РУТОКЕН

Вебинар

Технологии аутентификации.
Часть 1

Владимир Салыкин,
Менеджер по продуктам
Компания «Актив»

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

О чём поговорим сегодня:

- Что такое идентификация, аутентификация и авторизация?
  И как в них не путаться?
- Технологии идентификации:
  достоинства, недостатки, перспективы развития
- Факторы аутентификации
- Технологии аутентификации:
  достоинства и недостатки существующих решений

РУТОКЕН

Компания «Актив»

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

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

Идентификация
Аутентификация
Авторизация

Идентификация

Определение

- Формально. Идентификация — действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов [Р 50.1.053 – 2005]
- Не формально. Предъявление некоторого идентификатора, который позволит отделить один субъект\объект от другого.

РУТОКЕН

Примеры идентификации

Goc

Вх

Используйте а

Телефон или адрес эл. почты

IvanIvanov

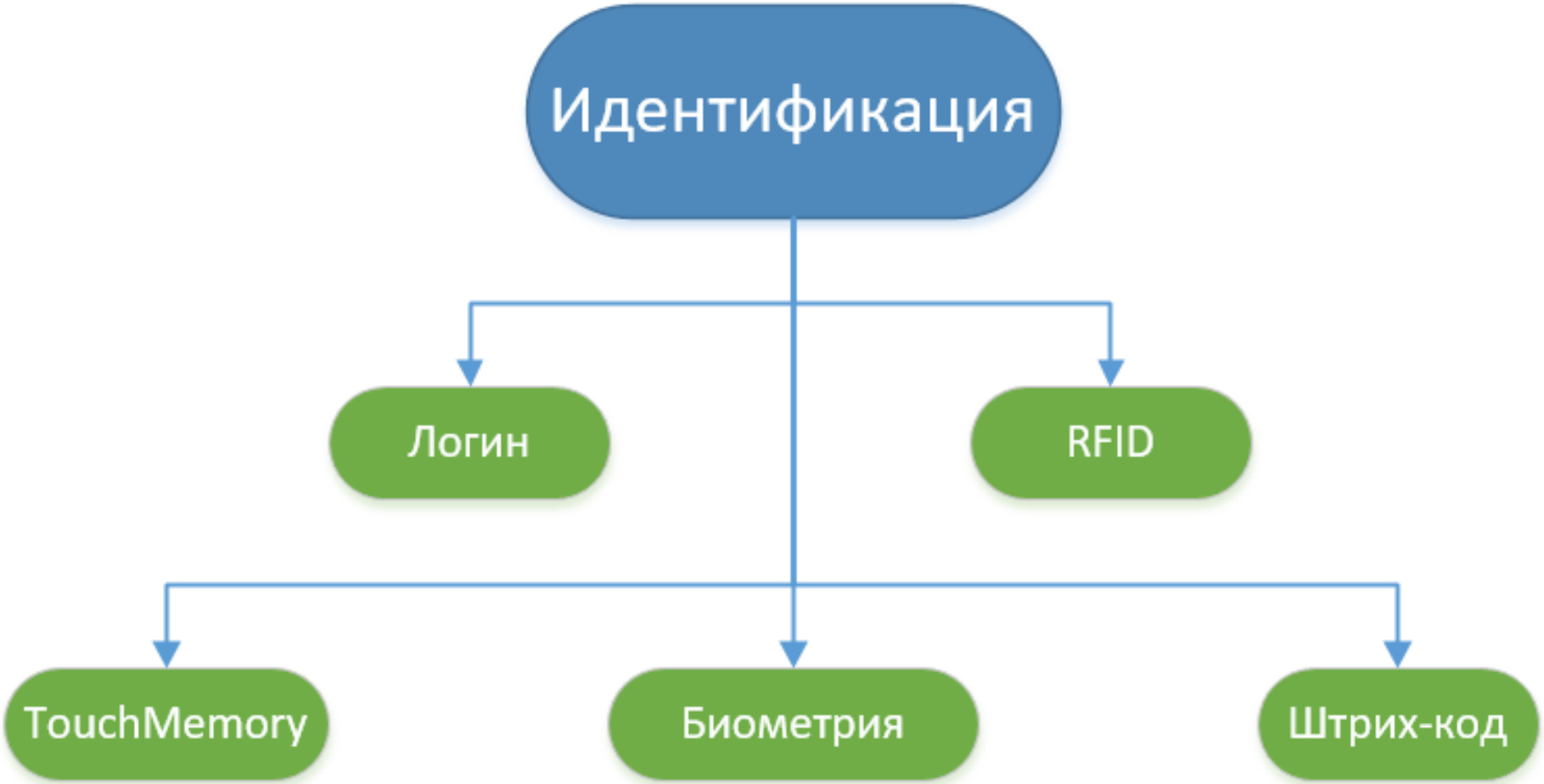
Забыли адрес эл. почты?

