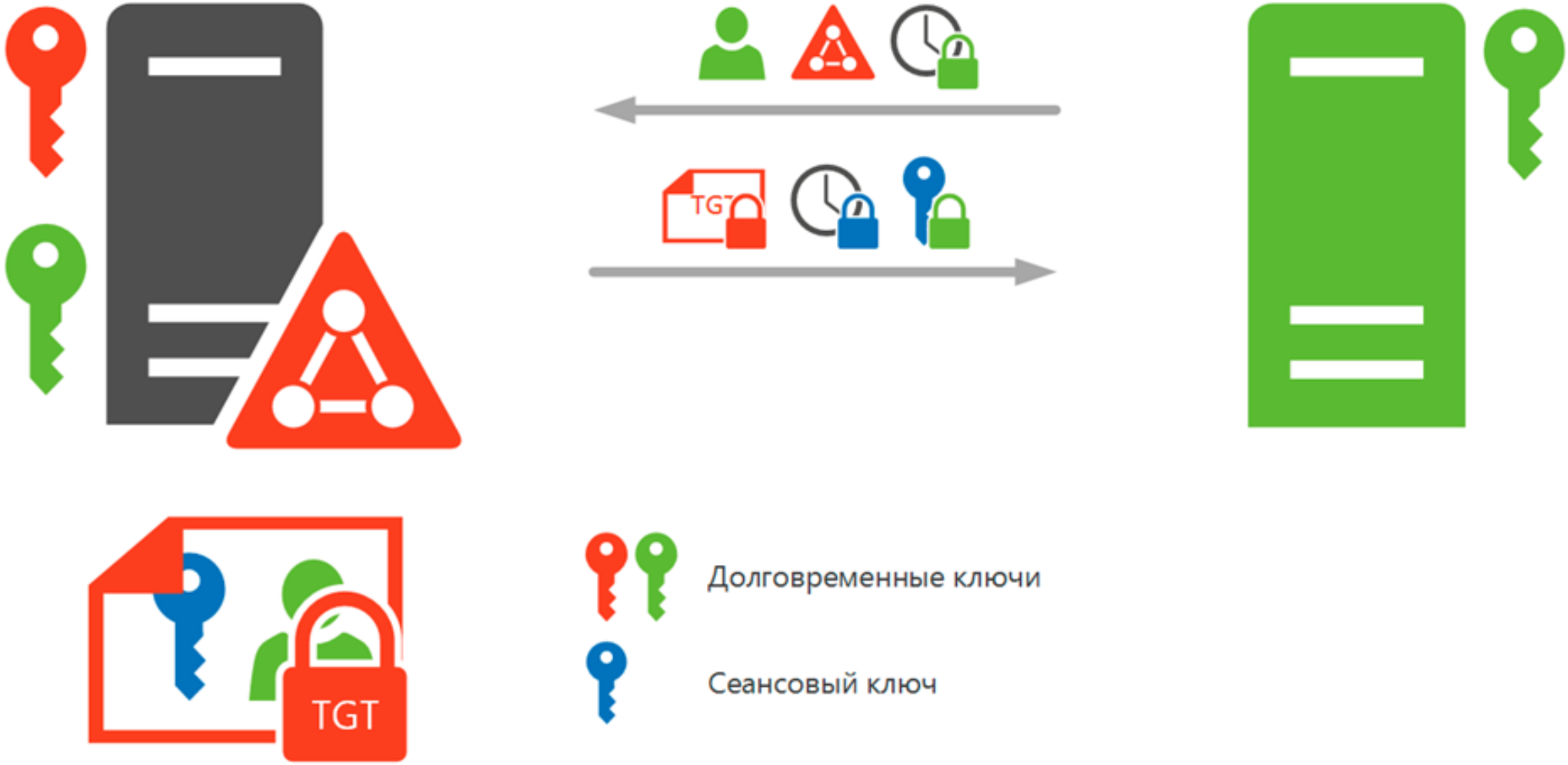
Kerberos

- Протокол использует понятие **Ticket** (билет, удостоверение).
- **Ticket** является зашифрованным пакетом данных, выданным выделенным доверенным центром аутентификации, в терминах протокола Kerberos - **KDC (Key Distribution Center, центр распределения ключей).**

- **KDC** состоит из двух компонент:
  - сервер аутентификации (англ. **Authentication Server**, сокр. **AS**);
  - сервер выдачи разрешений (англ. **Ticket Granting Server**, сокр. **TGS**).

- Когда пользователь выполняет первичную аутентификацию, после успешного подтверждения его подлинности KDC выдаёт первичное удостоверение пользователя для доступа к сетевым ресурсам - TGT (Ticket Granting Ticket). В дальнейшем при обращении к отдельным сетевым ресурсам пользователь, предъявляя TGT, получает от KDC удостоверение для доступа к конкретному сетевому ресурсу - Service Ticket.

Аутентификация клиента по протоколу Kerberos



Аутентификация клиента по протоколу Kerberos

- Желая пройти проверку подлинности в сети, клиент передает KDC открытым текстом свое имя, имя домена и метку времени (текущее время клиента), зашифрованное долговременным ключом клиента. Метка времени в данном случае выступает в роли аутентификатора - определенной последовательности данных, при помощи которой узлы могут подтвердить свою подлинность.
- Получив эти данные KDC извлекает долговременный ключ данного пользователя и расшифровывает метку времени, которую сравнивает с собственным текущим временем, если оно отличается не более чем на 5 минут (значение по умолчанию), то метка считается действительной. Эта проверка является дополнительной защитой, так как не позволяет использовать для атаки перехваченные и сохраненные данные.
- Убедившись, что метка времени действительна KDC выдает клиенту **сеансовый ключ** и **билет (тикет) на получение билета** (ticket granting ticket, **TGT**), который содержит копию сеансового ключа и сведения о клиенте, TGT шифруется с помощью долговременного ключа KDC и никто кроме него билет расшифровать не может. Сеансовый ключ шифруется с помощью долговременного ключа клиента, а полученная от клиента метка времени возвращается обратно, зашифрованная уже сеансовым ключом. Билет на получение билета является действительным в течении 8 часов или до завершения сеанса пользователя.
- Клиент в первую очередь расшифровывает сеансовый ключ, затем при помощи этого ключа метку времени и сравнивает ее с той, что он отправил KDC, если метка совпала, значит KDC тот, за кого себя выдает, так как расшифровать метку времени мог только тот, кто обладает долговременным ключом. В этом случае клиент принимает TGT и помещает его в свое хранилище.
- Чтобы лучше понять этот механизм приведем небольшой пример. Если злоумышленник перехватил посланный KDC запрос, то он может на основе открытых данных послать клиенту поддельный сеансовый ключ и TGT, но не сможет расшифровать метку времени, так как не обладает долговременным ключом. Точно также, он может перехватить отправленные клиенту TGT и сеансовый ключ, но также не сможет расшифровать последний, не имея долговременного ключа. Перехватить долговременный ключ он не может, так как они по сети не передаются.
- Успешно пройдя аутентификацию, клиент будет располагать сеансовым ключом, которым впоследствии он будет шифровать все сообщения для KDC и билетом на получение билета (TGT).

Kerberos. **Этап аутентификации клиента**

Клиент

Идентификатор клиента
Метка времени клиента
Идентификатор сервера (TGS)

Запрос к CA →

CA генерирует сессионный ключ (Клиент/TGS)

Пользовательская копия сессионного ключа
Идентификатор сервера (TGS)
Время жизни билета
TGT
Зашифровано ключом пользователя

Копия сессионного ключа для TGS
Идентификатор клиента
Время жизни билета
Метка времени ЦРК
IP адрес клиента
Зашифровано ключом TGS

← Ответ CA

Клиент

Kerberos. **Этап авторизации клиента на TGS**

Клиент

Идентификатор сервиса
TGT
Аутентификатор

Запрос к TGS →

TGS генерирует сессионный ключ (Клиент/сервис)

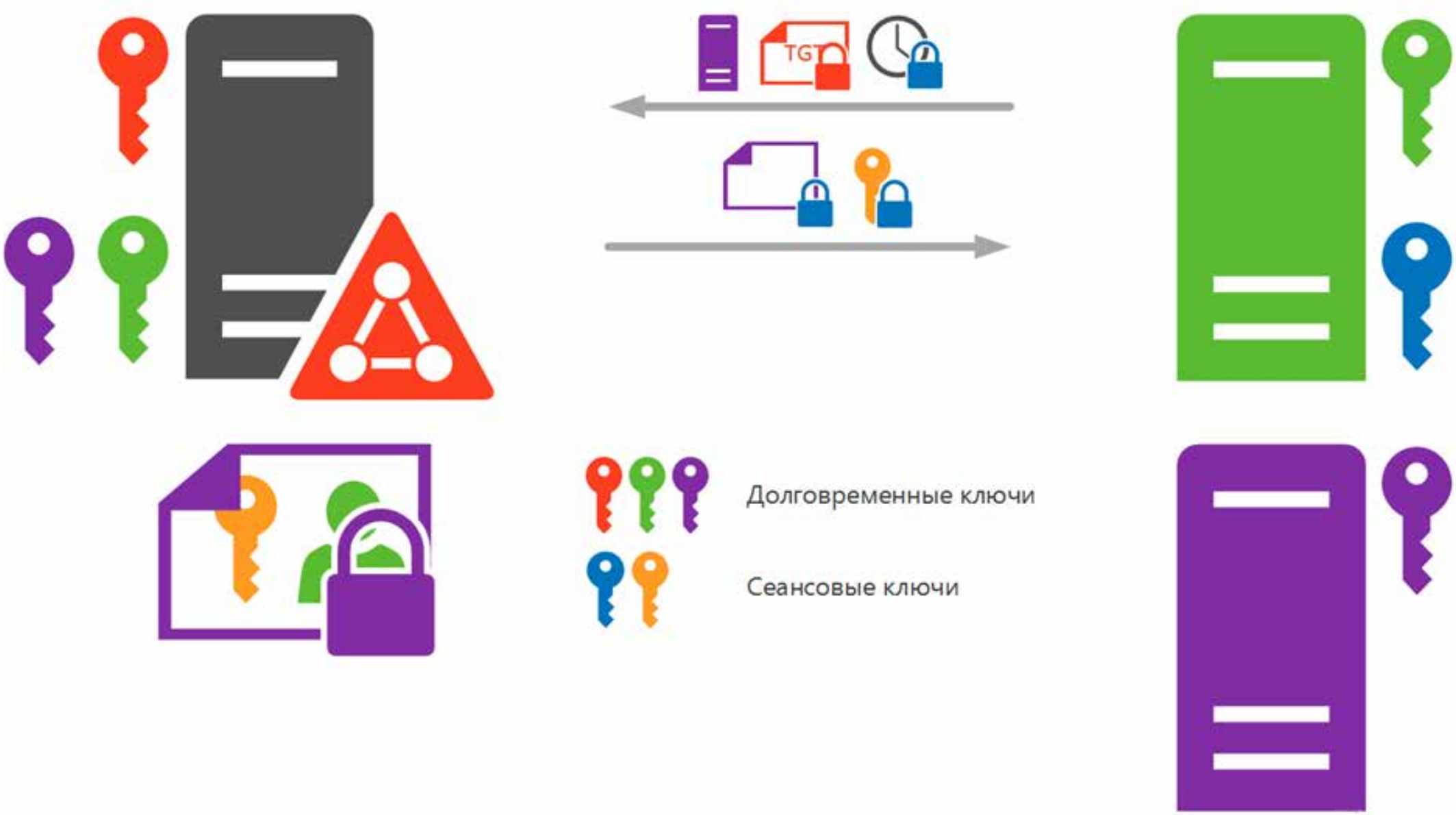
Пользовательская копия сессионного ключа
Идентификатор сервиса
Время жизни билета
Билет сервиса
Зашифровано сессионным ключом CA

Копия нового сессионного ключа для сервиса
Идентификатор клиента
Время жизни билета
Метка времени ЦРК
IP адрес клиента
Зашифровано ключом сервиса

