Вебинар

«Железная» аутентификация с помощью Рутокен OTP и U2F

Владимир Салыкин
Менеджер по продуктам
Компания «Актив»

https://www.youtube.com/user/AktivCompany

Компания «Актив»

Крупнейший российский производитель аппаратных средств аутентификации и электронной подписи, разработчик и поставщик комплексных решений в сфере информационной безопасности. Компания основана в 1994 году.

Направления деятельности

РУТОКЕН

Продукты и решения в области аутентификации, защиты информации и электронной подписи.

Guardant

Средства защиты и лицензирования программного обеспечения.

А теперь немного теории…

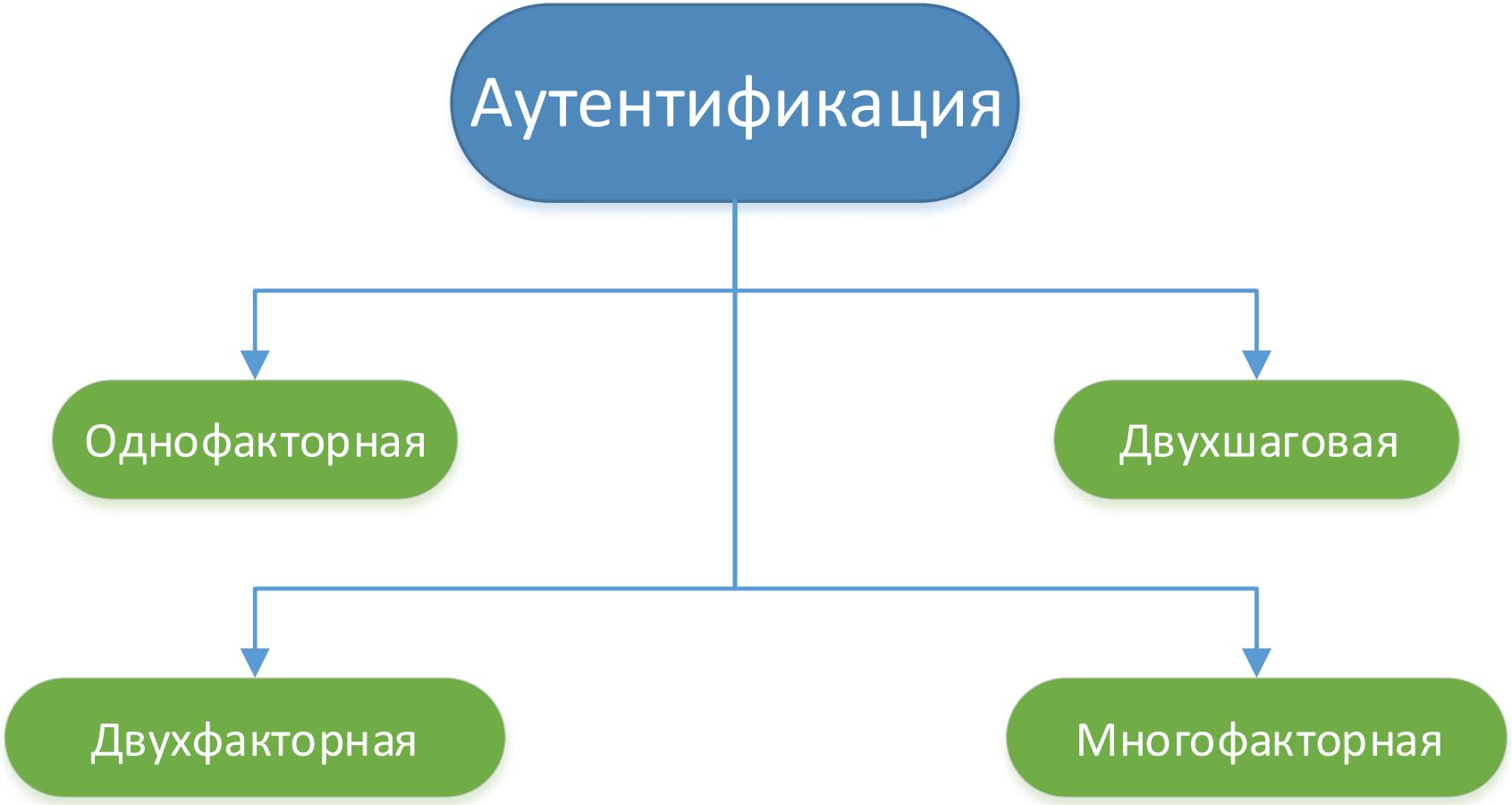
Определение

- Формально. Аутентификация - процесс проверки принадлежности субъекту прав доступа к информационным ресурсам системы в соответствии с предъявленным им идентификатором
- Не формально. Доказательство того, что идентификатор принадлежит пользователю.