Работаете на чужом компьк
инкогнито. Подробнее...

Создать аккаунт

Далее

Технологии идентификации



Основная проблема

Знание или наличие идентификатора
не гарантирует верную связь с субъектом
или объектом

Решение? **Аутентификация!**

Аутентификация

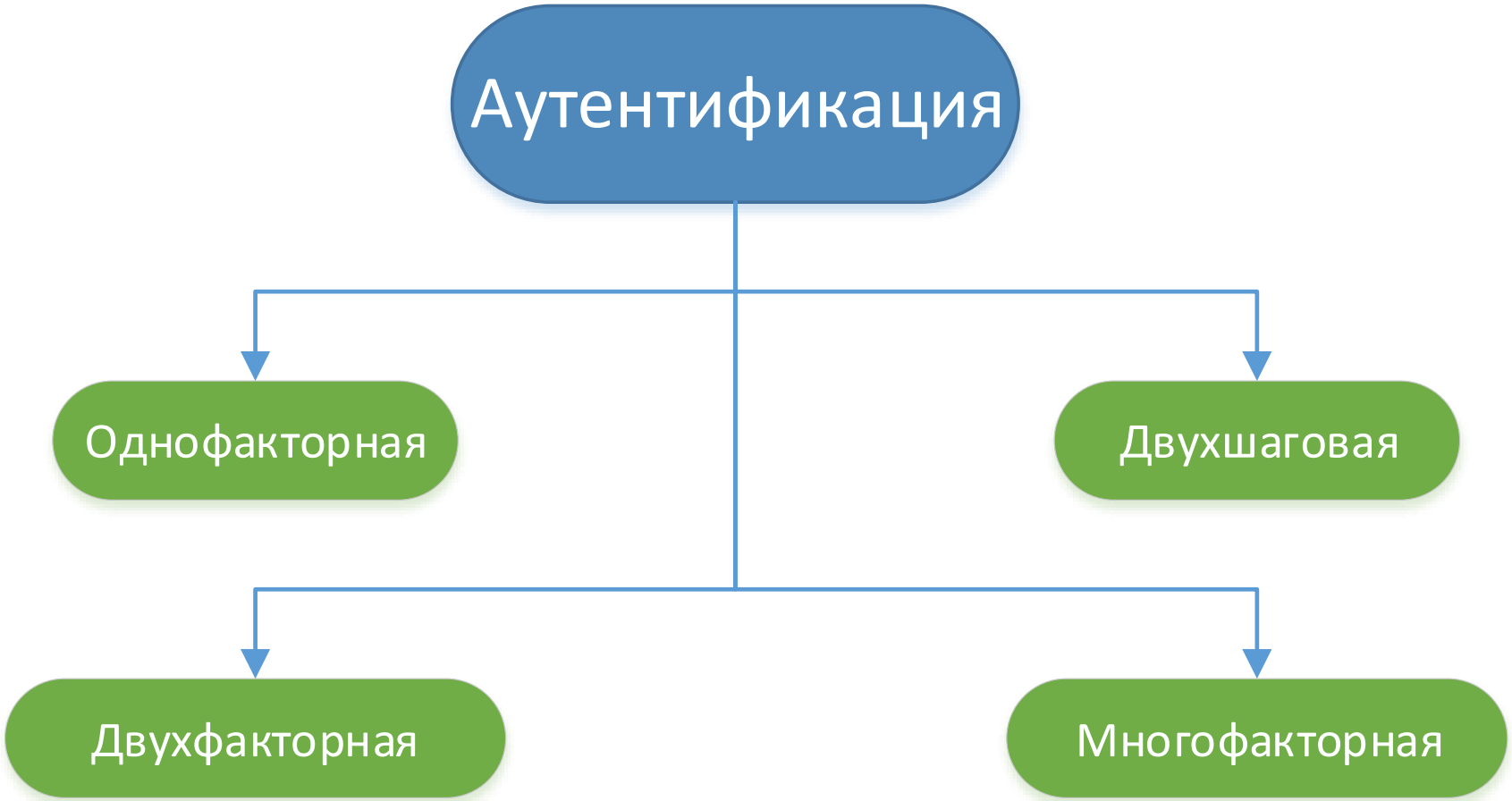
Определение

- 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

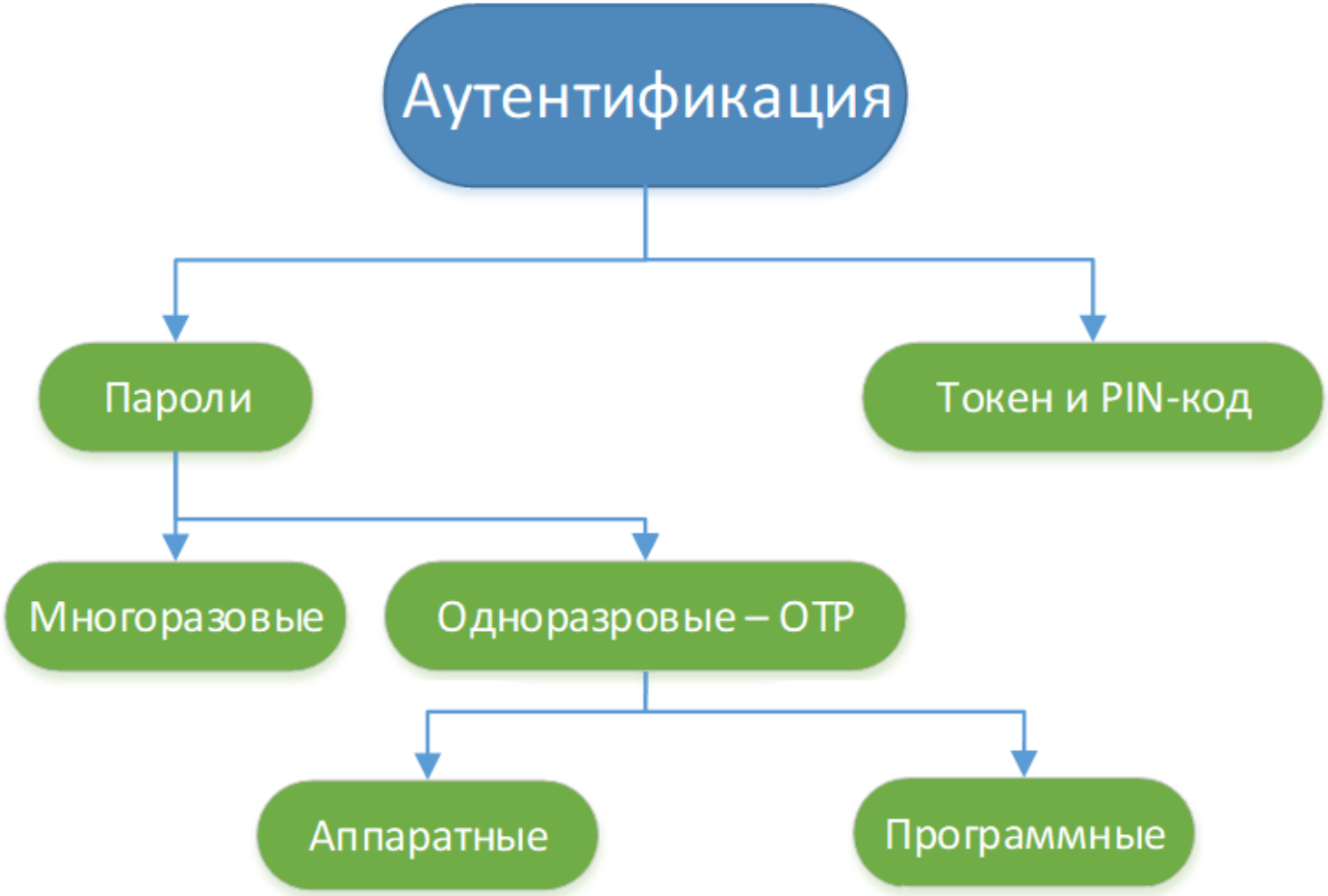
Аутентификация и факторы



Факторы аутентификации

- Однофакторная — один фактор
  Классические пароли, OTP