← Ответ TGS

Клиент

Kerberos. **Ситуация, когда клиент хочет обратиться к серверу**



Kerberos. **Ситуация, когда клиент хочет обратиться к серверу**

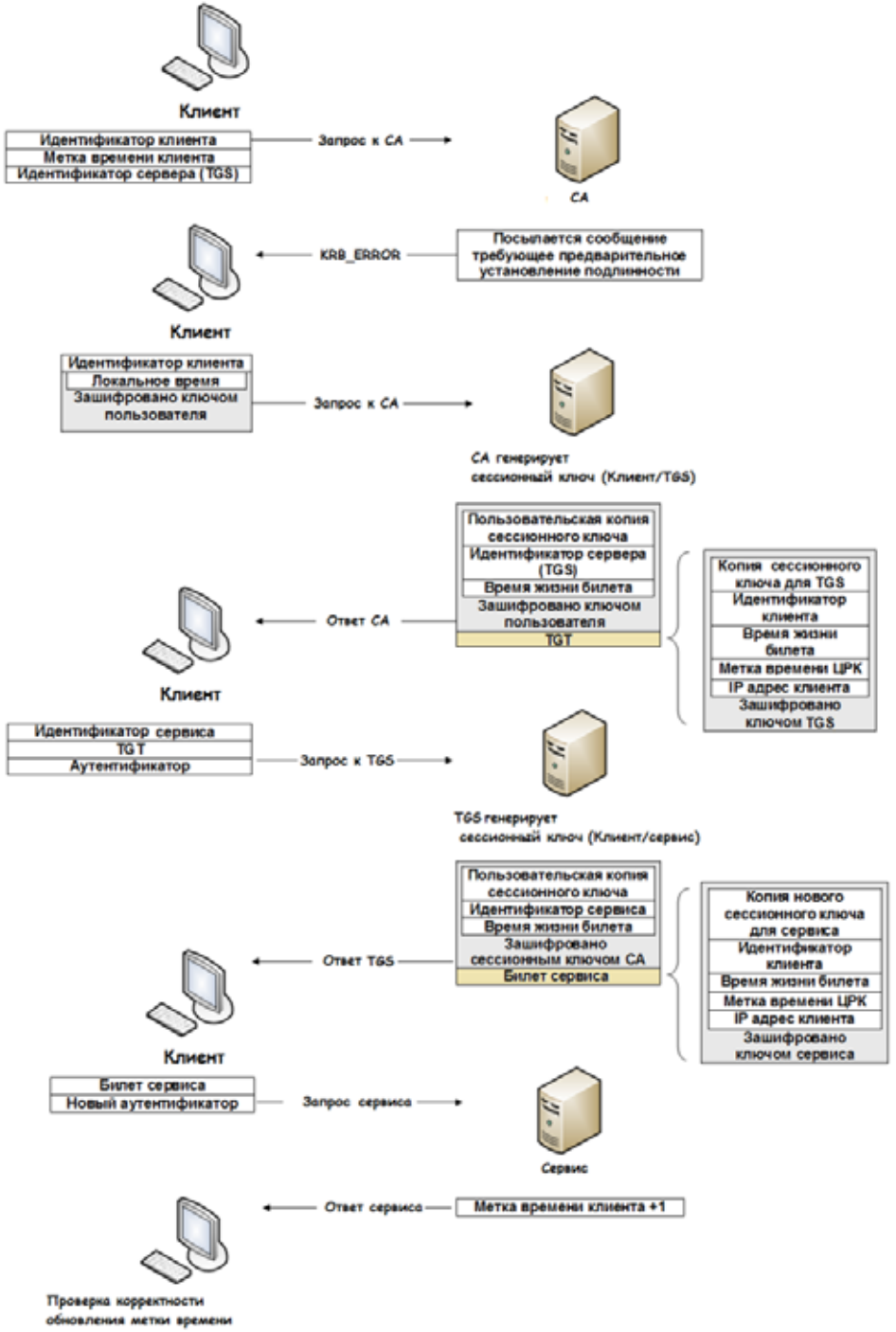
- Рассмотрим ситуацию, когда клиент хочет обратиться к серверу.
- Для этого он снова обращается к KDC и посылает ему билет на получение билета, зашифрованную сеансовым ключом метку времени и имя сервера. Прежде всего KDC расшифровывает предоставленный ему TGT и извлекает оттуда данные о клиенте и его сеансовый ключ, обратите внимание, что сам KDC сеансовые ключи не хранит. Затем сеансовым ключом он расшифровывает данные от клиента и сравнивает метку времени с текущим. Если расхождения нет, то KDC формирует общий сеансовый ключ для клиента и сервера.
- Теоретически теперь данный ключ следует передать как клиенту, так и серверу. Но KDC имеет защищенный канал и установленные доверительные отношения только с клиентом, поэтому он поступает по-другому. Экземпляр сеансового ключа для клиента он шифрует сессионным ключом, а копию сеансового ключа для сервера он объединяет с информацией о клиенте в **сеансовый билет** (session ticket), который шифрует закрытым ключом сервера, после чего также отправляет клиенту, дополнительно зашифровав сессионным ключом.
- Таким образом клиент получает сессионный ключ для работы с сервером и сессионный билет. Получить содержимое билета, как и TGT, он не может, так как не располагает нужными долговременными ключами.

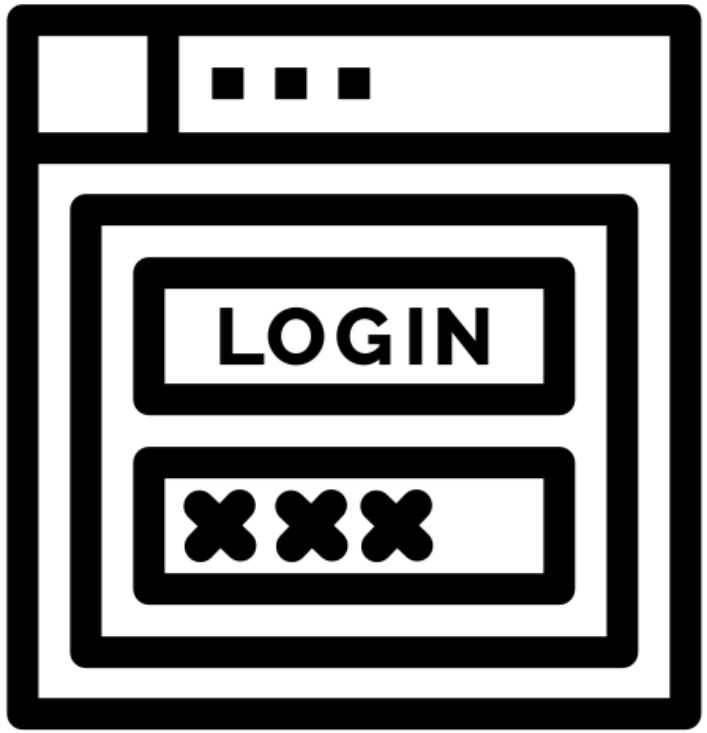
Kerberos. **Ситуация, когда клиент хочет обратиться к серверу**

- Теперь, имея новый ключ и билет, клиент обращается непосредственно к серверу:

- Он предъявляет ему сеансовый билет и метку времени, зашифрованную сессионным ключом. Сервер расшифровывает билет, извлекает оттуда свой экземпляр ключа и сведения о клиенте, затем расшифровывает метку времени и сравнивает ее с текущим. Если все нормально, то он шифрует полученную метку своим экземпляром сессионного ключа и посылает назад клиенту. Клиент расшифровывает ее своим сеансовым ключом и сравнивает с тем, что было послано серверу. Совпадение данных свидетельствует о том, что сервер тот, за кого себя выдает.
- Как можно заметить, сеансовые ключи никогда не передаются по незащищенным каналам и не передаются узлам, с которыми нет доверительных отношений. У KDC нет доверительных отношений с сервером, и он не может передать ему сессионный ключ, так как нет уверенности, что ключ будет передан кому надо. Но у него есть долговременный ключ этого сервера, которым он шифрует билет, это гарантирует, что никто иной не прочитает его содержимое и не получит сессионный ключ.
- Клиент имеет билет и свой экземпляр ключа, доступа к содержимому билета у него нет. Он передает билет серверу и ждет ответ в виде посланной метки времени. Сервера, как и KDC, не хранят сеансовые ключи, а, следовательно, расшифровать метку времени сервер может только в том случае, если сможет расшифровать билет и получить оттуда сеансовый ключ, для чего нужно обладать долговременным ключом. Получив ответ и расшифровав его, клиент может удостоверить подлинность сервера, так как прочитать аутентификатор и извлечь из него метку времени сервер сможет только при условии расшифровки билета и получения оттуда сеансового ключа.
- Несмотря на то, что мы рассмотрели крайне упрощенную модель протокола Kerberos, надеемся, что данная статья поможет устранить пробелы и получить первоначальные знания, которые затем можно расширить и углубить уже осмысленно подойдя к прочтению более серьезных материалов.

Схема работы
Kerberos 5





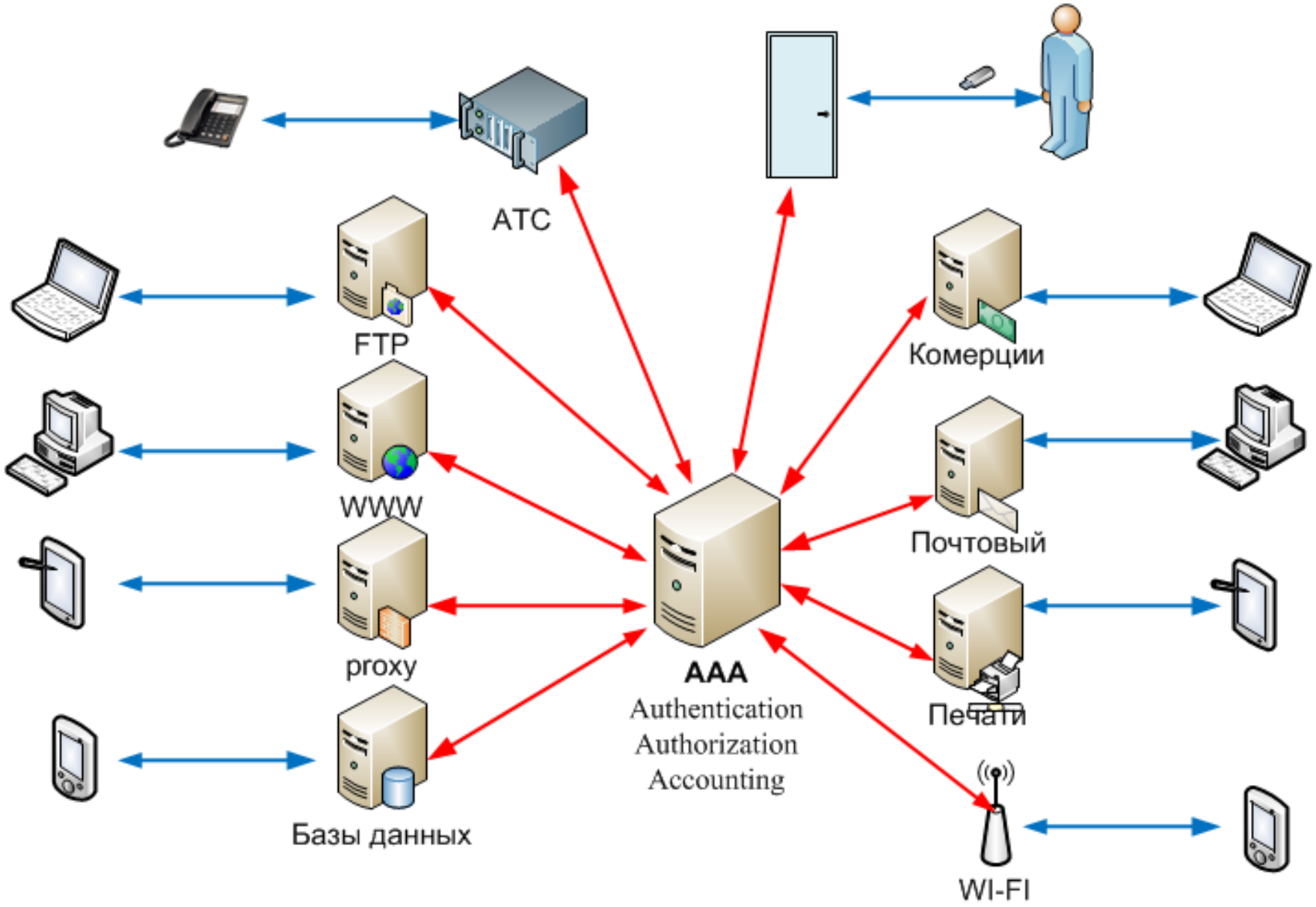
Протоколы аутентификации

Протоколы AAA (Authentication, Authorization, Accounting)

Протоколы AAA

- **AAA (Authentication, Authorization, Accounting)** — используется для описания процесса предоставления доступа и контроля за ним.
  - **Authentication** – **аутентификация** — сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю, сертификату, смарт-карте и т.д.
  - **Authorization** — **авторизация** — проверка полномочий, проверка уровня доступа) — сопоставление учётной записи в системе (и персоны, прошедшей аутентификацию) и определённых полномочий (или запрета на доступ). В общем случае авторизация может быть «негативной» (пользователю А запрещён доступ к серверам компании).
  - **Accounting** — **учёт, контроль** — слежение за потреблением ресурсов (преимущественно сетевых) пользователем. В accounting включается также и запись фактов получения доступа к системе (англ. access logs).

