Сервер аутентификации Kerberos

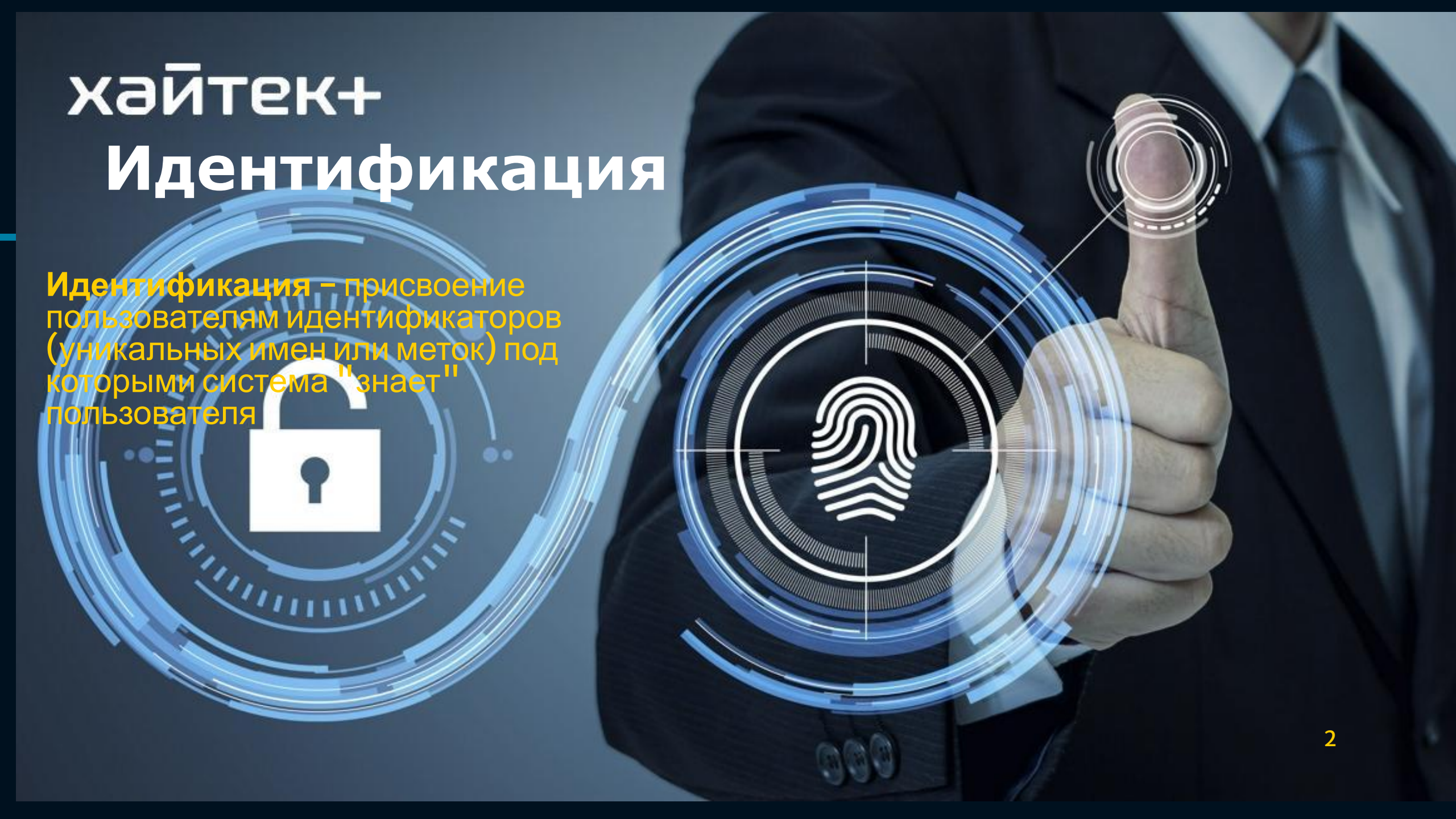
Выполнила:
Студент 402 группы
Колушова Диана

март
2020

хайтек+

Идентификация

Идентификация – присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система "знает" пользователя