Факторы аутентификации

- Нечто, чем мы обладаем
  например, какой-либо уникальный физический объект
- Нечто, что нам известно
  например, какая-либо секретная информация
- Нечто, что является неотъемлемой частью нас самих
  биометрика

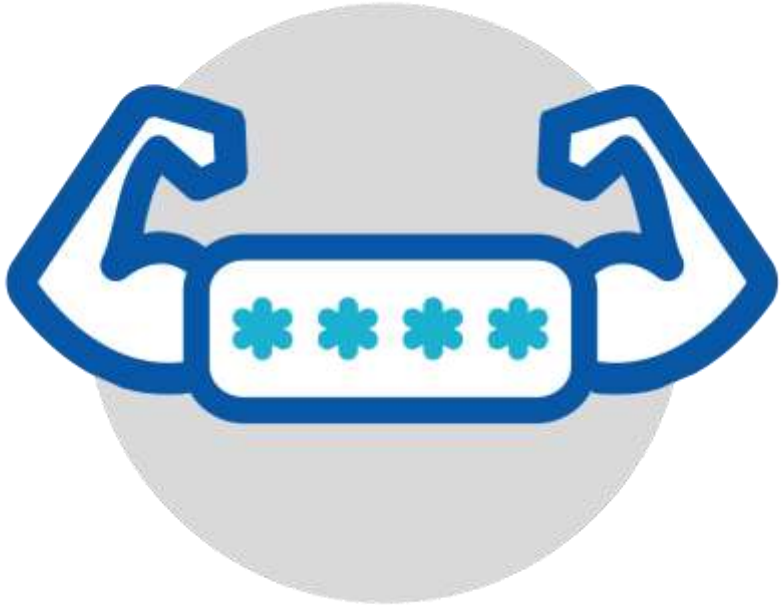
Аутентификация и факторы



Поговорим про пароли

Достоинства “Классических” паролей

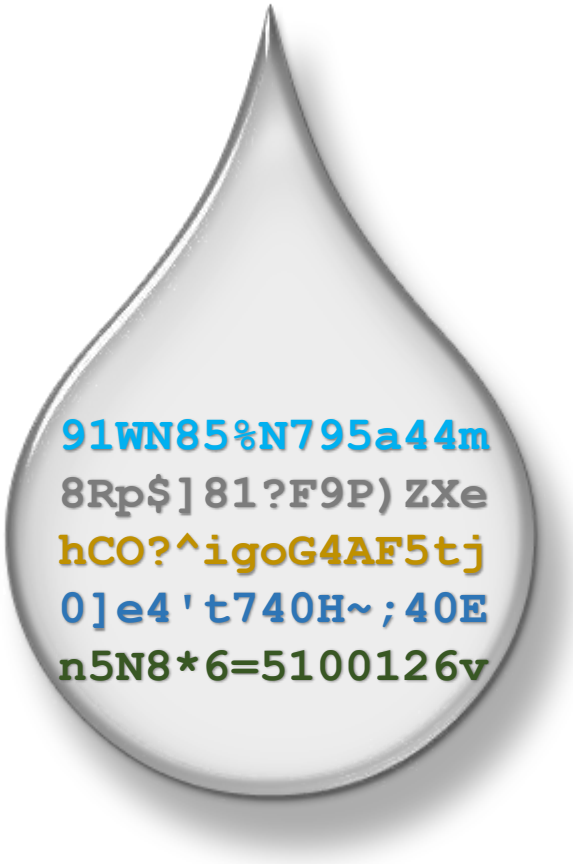
- Самая привычная технология для пользователей
- Самая распространённая технология для разработчиков
- Не требует дополнительных технических средств (телефонов, токенов, смарт-карты, считывателя биометрии и т.д.)
- Больше всего технических решений по упрощению работы
- Легко восстанавливается при компрометации