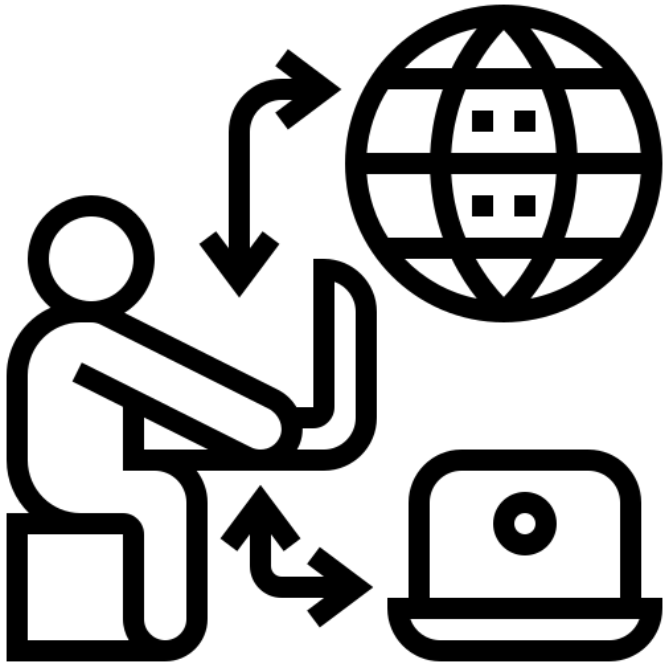
Протокол AAA



Протокол AAA

- Представьте организацию (например университет или крупная компания) с множеством систем (серверы, АТС, WI-FI, здания, помещения и т.д.). Необходимо регистрировать в каждой системе одного и того-же пользователя. Чтобы этого не делать, ставится сервер AAA и все пользователи регистрируются только в нем. Все системы организации обращаются к серверу AAA.
- **Алгоритм**:
  1. пользователь посылает запрос на аутентификацию системе (пароль, ключ и т.д.)
  2. система пересылает его серверу AAA (т.к. не может провести аутентификацию)
  3. сервер AAA посылает ответ системе
  4. пользователь получает или не получает доступ
- **Основные протоколы AAA:**
  - RADIUS, DIAMETER
  - TACACS, TACACS+ (компании Cisco)

  Наибольшее распространение получил RADIUS ему на смену создан DIAMETER. Закрытые протоколы не выдерживают конкуренции.



Протоколы аутентификации

Протоколы аутентификации для удалённого доступа

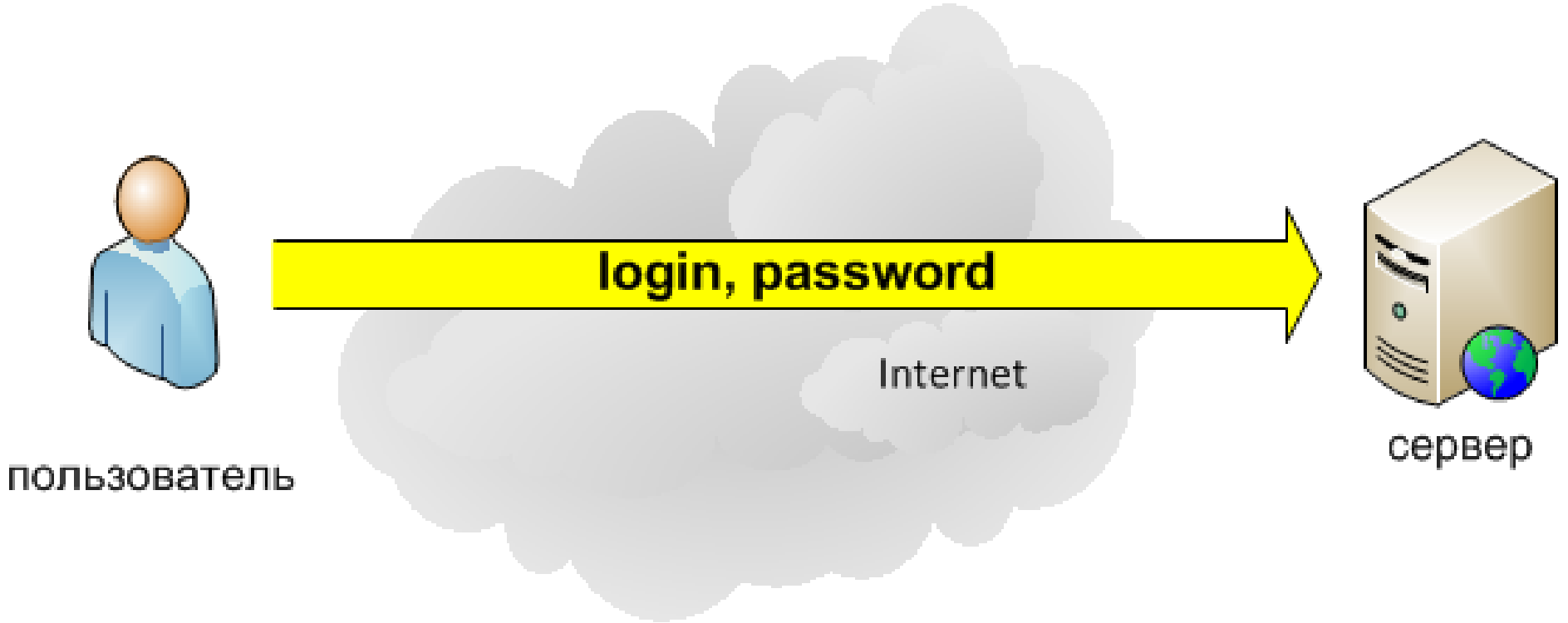
Протоколы аутентификации для удалённого доступа

- Часть протоколов сетевой аутентификации были разработаны специально для обеспечения удаленного доступа к информационным ресурсам посредством открытых каналов связи (к примеру, телефонные линии, Internet).
- Такими протоколами являются:
  - **PAP** (Password Authentication Protocol);
  - **CHAP** (Challenge Handshake Authentication Protocol);
  - **EAP** (Extensible Authentication Protocol);
  - **TACACS** (Terminal Access Controller Access Control System).
  - **RADIUS** (Remote Authentication Dial-in User Service), ему на смену создан протокол **DIAMETER;**

PAP (Password Authentication Protocol)

- **PAP (англ. Password Authentication Protocol) (RFC 1334) — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (без шифрования).**
- **Протокол аутентификации PAP используется в протоколе PPP** (англ. Point-to-Point Protocol), для предоставления пользователям доступа к серверным ресурсам. Почти все сетевые операционные системы поддерживают протокол PAP.
- PAP передает незашифрованные ASCII коды по сети и поэтому крайне небезопасен, поскольку пересылаемые пароли можно легко читать в пакетах, которыми обмениваются стороны в ходе проверки подлинности.

PAP (Password Authentication Protocol)



- **Алгоритм PAP:**
  - клиент посылает имя и пароль серверу
  - сервер сверяет присланный пароль с паролем в своем хранилище
- **Обычно PAP используется только при подключении к старым серверам удалённого доступа, которые не поддерживают никакие другие протоколы проверки подлинности.**

TACACS (Terminal Access Controller Access Control System)

- **TACACS (англ. Terminal Access Controller Access Control System)** — сеансовый протокол, использовавшийся на серверах доступа ARPANET (ARPANET прекратила своё существование в июне 1990 года.). Центральный сервер, который принимает решение, разрешить или не разрешить определённому пользователю подключиться к сети.
- **TACACS+** (англ. Terminal Access Controller Access Control System plus) — сеансовый протокол, **результат дальнейшего усовершенствования TACACS, предпринятого Cisco**. Улучшена безопасность протокола (шифрование), а также введено разделение функций аутентификации, авторизации и учёта.
- Устаревшие протоколы.

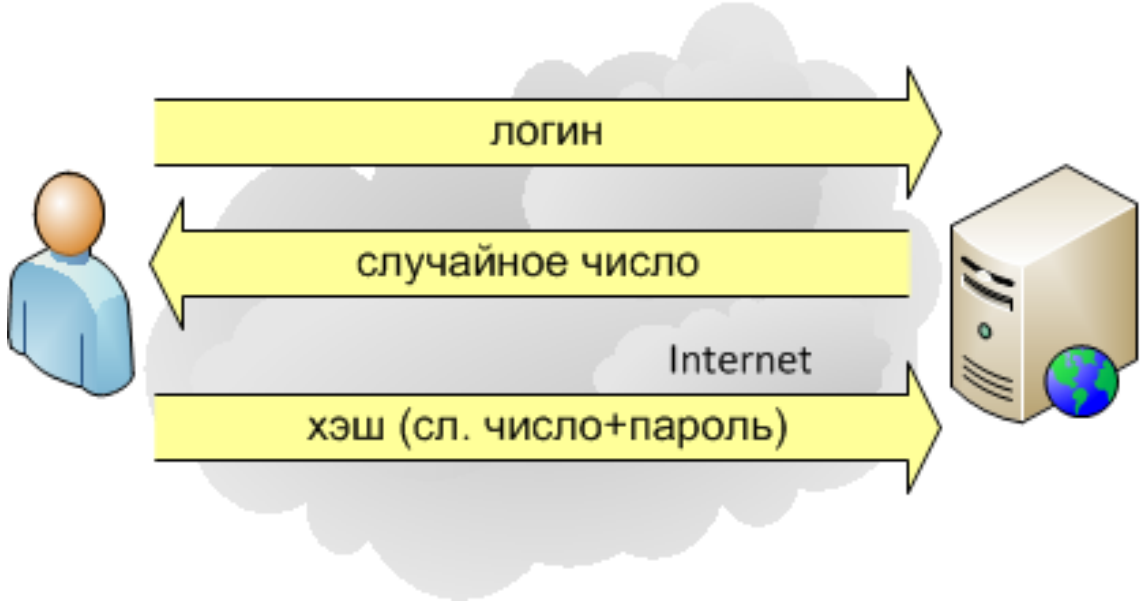
CHAP (Challenge Handshake Authentication Protocol)

- **CHAP (англ. Challenge Handshake Authentication Protocol)** — протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и **предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём.**
- **Аутентификация узла выполняется путём трехэтапной процедуры согласования.**
  1. После установления PPP-соединения и одобрения обеих сторон на подключение по CHAP-протоколу аутентификатор отправляет на узел пакет CHAP, имеющий тип Challenge (вызов), который содержит в себе открытый ключ.
  2. Узел на основе полученного открытого ключа и своего секрета, вычисляет хеш с помощью алгоритма хеширования MD5 и отправляет пакет CHAP, имеющий тип Response (отклик), содержащий в себе вычисленный хеш.
  3. Аутентификатор сравнивает полученное значение хеша со своим расчётом ожидаемого значения хеша. Если значения совпадают, то проверка подлинности считается успешной. При отличающихся значениях происходит разрыв соединения.

  Через различные промежутки времени аутентификатор посылает новый запрос узлу, и шаги 1-3 повторяются
- Протокол CHAP широко используется различными поставщиками серверов и клиентов сетевого доступа. Определён в RFC 1994.

CHAP (Challenge Handshake Authentication Protocol)

- **CHAP - аутентификация без передачи пароля.**
- Алгоритм CHAP:
  1. пользователь посылает серверу запрос на доступ (login)
  2. сервер отправляет клиенту случайное число
  3. на основе этого случайного числа и пароля пользователя клиент вычисляет хеш
  4. клиент пересылает хеш серверу
  5. сервер сверяет присланный хеш со своим вычисленным
  6. в случайные промежутки времени сервер отправляет новый и повторяет шаги с 2 по 5.
- Основной недостаток - необходимо хранить пароль на сервере.



MS-CHAP
(Microsoft Challenge Handshake Authentication Protocol)

- **MS-CHAP (англ. Microsoft Challenge Handshake Authentication Protocol)** — протокол проверки подлинности соединений между сервером и клиентом без передачи пароля последнего, использующий механизм «вызов-ответ».
- **MS-CHAP является реализацией протокола CHAP**, в которой предусмотрены механизм возврата сообщений об ошибках аутентификации и возможность изменения пароля пользователя.
- Кроме того MS-CHAP обеспечивает создание ключей шифрования для протокола MPPE, совместно с которым применяется в Microsoft PPTP.