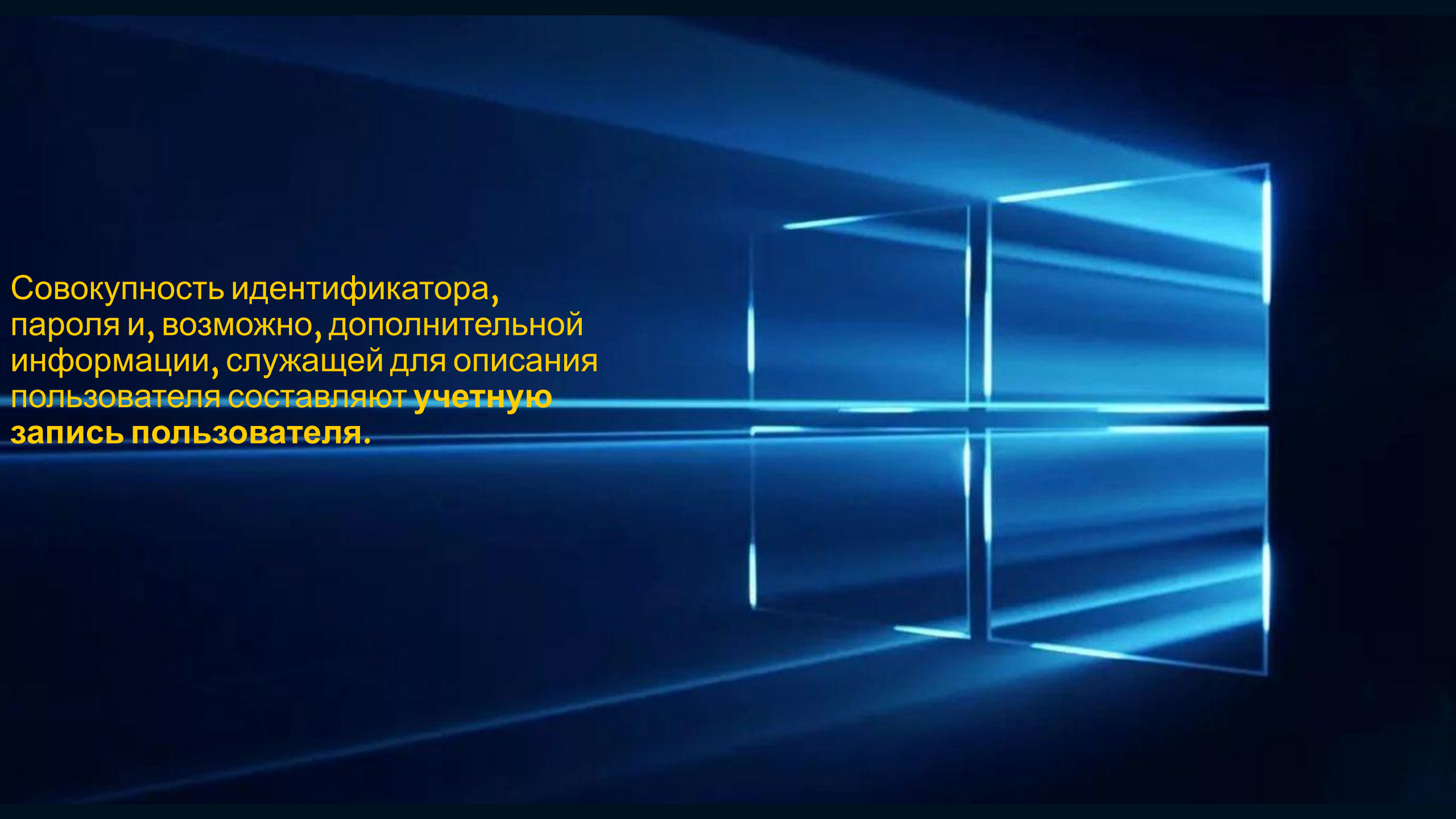


Аутентификация

Аутентификация – установление подлинности – проверка принадлежности пользователю предъявленного им идентификатора.