40En5N8*6=goG4A26v

«Сильный» пароль нужно:

- Придумать
- Запомнить
- Набрать на клавиатуре
- Никому не показывать
- Повторять всё это периодически

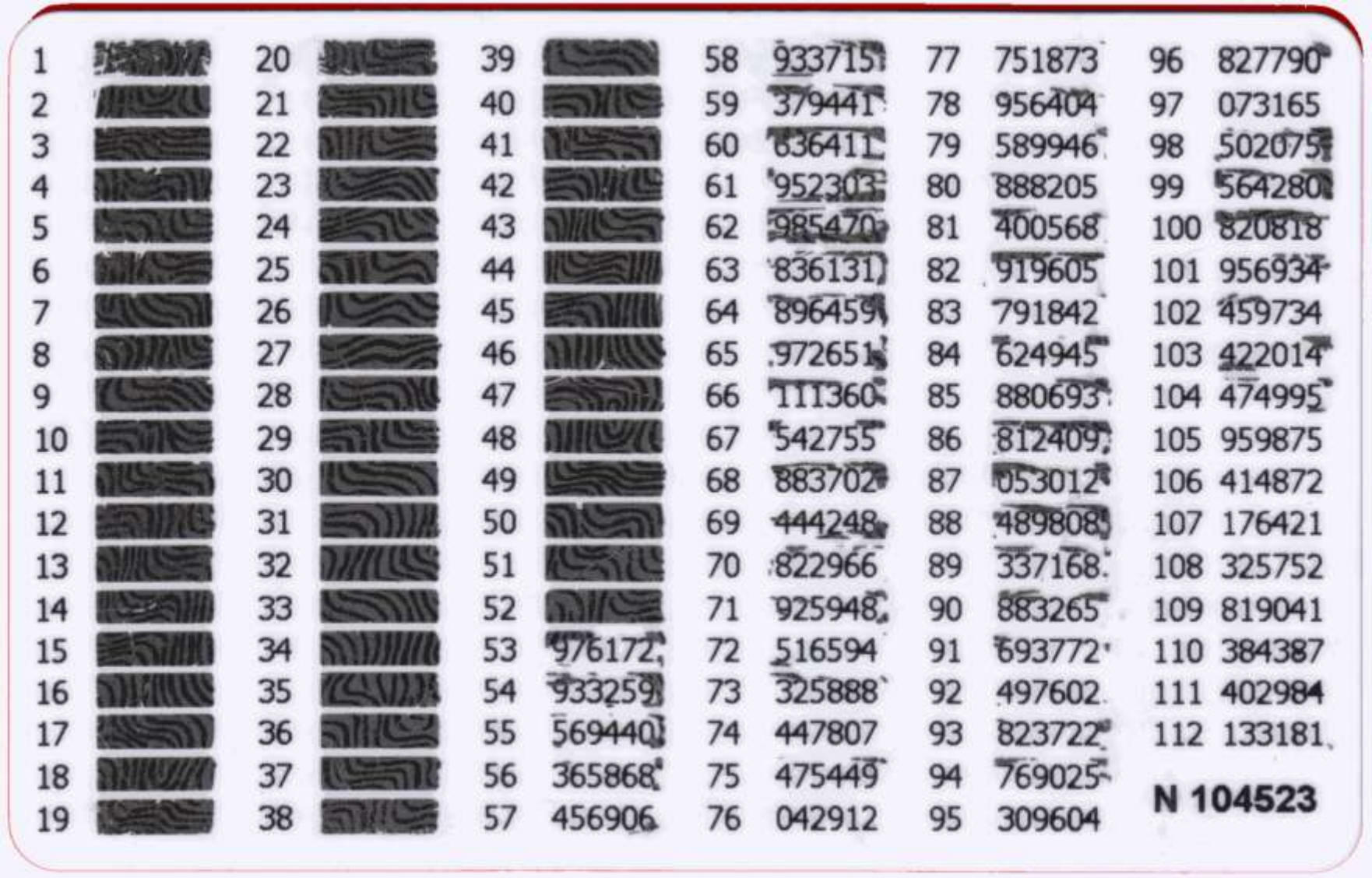


Недостатки “Классических” паролей

- Пользователи используют нестойкие пароли
- Пользователям тяжело запомнить сложные пароли
- Легко передать третьим лицам
- Пользователи используют одинаковые пароли
- Необходимо периодически менять\придумывать\запоминать
- Легко компрометируются техническими средствами
- Могут быть скомпрометированы на аутентифицирующей стороне
- Невозможно установить факт компрометации