EAP (Extensible Authentication Protocol)

- **EAP (англ. Extensible Authentication Protocol, Расширяемый Протокол Аутентификации) — фреймворк аутентификации**, который часто используется в беспроводных сетях и соединениях точка-точка. Формат был впервые описан в RFC 3748 и обновлён в RFC 5247.
- EAP используется для выбора метода аутентификации, передачи ключей и обработки этих ключей подключаемыми модулями называемыми методами EAP. **Существует множество методов EAP**, как определенных вместе с самим EAP, так и выпущенных отдельными производителями. EAP не определяет канальный уровень, он только определяет формат сообщений. Каждый протокол использующий EAP имеет собственный протокол инкапсуляции сообщений EAP.
- **EAP довольно популярный формат, он используется в IEEE 802.11 (WiFi), около ста методов EAP из IEEE 802.1X были приняты в качестве официальных механизмов аутентификации в стандартах WPA и WPA2**.

RADIUS (Remote Authentication Dial-in User Service)

- **Протокол аутентификации Remote Authentication Dial-in User Service (RADIUS)** рассматривается как механизм аутентификации и авторизации удалённых пользователей в условиях распределённой сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учёту для служб удалённого доступа.
- **RADIUS используется как протокол AAA.**
- В рамках стандарта выделяются следующие **роли**:
  - **Клиент RADIUS**. Клиент RADIUS принимает от пользователей запросы на аутентификацию. Все принятые запросы переадресовываются серверу RADIUS для последующей аутентификации и авторизации. Как правило, в качестве клиента протокола RADIUS выступает сервер удалённого доступа.
  - **Сервер RADIUS**. Основная задача сервера RADIUS заключается в централизованной обработке информации, предоставленной клиентами RADIUS. Один сервер способен обслуживать несколько клиентов RADIUS. Сервер осуществляет проверку подлинности пользователя и его полномочий. При этом в зависимости от реализации сервера RADIUS для проверки подлинности используются различные базы данных учётных записей.
  - **Посредник RADIUS**. Взаимодействие клиентов и серверов RADIUS осуществляется посредством специальных сообщений. В распределённых сетях клиент и сервер RADIUS могут быть разделены различными сетевыми устройствами (такими, например, как маршрутизатор). Под посредником RADIUS понимается сетевое устройство, способное осуществлять перенаправление сообщений протокола RADIUS.

RADIUS (Remote Authentication Dial-in User Service)

- Поддержка протокола RADIUS реализована на многих современных платформах, что позволяет использовать его в межплатформенных решениях.
- **В качестве примера сервера и посредника RADIUS** можно привести реализованную в Windows Server 2003 службу проверки подлинности в Интернете (**Internet Authentication Service, IAS**).
- Эта служба позиционируется как механизм централизованной аутентификации и авторизации пользователей, использующих различные способы подключений к сети. **Служба IAS интегрирована с другими сетевыми службами Windows Server 2003**, такими, как служба маршрутизации и удалённого доступа и служба каталога **Active Directory**.

RADIUS (Remote Authentication Dial-in User Service)

- В RADIUS применяются **модели разграничения доступа**
  - **DAC - Discretionary access control** (дискреционная модель разграничения доступа)
  - **MAC - Mandatory access control** (мандатная модель разграничения доступа)
  - **RBAC - Role-based access control** (ролевая модель разграничения доступа)
  - **ABAC - Attribute-based access control** (модель разграничения доступа на основе атрибутов)
  - **Гибридные модели**

DIAMETER

- **DIAMETER — сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS.** Обеспечивает взаимодействие между клиентами в целях аутентификации, авторизации и учёта различных сервисов (AAA, англ. authentication, authorization, accounting).
- В основе протокола DIAMETER лежит концепция в создании базового протокола с возможностью его расширения для предоставления сервисов AAA при появлении новых технологий доступа.
- Описание: RFC 6733 (Diameter Base Protocol), RFC 3589 (Diameter Command Codes for 3GPP), RFC 4006 (Diameter Credit-Control Application).

Diameter

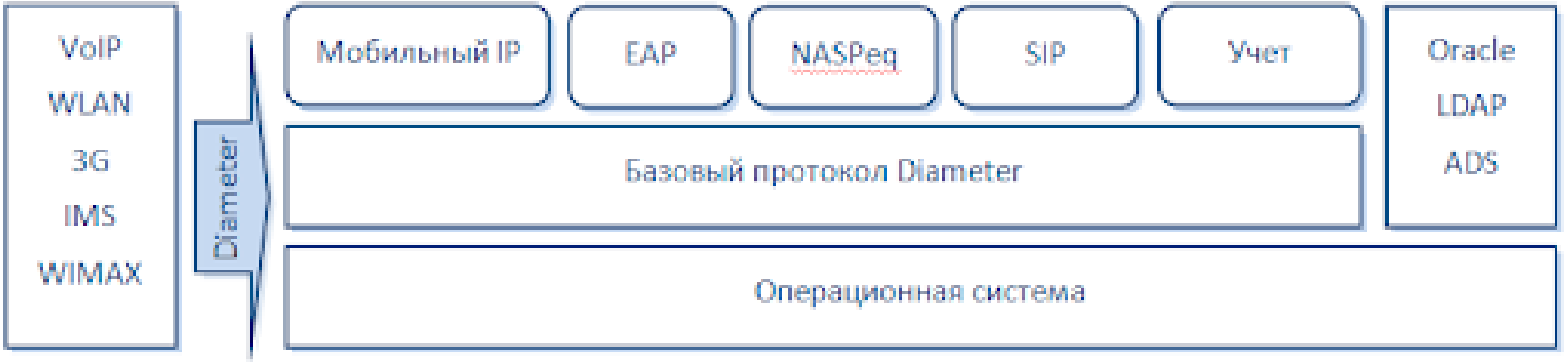
- Одно время все удаленные подключения осуществлялись по протоколам PPP и SLIP, а аутентификация пользователей производилась через PAP или CHAP. Но сегодня технологии стали значительно сложнее, появилось множество различных устройств и протоколов, между которыми можно выбирать. **Сегодня мы хотим, чтобы наши беспроводные устройства и смартфоны могли аутентифицироваться в нашей сети**, мы используем протоколы роуминга, мобильные IP, PPP через Ethernet, голос через IP (VoIP) и т.п. **Традиционные AAA-протоколы не могут работать со всем этим.**
- **Поэтому был разработан новый AAA-протокол Diameter, который решает эти проблемы, а также многие другие.**

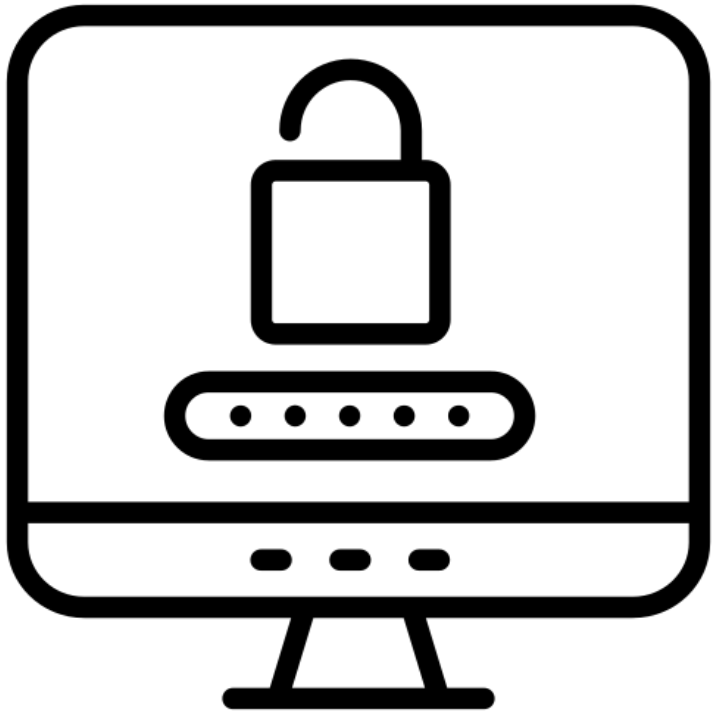
Diameter

- **Diameter – это протокол, разработанный на базе функциональности RADIUS, устраняющий многие из его ограничений.**
- **Diameter – это еще один AAA-протокол**, предоставляющий такую же функциональность, как RADIUS и TACACS+, но являющийся более гибким и отвечающий современным требованиям.
- Название **DIAMETER** - игра слов, отражающая превосходство нового протокола над предшественником RADIUS (диаметр - удвоенный радиус). Diameter не имеет обратной совместимости по отношению к RADIUS, но предоставляет механизмы миграции.
- Diameter является основным протоколом архитектуры IMS.

Diameter

- **Протокол Diameter состоит из двух частей.**
- **Первая часть** – это базовый протокол, который обеспечивает безопасное взаимодействие между участниками Diameter, определение характеристик и соглашение о версии.
- **Вторая** является расширением, которое надстроено над базовым протоколом. Эта часть позволяет различным технологиям использовать Diameter для аутентификации.





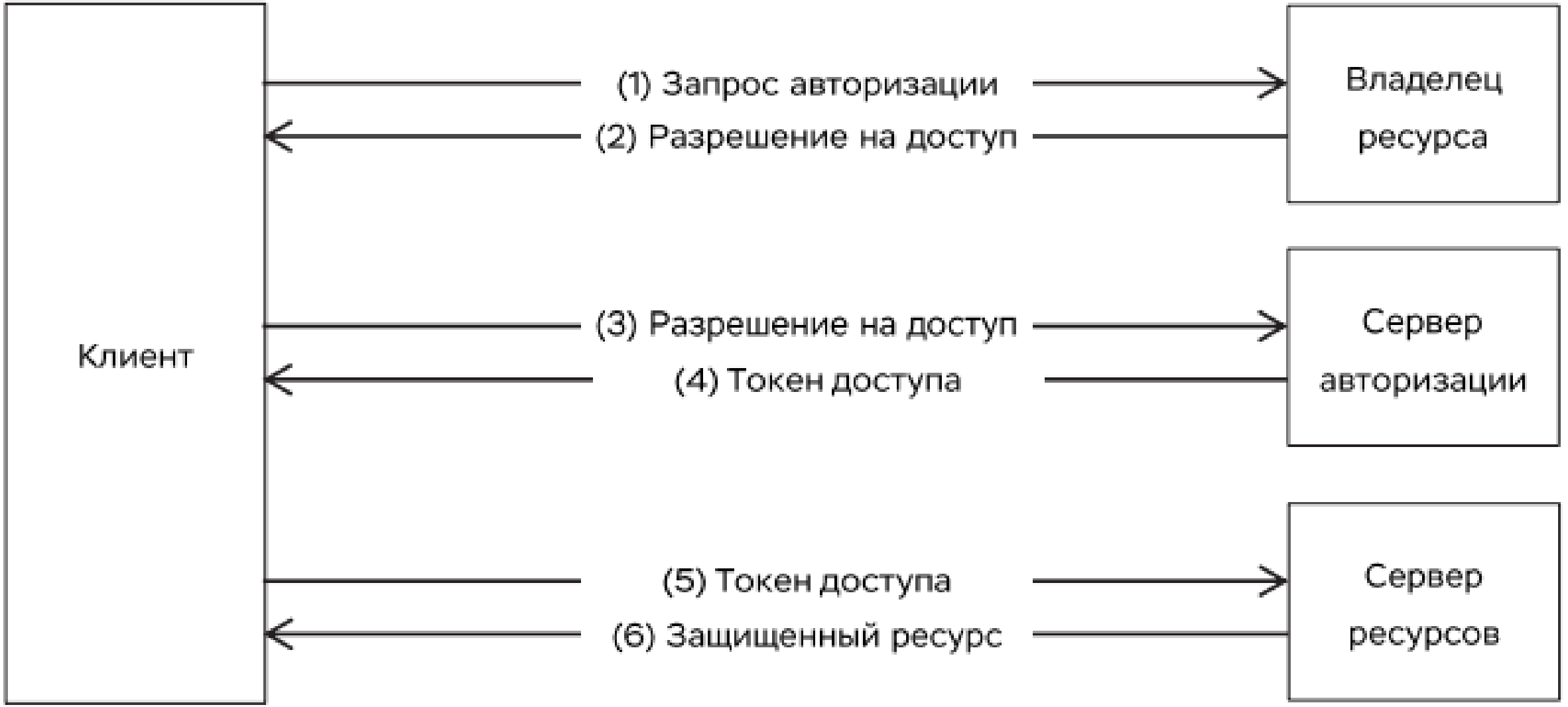
Протоколы аутентификации

Децентрализованная аутентификация (OAuth 2.0, OpenID Connect)

Технология авторизации OAuth 2.0

- **OAuth 2.0 – семейство протоколов авторизации, позволяющих одному приложению – клиенту – получить доступ к данным другого приложения – сервера ресурсов**. При этом клиент получает разрешение на доступ от имени пользователя – владельца ресурса, который владеет необходимыми учетными данными, позволяющими его аутентифицировать. Непосредственно разрешение на доступ (grant) выдает клиенту сервер авторизации, на котором зарегистрирован владелец ресурса. Сервер ресурсов и сервер авторизации могут совпадать.
- Сведения о спецификации OAuth 2.0 приведены в документах RFC 6749 и RFC 6750

Сценарий протокола OAuth 2.0



Сценарий протокола OAuth 2.0

1 Клиент запрашивает авторизацию у владельца ресурса. Запрос авторизации может быть направлен владельцу ресурса напрямую, или косвенно через сервер авторизации. Предпочтительным является второй вариант.