- Двухшаговая — первый фактор + ещё один зависимый
  Классический пароль + OTP
- Двухфакторная — два независимых фактора
  Токен\смарт-карта + PIN-код
- Многофакторная — более двух независимых факторов

Технологии аутентификации



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

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

Достоинства программных OTP

- Компрометация пароля не компрометирует аккаунт
- Не требует создания\запоминания\смены\политик ИБ
- Может иметь криптографическую основу
- Нельзя просто передать третьим лицам
- Разные пароли для разных аккаунтов
- Не могут быть скомпрометированы на аутентифицирующей стороне

Недостатки программных OTP

- Необходимо носить с собой средство генерации
- При утере средства генерации аккаунт компрометируется
- Сложно восстанавливается при компрометации
- Легко компрометируется программно
- Невозможно установить факт компрометации
- Необходима поддержка от разработчиков

Аппаратные одноразовые пароли

Основные отличия от программных OTP

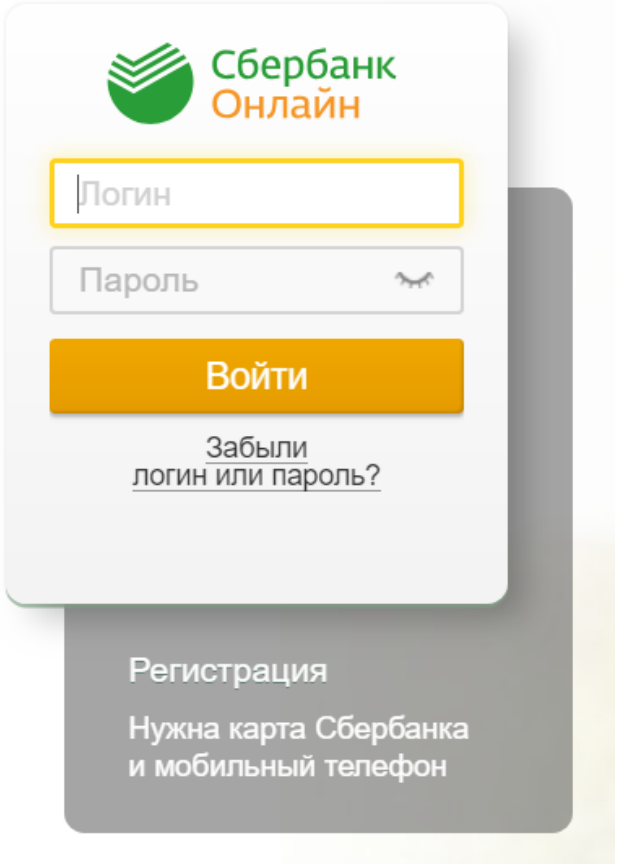
Достоинства:

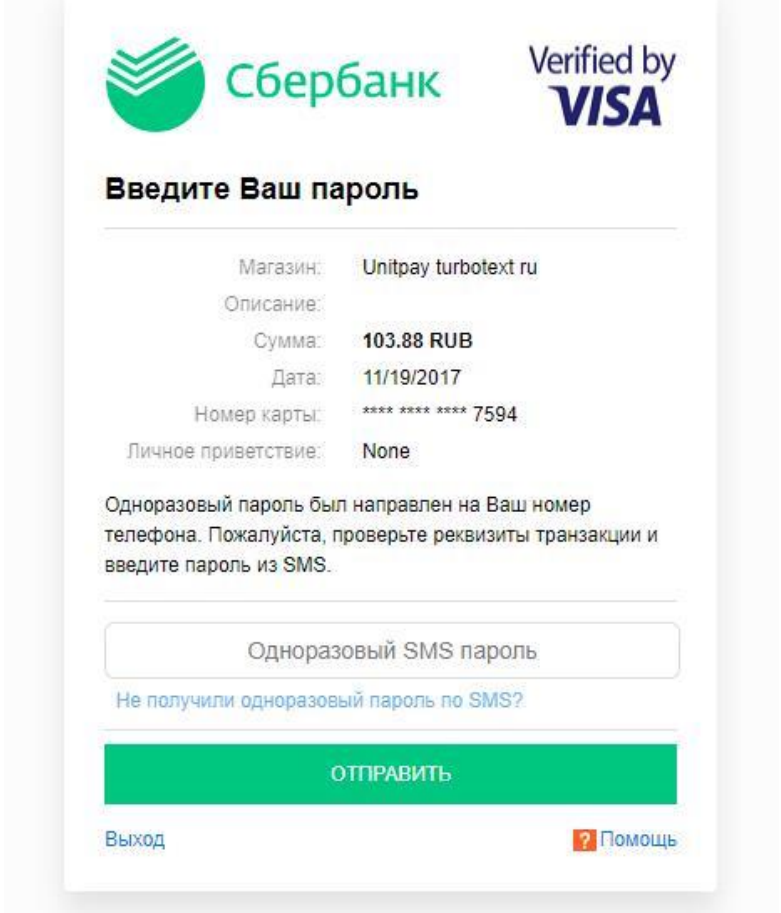
- Нельзя скомпрометировать программно
- Легко установить факт компрометации
- Развитие стандартов и их поддержка ведущими разработчиками (FIDO U2F)

РУТОКЕН

Двухшаговая аутентификация

В основе лежат 2 фактора, которые проверяются друг за другом





Двухшаговая аутентификация

Достоинства:

- Более безопасна, чем аутентификация по паролям или программные OTP по отдельности

Недостатки:

- Факторы могут быть скомпрометированы независимо друг от друга

РУТОКЕН

Криптографическая аутентификация на токенах

РУТОКЕН

Криптографическая аутентификация на токенах

Достоинства. Часть 1

- Сложно передать третьим лицам
- В основе лежит стойкая криптография
- Легко восстанавливается при компрометации
- Можно использовать разные секреты для работы с разными сервисами
- Нельзя скомпрометировать на аутентифицирующей стороне
- Не требует создания\запоминания\смены\политик ИБ
- Легко установить факт компрометации

РУТОКЕН

Криптографическая аутентификация на токенах

Достоинства. Часть 2

- Нельзя скомпрометировать программно
- Давно стандартизирована и поддерживается ведущими разработчиками

Криптографическая аутентификация на токенах

Недостатки:

- Требует наличия устройства
- Может потребовать встраивание в конкретную систему

РУТОКЕН

О чём поговорим в следующий раз:

Часть 2

- Биометрия. Идентификация и аутентификация. Проблемы и возможные решения.

Часть 3

- Системы идентификации и аутентификации
- Менеджеры паролей
- SSO системы
- IDM системы
- PKI

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

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