One Time Password

История одноразовых паролей



Виды одноразовых паролей

По реализации:

- Программные
- Аппаратные

По технологии:

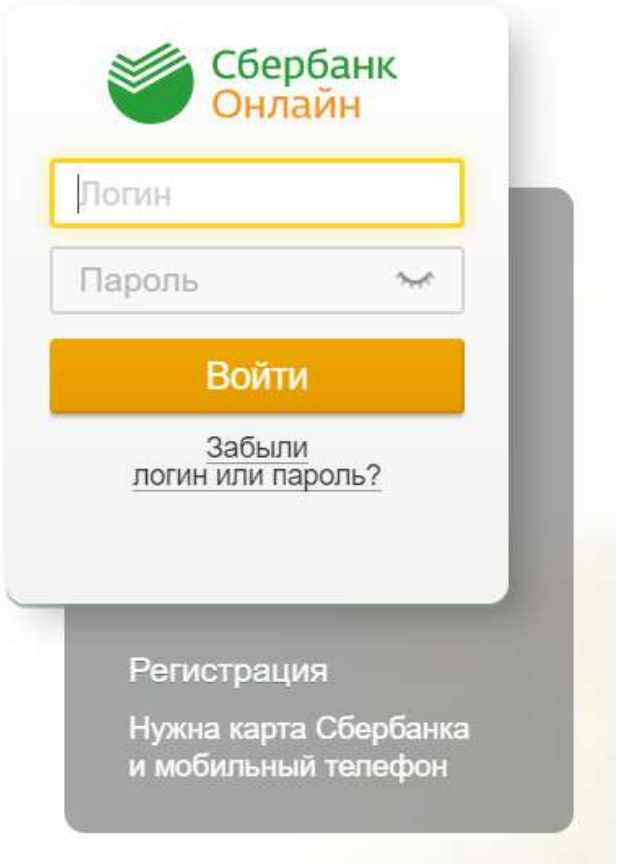
- S/Key
- OTP
- TOTP
- HOTP

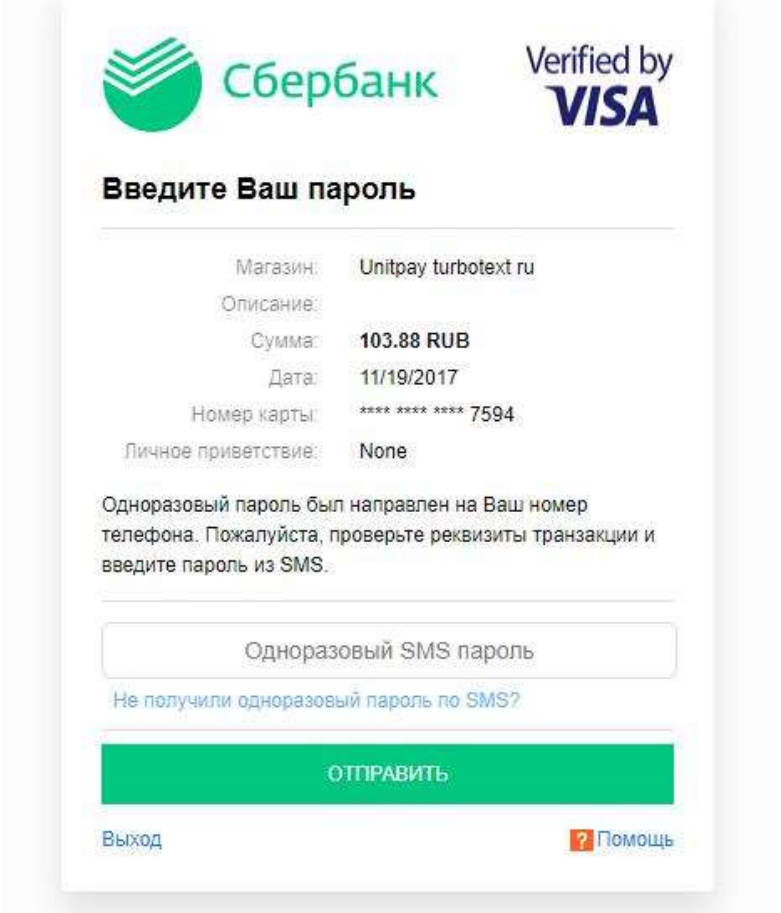
По виду:

- С экраном
- HID-токены

Как это происходит в реальной жизни

В основе лежат 2 фактора, которые проверяются друг за другом





Что происходит внутри HOTP?