2 Клиент получает разрешение на доступ (grant), структуру данных, представляющую авторизацию владельца ресурса, выраженную с использованием одного из четырех типов разрешений: код авторизации (authorization code), неявное разрешение (implicit), пароль владельца ресурса (resource owner password credentials) и учетные данные клиента (client credentials). Тип разрешения на доступ зависит от метода, используемого клиентом для запроса авторизации, и типов разрешений, поддерживаемых сервером авторизации. Типы разрешений, поддерживаемые сервером авторизации, определяются при его разработке, исходя из его прикладных целей и задач. Настоящий стандарт регламентирует использование в качестве типа разрешения код авторизации.

3 Клиент запрашивает токен доступа посредством аутентификации на сервере авторизации и предоставления разрешения на доступ.

4 Сервер авторизации аутентифицирует клиента, проверяет разрешение на доступ и, если оно действительно, выдает токен доступа.

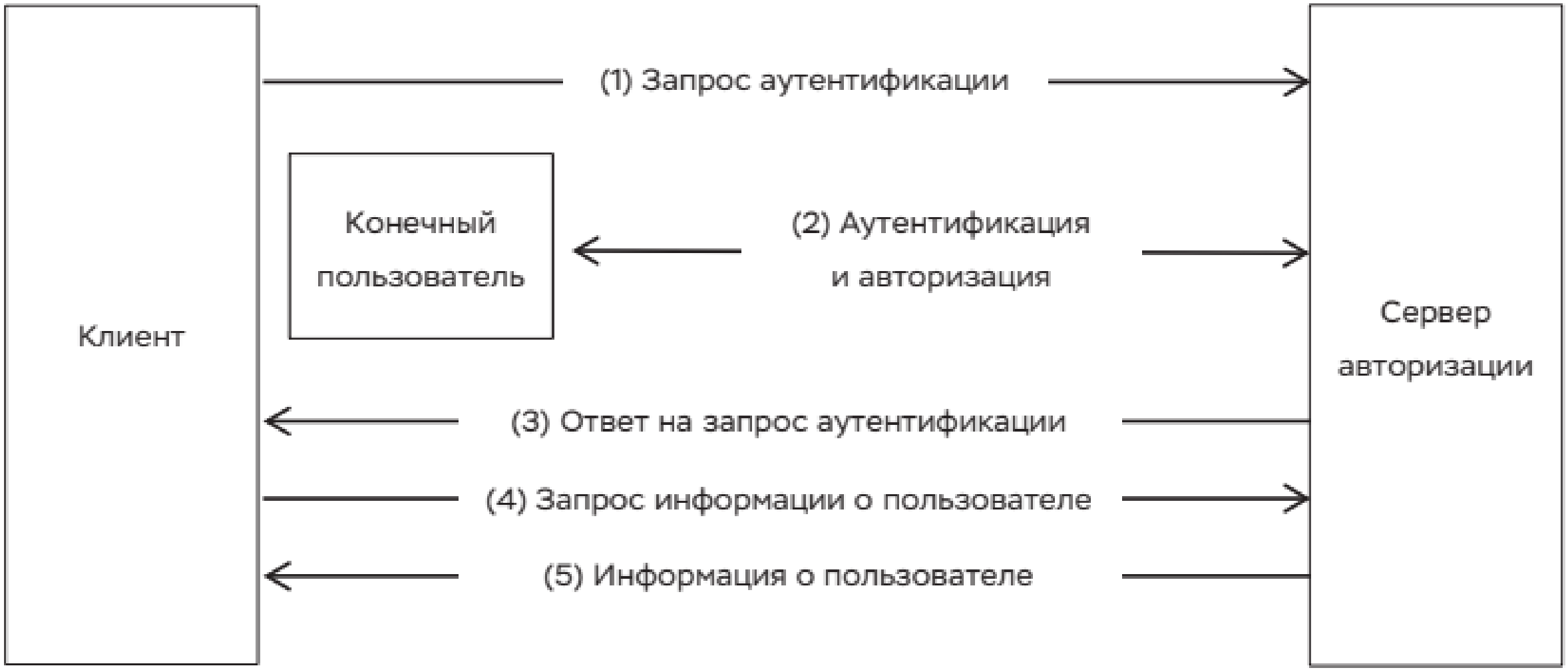
5 Клиент запрашивает защищенный ресурс на сервере ресурсов и аутентифицируется, представляя токен доступа.

6 Сервер ресурсов проверяет токен доступа и, если он действителен, обслуживает запрос.

Протокол OpenID Connect

- Протокол **OpenID** Connect. OIDC - семейство протоколов, являющихся расширением протоколов OAuth 2.0, позволяющих расширить их функционал путем более точного описания процесса аутентификации владельца ресурса и возможности клиенту получить информацию о нем.
- **OpenID** — открытый стандарт децентрализованной системы аутентификации, предоставляющей пользователю возможность создать единую учётную запись для аутентификации на множестве не связанных друг с другом интернет-ресурсов, используя услуги третьих лиц

Протокол OpenID Connect



Протокол OpenID Connect

- **Схематично протокол OpenID Connect выглядит следующим образом:**
- 1 Клиент отправляет серверу авторизации запрос аутентификации.
- 2 Сервер авторизации аутентифицирует конечного пользователя и получает согласие пользователя на доступ клиента к запрошенному ресурсу.
- 3 Сервер авторизации отвечает клиенту ID токеном и (опционально) токеном доступа.
- 4 Клиент может отправить серверу авторизации запрос информации о пользователе по токену доступа.
- 5 Сервер авторизации возвращает клиенту информацию о конечном пользователе.

Протокол OpenID Connect

- Сервер авторизации **OpenID Connect поддерживает три сценария аутентификации**, реализующие этот сценарий:
  - **с генерацией кода авторизации** (Authorization Code Flow),
  - **неявный сценарий** (Implicit Flow),
  - **гибридный сценарий** (Hybrid Flow).

  Настоящий стандарт не предполагает использование неявного сценария.

- Передача сообщений между клиентом и сервером авторизации (на конечных точках авторизации, токена и UserInfo) должна производиться с использованием протокола TLS.

Отличие OAuth и OpenID

- Хотя OAuth и OpenID имеют много общего, OAuth является самостоятельным протоколом, никак не связанным с OpenID:
- **OAuth является протоколом авторизации**, который позволяет предоставить права на использование какого-то ресурса (например, API какого-либо сервиса). Наличие прав определяется токеном (уникальным идентификатором), который может быть одним и тем же для разных пользователей, или же у одного пользователя в разное время могут быть разные токены. Предоставление прав происходит в обмен на предоставление токена. В общем случае нельзя определить, кому принадлежит токен и кто в настоящий момент пользуется правами.
- **OpenID является средством аутентификации**: с помощью этой системы можно удостовериться, что пользователь — именно тот, за кого себя выдаёт. Какие действия сможет совершать пользователь, прошедший аутентификацию посредством OpenID, определяется стороной, проводящей аутентификацию.

Отличие OAuth и OpenID

- **OAuth 2.0 разработан только для авторизации** — для предоставления доступа к данным и функциям от одного приложения другому. **OpenID Connect (OIDC) — это тонкий слой поверх OAuth 2.0, добавляющий сведения о логине и профиле пользователя**, который вошел в учетную запись.
- **OpenID Connect позволяет реализовывать сценарии**, когда единственный логин можно использовать во множестве приложений, — этот подход также известен как **single sign-on (SSO)**

Протоколы аутентификации

Протоколы аутентификации в беспроводных сетях (wi-fi)

Беспроводная связь

- **Беспроводная связь** относится к любому типу обмена данными между сторонами, который осуществляется по беспроводной связи (по беспроводной связи).
- Это определение чрезвычайно широко, так как оно может соответствовать многим типам беспроводных технологий, таких как:
  - **Wi-Fi сеть связи**
  - Bluetooth связь
  - Спутниковая связь
  - Мобильная связь
- Все технологии, упомянутые выше, используют различную коммуникационную архитектуру, однако все они имеют одинаковую возможность «Wireless Medium».

Беспроводные клиенты

- Беспроводными клиентами считаются любые конечные устройства с установленной беспроводной картой или беспроводным адаптером.
- Эти устройства могут быть почти чем угодно:
  - Современные смартфоны (Bluetooth, Wi-Fi, GSM)
  - Ноутбуки (Bluetooth, Wi-Fi)
  - SmartWatch (Bluetooth)
  - Оборудование для «умного дома» (Wi-Fi)
  - и др.

Беспроводная безопасность — сеть

Категория	покрытие	Примеры	Приложения
Беспроводная персональная сеть (**WPAN**)	Очень короткий — максимум 10 метров, но обычно намного меньше	Bluetooth, 802.15, ИК-связь	•Обмен данными между смартфонами •Гарнитуры •Умные часы
Беспроводная локальная сеть (**WLAN**)	Умеренный — внутри квартир или рабочих мест.	802.11 Wi-Fi	Беспроводное расширение локальной сети, используемое в •Компании •рынки •аэропорт •Главная
Беспроводная городская сеть (**WMAN**)	По всему городу	Wimax, IEEE 802.16 или проприетарные технологии	Между домами и бизнесом
Беспроводная глобальная сеть (**WWAN**)	По всему миру	3G, LTE	Беспроводной доступ в интернет от

Беспроводная безопасность — точка доступа

- Точка доступа (AP) Wi-Fi является центральным узлом в беспроводных реализациях 802.11.
- Это интерфейс между проводной и беспроводной сетью, с которым все беспроводные клиенты связываются и обмениваются данными.

Беспроводная безопасность — точка доступа

Базовая приемопередающая станция

- **Базовая приемопередающая станция (BTS)** является эквивалентом точки доступа из мира 802.11, но используется операторами мобильной связи для обеспечения покрытия сигнала, напр. 3G, GSM и т. Д.

Беспроводная безопасность — точка доступа

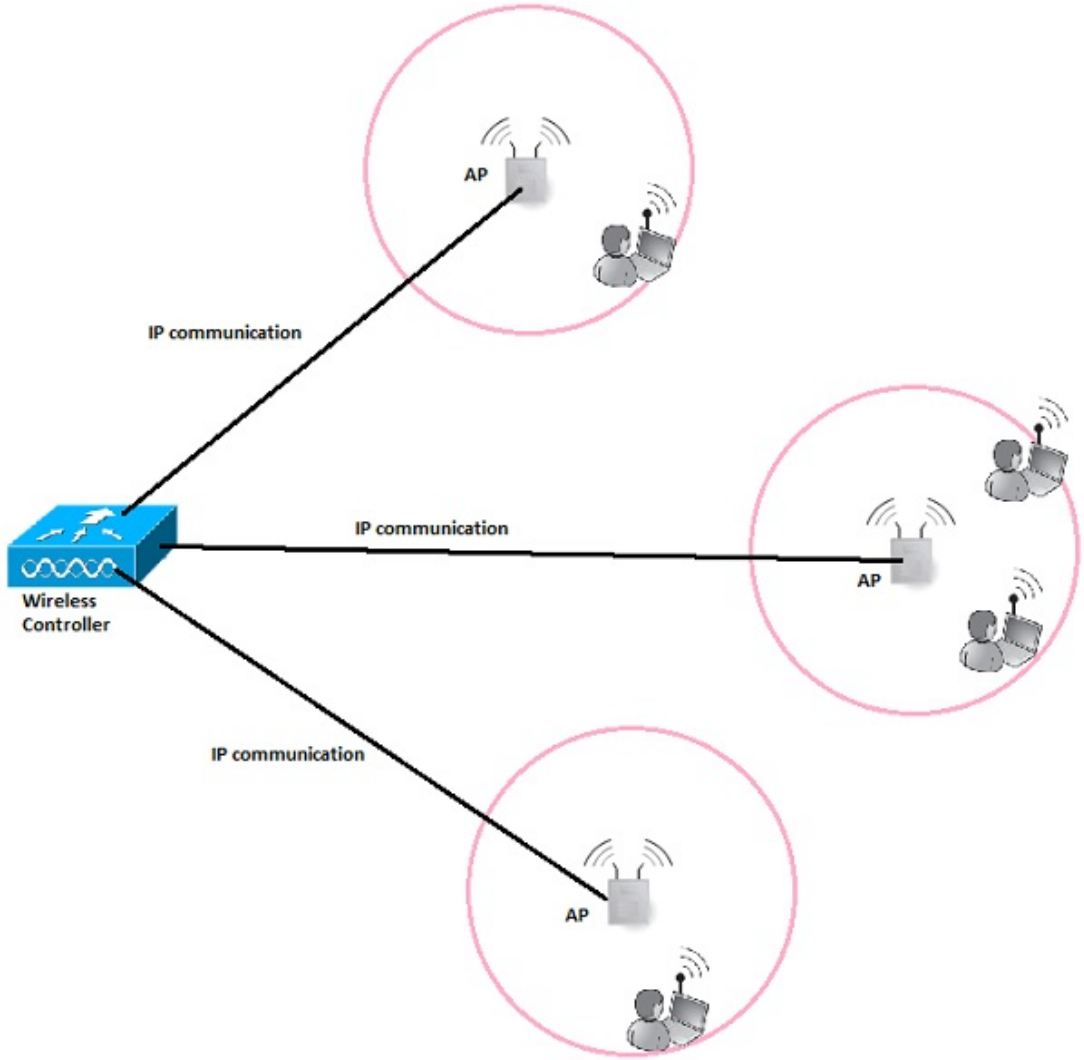
Базовая приемопередающая станция

- В корпоративной беспроводной реализации количество точек доступа часто исчисляется сотнями или тысячами единиц.
- Административно невозможно управлять всеми точками доступа и их конфигурацией (назначением каналов, оптимальной выходной мощностью, конфигурацией роуминга, созданием SSID для каждой точки доступа и т. д.)