Методы аутентификации

- Аутентификация по наличию у пользователя уникального объекта заданного типа.
- Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация
- Аутентификация пользователя по его собственным уникальным характеристикам


Совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя составляют **учетную запись пользователя.**

Рекомендации *по* администрированию парольной системы

- Задание минимальной длины используемых в системе паролей;
- Установка требования использовать в пароле разные группы символов – большие и маленькие буквы, цифры, специальные символы;
- Периодическая проверка *администраторами безопасности* качества используемых паролей путем *имитации атак*;
- Установка максимального и минимального сроков жизни пароля, использование механизма принудительной смены старых паролей;
- Ограничение числа неудачных попыток ввода пароля;
- Ведение журнала истории паролей, чтобы пользователи, после принудительной смены пароля, не могли вновь выбрать себе старый, возможно скомпрометированный пароль.

Протокол Kerberos

Стандартом системы централизованной аутентификации и *распределения ключей* симметричного шифрования.

Протокол Kerberos

В сетях *Windows* (начиная с *Windows*'2000 Serv.) *аутентификация по* протоколу Kerberos v.5 (*RFC* 1510) реализована на уровне доменов. Kerberos является основным протоколом аутентификации в домене, но в целях обеспечения совместимости с с предыдущими версиями, также поддерживается протокол *NTLM*.

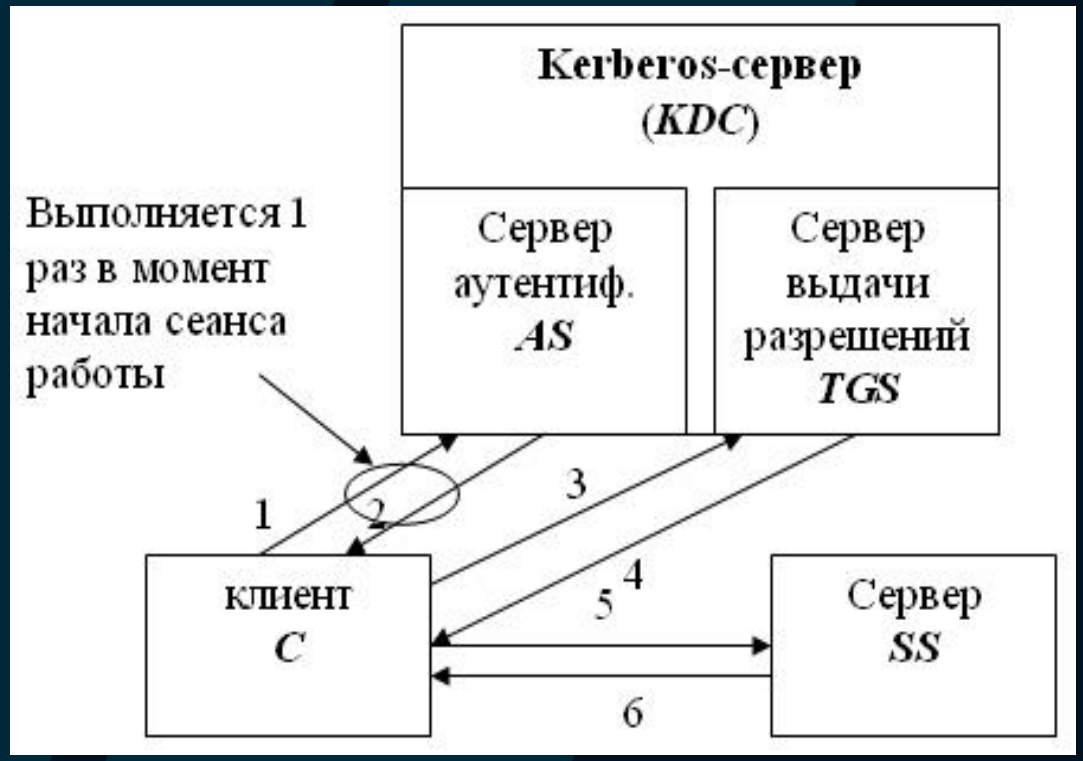
Протокол Kerberos

Серверная часть Kerberos называется *центром распределения ключей* (англ. Key *Distribution Center*, сокр. *KDC*) и состоит из двух *компонент*:

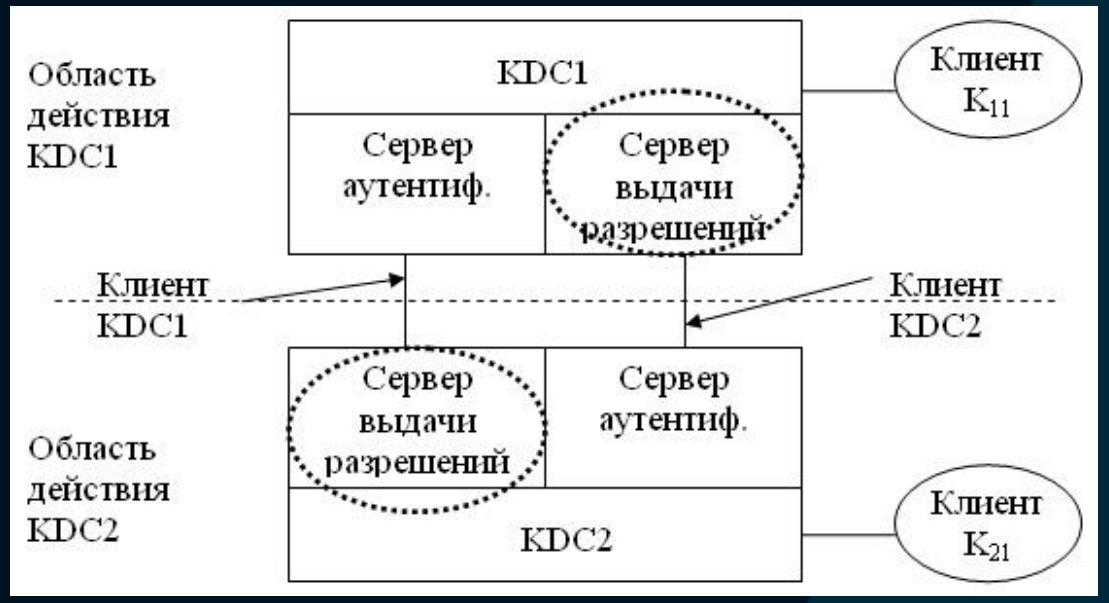
- сервер аутентификации (англ. *Authentication Server*, сокр. AS);
- сервер выдачи разрешений (англ. *Ticket* Granting Server, сокр. *TGS*)

Протокол Kerberos

1. C->AS: {c}.
2. AS->C: $\{\{TGT\}K_{AS\_TGS}, K_{C\_TGS}\}K_C$,
3. $\{TGT\}=\{c,tgs,t_1,p_1, K_{C\_TGS}\}$
4. C->*TGS*: $\{TGT\}K_{AS\_TGS}, \{Aut_1\}K_{C\_TGS}$, {ID}
5. *TGS*->C: $\{\{TGS\}K_{TGS\_SS},K_{C\_SS}\}K_{C\_TGS}$
6. C->SS: $\{TGS\}K_{TGS\_SS}, \{Aut_2\}K_{C\_SS}$
7. SS->C: $\{t_4+1\}K_{C\_SS}$



Взаимодействие между Kerberos-областями



При использовании протокола Kerberos компьютерная *сеть* логически делится на области действия серверов Kerberos. Kerberos-область – это участок сети, пользователи и серверы которого зарегистрированы в базе данных одного сервера Kerberos (или в одной базе, разделяемой несколькими серверами). Одна область может охватывать сегмент локальной сети, всю локальную *сеть* или объединять несколько связанных локальных сетей.

Протокол Kerberos

Для взаимодействия между областями, должна быть осуществлена взаимная *регистрация* серверов Kerberos, в процессе которой *сервер* выдачи разрешений одной области регистрируется в качестве клиента в другой области (т.е. заносится в базу сервера аутентификации и разделяет с ним *ключ*).

Реализация протокола Kerberos в *Windows*

1. Ключ пользователя генерируется на базе его пароля.
2. В роли **Kerberos**-серверов выступают контроллеры домена, на каждом из которых должна работать служба **Kerberos Key Distribution Center** (*KDC*);
3. **Microsoft** в своих ОС использует расширение **Kerberos** для применения криптографии с открытым ключом;
4. Использование **Kerberos** требует синхронизации внутренних часов компьютеров, входящих в домен **Windows**.

Спасибо за внимание!

Колушова Диана