1. Симметричный ключ уникальный для пользователя, хранится на сервере и внутри генератора
2. При каждом нажатии увеличивается счетчик внутри генератора
3. Вычисляется хеш-функция от секретного ключа и счетчика
4. Часть полученного результата и есть одноразовый пароль
5. Сервер выполняет те же действия и получает свое значение
6. На сервере происходит сравнение двух значений и принимается решение об аутентификации

Достоинства одноразовых паролей

- Компрометация пароля не компрометирует аккаунт
- Может иметь криптографическую основу
- При необходимости можно предоставить доступ коллеге
- Разные пароли для разных аккаунтов
- Нельзя скомпрометировать программно
- Легко установить факт компрометации
- Развитие стандартов и их поддержка ведущими разработчиками

Недостатки одноразовых паролей

- Необходимо носить с собой средство генерации
- Нужен резервный способ входа при компрометации

Рутокен OTP

Рутокен OTP

- Аппаратный генератор одноразовых паролей
- HID-устройство
- HOTP
- 1299 рублей

Какие площадки поддерживают OTP?

- AeroFS
- Dropbox
- Evernote
- Mega
- OneDrive
- Synology
- Amazon Web Services
- Heroku
- Microsoft Azure
- Discord
- MailChimp
- Salesforce
- Slack
- Bitbucket
- и другие…

Universal 2nd Factor

Universal 2nd Factor

- Открытый, без драйверный протокол для двухфакторной аутентификации
- Разработан компаниями Google, Yubico и NXP Semiconductors
- Стандарт поддерживается и развивается консорциумом FIDO Alliance
- В основе лежит криптография с открытым ключём

Криптографические примитивы:

- Для подписи – ECDSA над кривой P-256
- Для хеширования – SHA-256

Где уже работает?

Поддержка в браузерах “из коробки”:

- Google Chrome с 38 версии
- Opera с 40 версии
- Firefox поддержка добавляется через расширение
- Microsoft Edge после установки October 2018 Windows Update

Что происходит внутри U2F?

Регистрация пользователя

1. Веб-сервис отправляет данные (challenge) для подписи устройством
2. Браузер добавляет URI и ID канала TLS и отправляет их на устройство
3. Пользователь подтверждает свое согласие нажатием на кнопку
4. Устройство генерирует ключевую пару и дескриптор ключа
5. Устройство возвращает открытый ключ, дескриптор ключа
6. Веб-сервис проверят подпись и запоминает открытый ключ и дескриптор ключа для данного пользователя

Что происходит внутри U2F?

Аутентификация

1. Веб-сервис отправляет данные (challenge) и дескриптор ключа
2. Браузер добавляет URI и ID канала TLS и отправляет их на устройство
3. Пользователь подтверждает свое согласие нажатием на кнопку
4. Используя дескриптор ключа, устройство выбирает закрытый ключ
5. Если все прошло успешно, то производится подпись от данных клиента плюс значения счетчика
6. Веб-сервис проверяет подпись и значение счетчика

Рутокен U2F

Какие площадки поддерживают U2F?

- Dropbox
- Google Drive
- Amazon Web Services
- Google Cloud Platform
- Hangouts
- Salesforce
- Bitbucket
- GitHub
- GitLab
- Sentry
- FastMail
- Gmail
- YouTube
- Bitwarden
- Vanguard
- Norton
- Linux PAM
- WordPress
- Mastodon
- Nextcloud

Контактная информация

Электронная почта:

Личная – sv@rutoken.ru

Отдел продаж – sales@rutoken.ru

Тех. поддержка – hotline@rutoken.ru

Facebook:

facebook.com/vladimir.salykin

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90