Беспроводная безопасность — точка доступа

Базовая приемопередающая станция

Это ситуация, когда концепция беспроводного контроллера вступает в игру. Это «Мастер», стоящий за всей работой беспроводной сети. Этот централизованный сервер, имеющий IP-подключение ко всем точкам доступа в сети, позволяет легко управлять ими всеми из единой платформы управления, выдвигать шаблоны конфигурации, отслеживать пользователей со всех точек доступа в режиме реального времени и т. д.



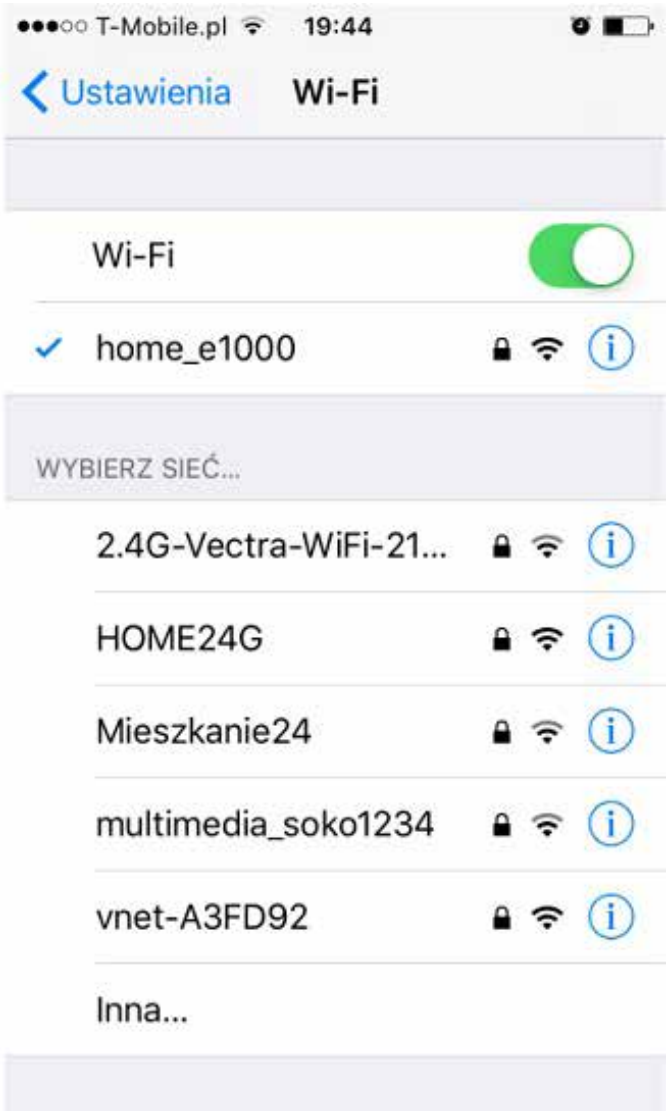
Wi-Fi

- **Wireless Fidelity (Wi-Fi)** относится к беспроводной локальной сети, как мы все их знаем. **Он основан на стандарте IEEE 802.11**.
- Wi-Fi — это тип беспроводной сети, которую вы встречаете практически везде, дома, на работе, в отелях, ресторанах и даже в такси, поездах или самолетах. Эти стандарты связи 802.11 **работают в диапазонах ISM 2,4 ГГц или 5 ГГц.**

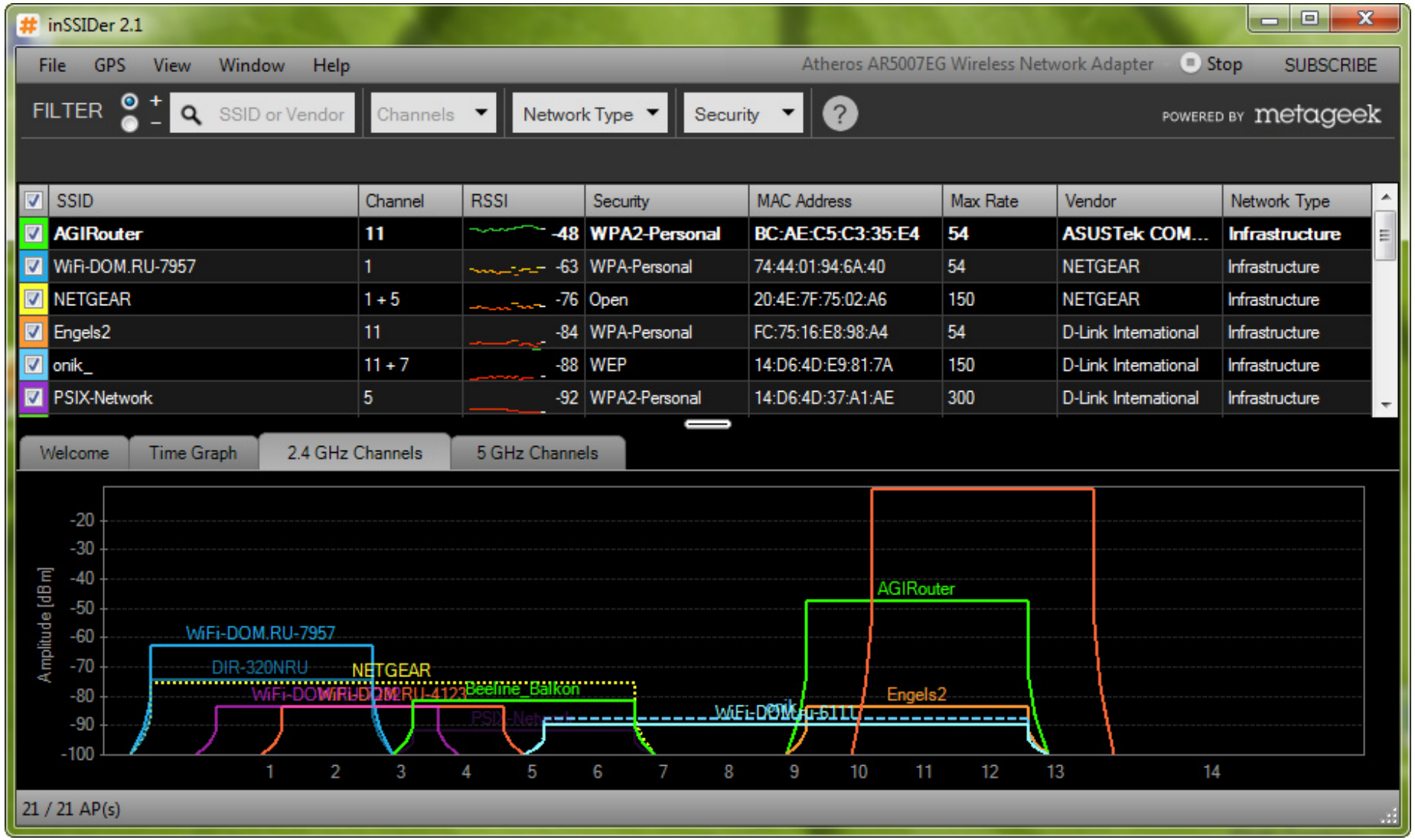
стандарт	частота	максимальная скорость
802,11	2,4 ГГц	2 Мбит / с
802.11a	5 ГГц	54 Мбит / с
802.11b	2,4 ГГц	11 Мбит / с
802.11g	2,4 ГГц	54 Мбит / с
802.11n	2,4 или 5 ГГц	600 Мбит / с
802.11ac	5 ГГц	1 Гбит / с

Идентификатор набора услуг (SSID)

SSID напрямую идентифицирует сам беспроводной WLAN. Для подключения к беспроводной локальной сети беспроводному клиенту необходимо отправить тот же точный SSID в кадре ассоциации, что и имя SSID, предварительно настроенное на точке доступа.



inSSIDer

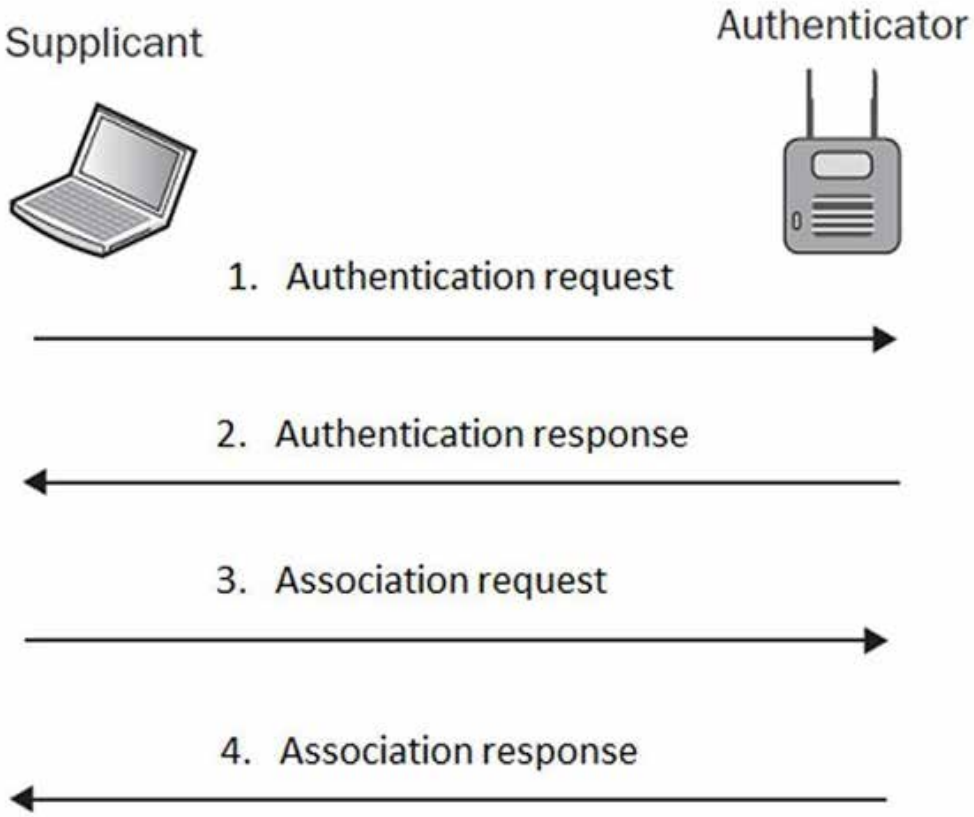


InSSIDer – программное обеспечение, которое позволяет качественно и функционально сканировать беспроводные сети в вашем окружении (https://insssider.com , https://www.metageek.com/products/inssider/)

Режимы аутентификации беспроводной безопасности Wi-Fi - Открытая аутентификация

Сам термин **«открытая аутентификация»** вводит в заблуждение. Предполагается, что существует какая-то аутентификация, но **на самом деле процесс аутентификации в этой схеме больше похож на формальный шаг**, чем на механизм аутентификации. Процесс выглядит так, как показано на рисунке.

Говоря простым языком, этот обмен говорит о том, что в запросе на аутентификацию беспроводной клиент (соискатель) говорит: «Привет, AP, я хотел бы аутентифицироваться», а в ответе аутентификации от AP говорится: «Хорошо, вот и все».



Видите ли вы какой-либо безопасности в этой настройке? И я нет...
Вот почему открытую аутентификацию никогда не следует использовать, поскольку она просто позволяет любому клиенту проходить аутентификацию в сети без правильной проверки безопасности.

Режимы аутентификации беспроводной безопасности Wi-Fi – Протоколы аутентификации

- В инфраструктуре IEEE 802.1x существуют **два протокола**, используемых для транспортировки сообщений аутентификации между клиентом и сервером аутентификации:
  1. расширяемый протокол аутентификации Extensible Authentication Protocol (**EAP**)
  2. и протокол аутентификации для удаленного доступа к пользовательским сервисам **RADIUS**.

Протокол RADIUS

Протокол RADIUS всегда используется провайдерами интернет-услуг (ISP) для предоставления централизованных служб аутентификации.

Он используется IEEE 802.1x для транспортировки между аутентификатором и сервером аутентификации. Во время аутентификации аутентификатор отвечает за преобразование инкапсуляции между EAPoL и RADIUS, соответственно. Оба протокола обеспечивают гибкость для известных методов аутентификации. После каждой аутентификации аутентификатор поддерживает состояние авторизации для каждого клиента на некоторое время, идентифицируя их по MAC-адресам. После того, как время авторизации истекает, клиент вынужден снова выполнить повторную аутентификацию, даже если он подключен к тому же аутентификатору, что и ранее. Статус авторизации должен периодически обновляться из-за тайм-аута аутентификатора или тайм-аута сеанса RADIUS.

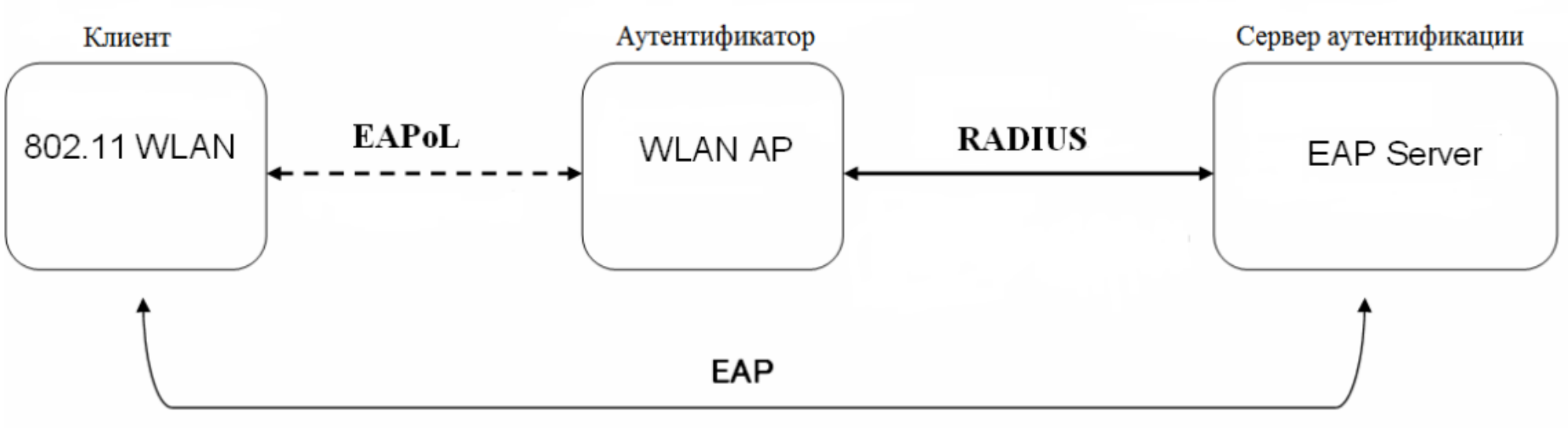
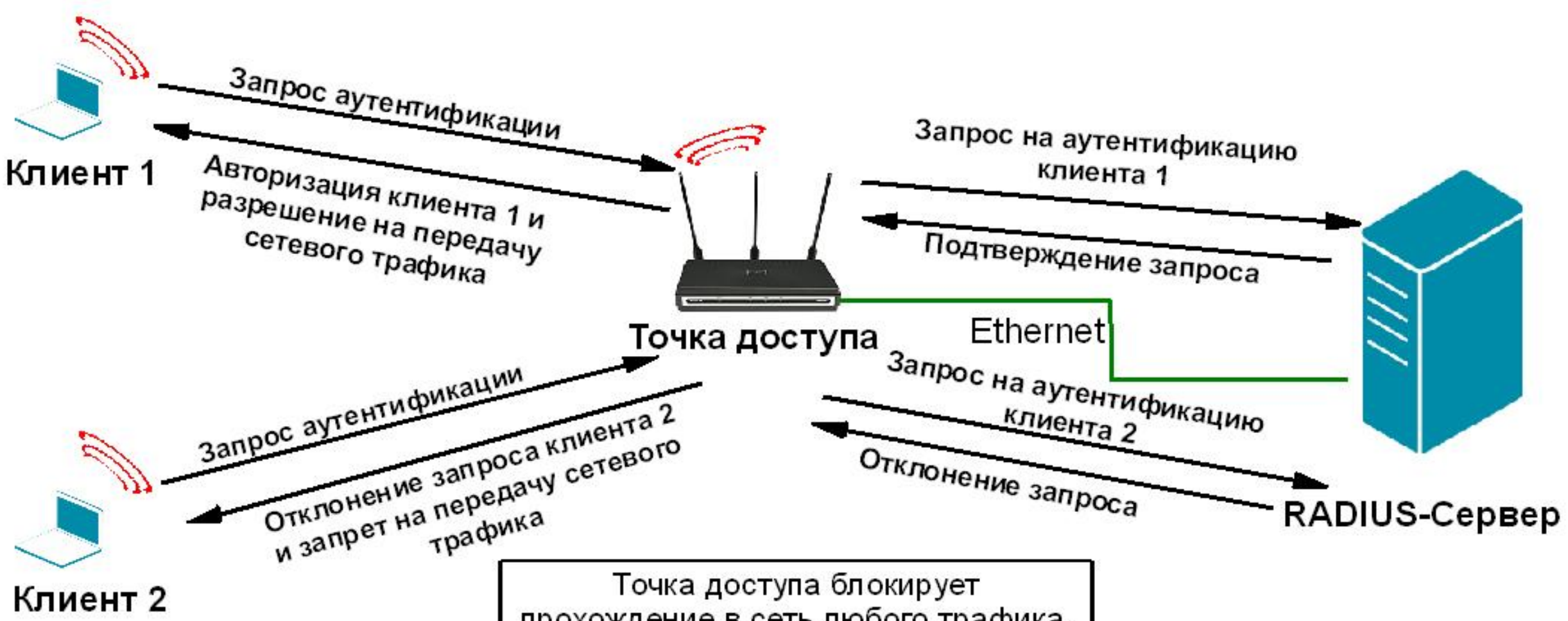


Схема взаимодействия между объектами 802.1X

Процесс аутентификации



Точка доступа блокирует прохождение в сеть любого трафика, кроме 802.1x, до завершения процесса авторизации

Extensible Authentication Protocol (EAP)

- **EAP (англ. Extensible Authentication Protocol, Расширяемый Протокол Аутентификации)** — фреймворк аутентификации, который часто используется в беспроводных сетях и соединениях точка-точка. Формат был впервые описан в RFC 3748 и обновлён в RFC 5247.
- EAP используется для выбора метода аутентификации, передачи ключей и обработки этих ключей подключаемыми модулями называемыми методами EAP. Существует множество методов EAP, как определенных вместе с самим EAP, так и выпущенных отдельными производителями. EAP не определяет канальный уровень, он только определяет формат сообщений. Каждый протокол использующий EAP имеет собственный протокол инкапсуляции сообщений EAP.
- **EAP довольно популярный формат, он используется в IEEE 802.11 (WiFi), около ста методов EAP из IEEE 802.1X были приняты в качестве официальных механизмов аутентификации в стандартах WPA, WPA2 и WPA3.**

Extensible Authentication Protocol (EAP)

- Поскольку **EAP является фреймворком аутентификации**, а не конкретным механизмом, он обеспечивает некоторые общие функции и согласование методов проверки подлинности (методы EAP).
- **В настоящее время определено около 40 различных методов.**
- Обычно методы определяются в IETF, например: EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA и EAP-AKA и др.
- Также существуют методы и предложения конкретных поставщиков решений и производителей оборудования. Обычно используются современные методы, способные работать в беспроводных сетях, к примеру: EAP-TLS, EAP-SIM, EAP-AKA, LEAP и EAP-TTLS и др.

Некоторые варианты реализации 802.1x

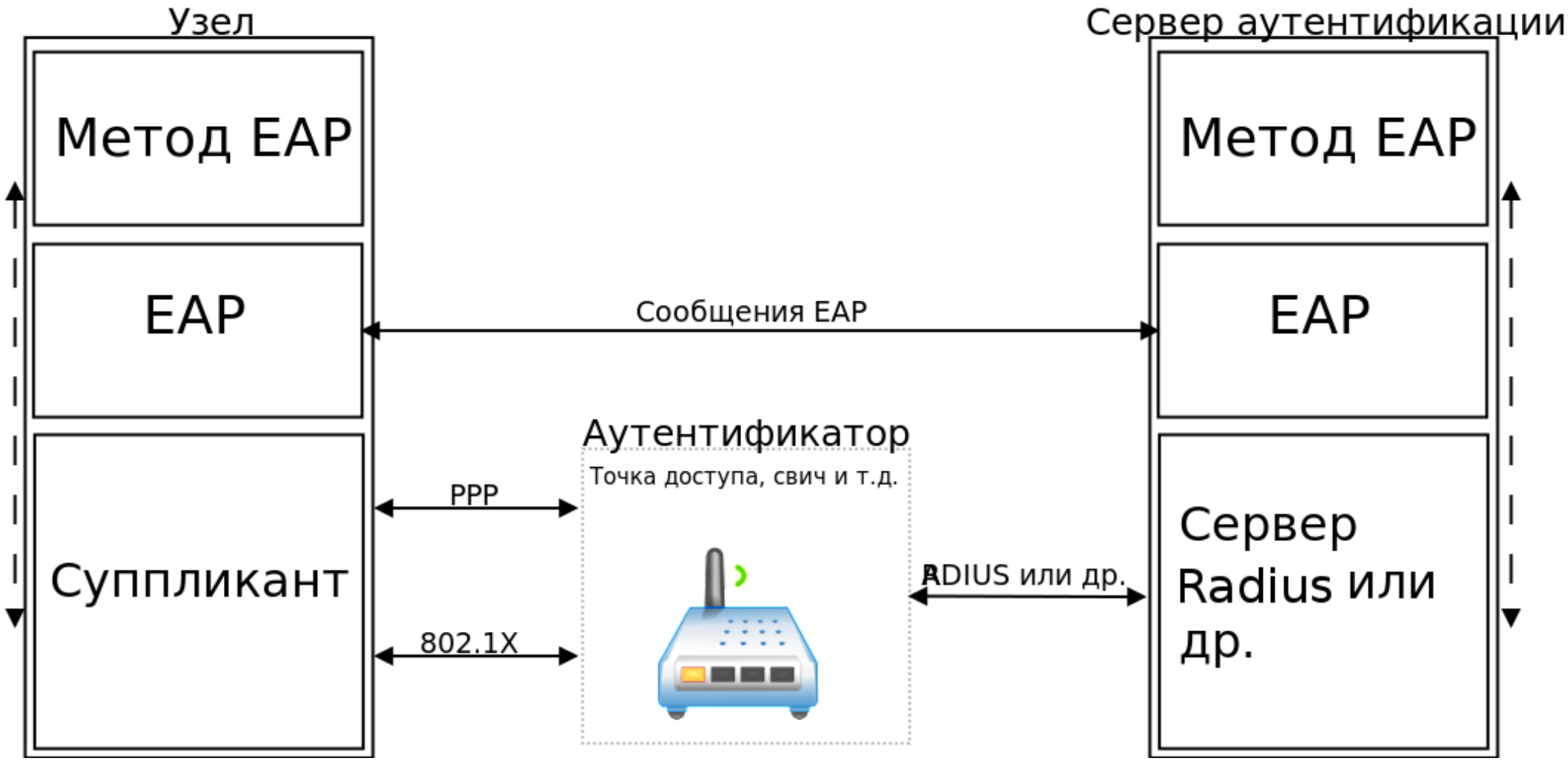
Comparing 802.1X Authentication Methods

Characteristics	EAP-TLS	Cisco Wireless EAP	PEAP Version 1 (with Generic Token Card)	PEAP Version 0 (with MS-CHAP Version 2)	EAP-FAST
User Authentication Database and Server	OTP LDAP Novell NDS Windows NT Domains Active Directory	Windows NT Domains Active Directory	OTP LDAP Novell NDS Windows NT Domains Active Directory	Windows NT Domains Active Directory	Windows NT Domains Active Directory LDAP
Server Certificates Required?	Yes	No	Yes	Yes	No
Client Certificates Required?	Yes	No	No	No	No
Operating Systems	Windows XP/2000/CE Other OSes supported with third-party utility.	Windows 98/2000/NT/ME/XP/CE Mac OS Linux DOS	Windows XP/2000/CE Other OSes supported with third-party utility.	Windows XP/2000/CE Other OSes supported with third-party utility.	Windows XP/2000/CE Other OSes supported with third-party utility.
Characteristics	EAP-TLS	Cisco Wireless EAP	PEAP Version 1 (with Generic Token Card)	PEAP Version 0 (with MS-CHAP Version 2)	EAP-FAST
Credentials Used	Digital certificate	Windows password	Clients: Windows, Novell NDS, LDAP password, and OTP or token. Server: Digital certificate	Windows password Server: Digital certificate	Windows password, LDAP user ID and password PAC
Single Sign-On Using Windows Login?	Yes	Yes	No	Yes	Yes
Password Expiration and Change?		No	No	Yes	Yes
Fast Secure Roaming Compatible?	No	Yes	No	No	Yes
WPA Compatible?	Yes	Yes	Yes	Yes	Yes

Схема протокола Extensible Authentication Protocol (EAP)

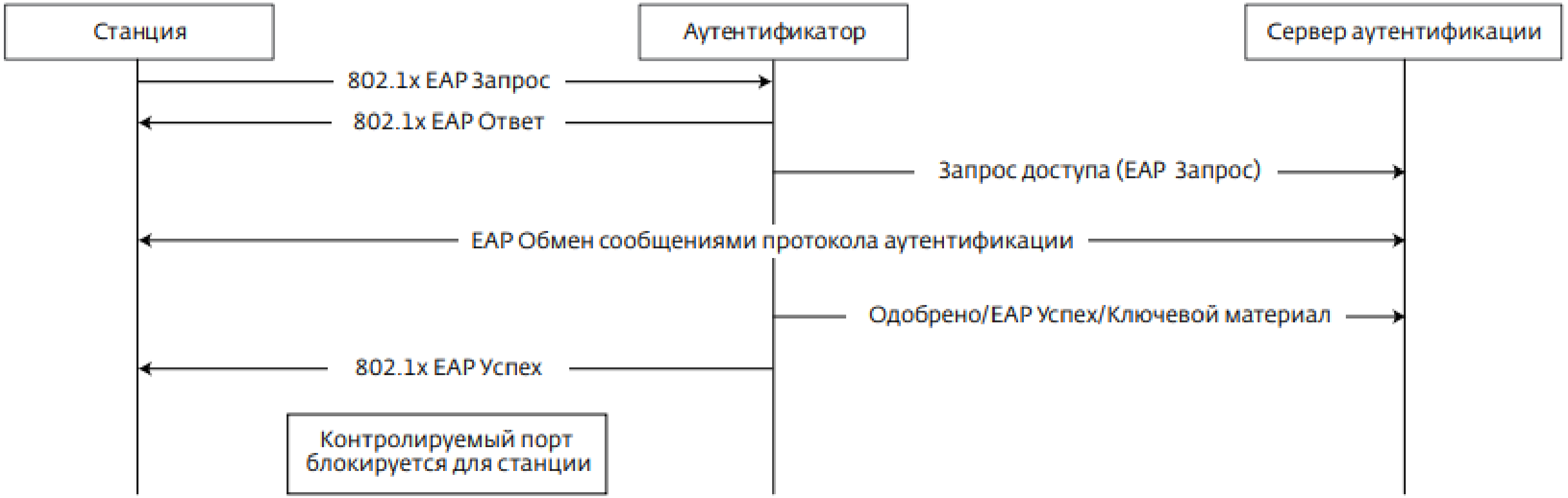
- В процессе аутентификации можно выделить три основных участника процесса:
  - **Аутентификатор** (англ. Authenticator) — участник процесса требующий провести аутентификацию (WiFi точка доступа, сетевой коммутатор и т. д.).
  - **Узел или клиент** (англ. Peer) — участник процесса который будет аутентифицирован (компьютер, ноутбук, телефон и т.д.).
  - **Сервер аутентификации** (англ. Authentication Server (AS)) — участник процесса способный по некоторым данным от узла аутентифицировать его.
- **В некоторых случаях сервер аутентификации и аутентификатор могут быть одним устройством, например домашние устройства использующие метод EAP-PSK.**

Схема протокола
Extensible Authentication Protocol (EAP)



Общая абстрактная схема работы EAP

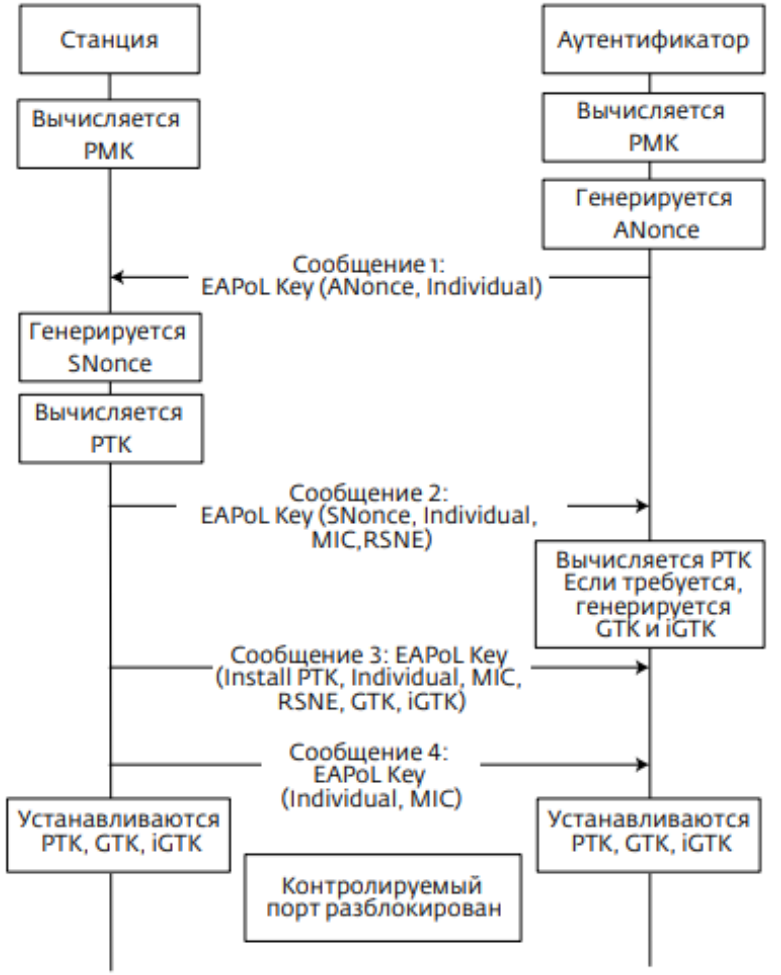
Аутентификация 802.1x с использованием протокола Extensible Authentication Protocol (EAP)



Четырехстороннее рукопожатие на основе EAP (Extensible Authentication Protocol) с WPA / WPA2

Когда беспроводной клиент аутентифицируется на AP, они оба проходят 4-х этапный процесс аутентификации, называемый **4-х сторонним рукопожатием** .

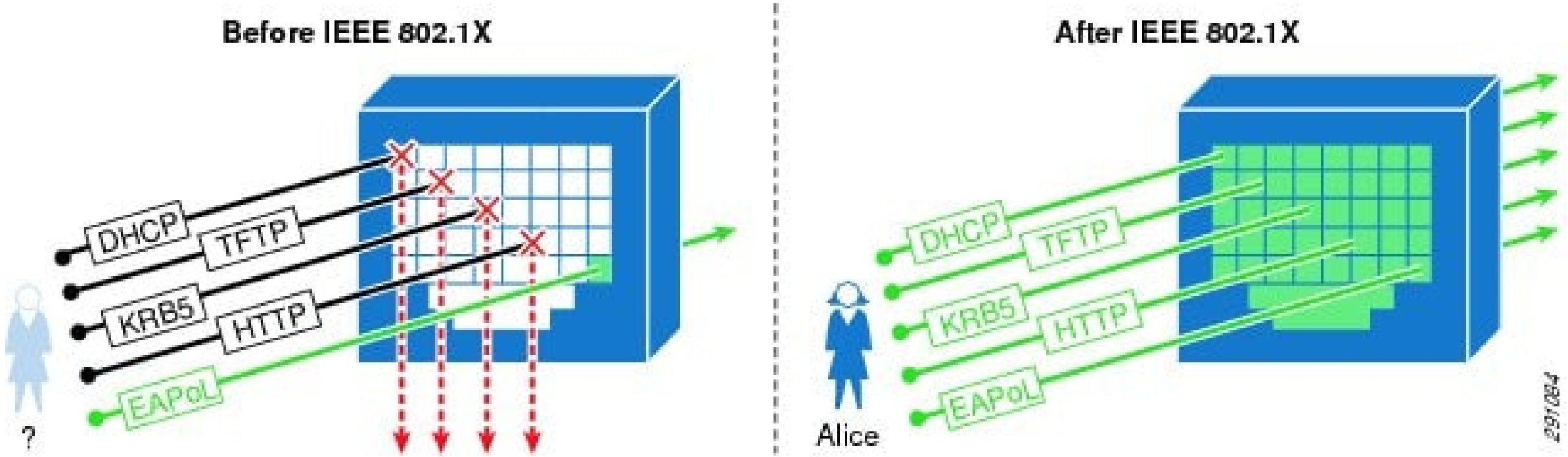
Во время этих обменов сообщениями общий пароль получается между AP и беспроводным клиентом, но не передается ни в одном из этих сообщений EAP.



Обмен сообщениями при выполнении четырехстороннего рукопожатия

- **4-way handshake.** Процедура рукопожатия начинается с вычисления клиентом и аутентификатором парного мастер-ключа (PMK). После генерации PMK начинается обмен сообщениями EAPoL-key.
- **В первом сообщении** аутентификатор посылает кадр EAPoL-key, содержащий Anonce (Authenticator Nonce). ANonce – одноразовое случайное или псевдослучайное число, которое генерируется с помощью счетчика глобальных ключей размером 256 бит, содержащегося в каждой беспроводной станции. Он инициализируется при загрузке системы. Значение счетчика устанавливается с помощью псевдослучайной функции Nonce: Nonce ← PRF-256(Random number, "Init Counter", Local MAC Address || Time), где PRF-256 – псевдослучайная функция (Pseudorandom Function), результат которой имеет размер 256 бит; Random number – случайное число; "Init Counter" – символьная строка; Local MAC Address – MAC-адрес устройства; Time – значение текущего времени в формате протокола NTP (Network Time Protocol).
- **Во втором сообщении** клиент генерирует случайное число SNonce (Supplicant Nonce) с помощью функции Nonce. Далее, используя полученный ANonce и сгенерированный SNonce, клиент вычисляет парный передаточный ключ (PTK - Pairwise Transient Key). Клиент посылает кадр EAPoL-key, который содержит SNonce, RSNE (Robust Security Network element) и код целостности сообщения MIC (Message Integrity Code). RSNE указывает на поддерживаемые узлом конфигурации безопасности и содержит в своем теле описание используемых криптографических профилей и механизмов AKM. Аутентификатор также использует ANonce и SNonce для вычисления PTK с помощью той же псевдослучайной функции, что и клиент. Также аутентификатор вычисляет MIC и сверяет его с полученным от клиента. Если аутентификатор обнаруживает несовпадение, сообщение отбрасывается. Далее аутентификатор отсылает третье сообщение, содержащее ANonce, RSNE из кадров Beacon или Probe Response, MIC, а также указание клиенту на возможность установки временных ключей. В завершающем сообщении клиент отсылает MIC и указание на то, что ключи установлены.
- Вычисление парного передаточного ключа - одна из важнейших задач, выполняемых с помощью процедуры четырехстороннего рукопожатия, так как именно этот ключ содержит в себе ключевой материал для дальнейших криптографических преобразований. Вся совокупность ключей стандарта 802.11-2012 представляется с помощью иерархии ключевого материала.

Доступ к сети по умолчанию До и После 802.1 X



Перед аутентификацией идентификатор конечной точки неизвестен, и весь трафик блокируется. После аутентификации становится известна личность конечной точки, и весь трафик с этой конечной точки разрешен. Коммутатор выполняет фильтрацию исходного MAC-адреса, чтобы гарантировать, что только прошедшей проверку подлинности конечной точке разрешено отправлять трафик.

Защита информации

Тема: Идентификация, аутентификация и авторизация

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024