



ПОЛИТЕХ

Санкт-Петербургский политехнический университет Петра Великого

Тема:

Идентификация, аутентификация,
авторизация

Выполнили: Гончарова Т.И., 4731204/50003
Козлов В.А., 4731204/50003

Цель и задачи

Цель: Изучить теоретические основы и практические аспекты процессов идентификации, аутентификации и авторизации как ключевых механизмов обеспечения информационной безопасности

Задачи:

- 1)Объяснить разницу между идентификацией, аутентификацией и авторизацией
- 2)Проанализировать плюсы и минусы современных способов идентификации
- 3)Раскрыть многофакторную аутентификацию как стандарт безопасности
- 4)Продемонстрировать модели авторизации на практических примерах

Идентификация

Определение

Это процесс, когда пользователь сообщает системе, кто он, используя уникальный идентификатор

Это может быть:

Логин;

Номер телефона;

Биометрия;

Номер карты/пропуска;

Имя устройства в сети.



Принцип работы любой системы идентификации: два одинаковых идентификатора не могут существовать одновременно.

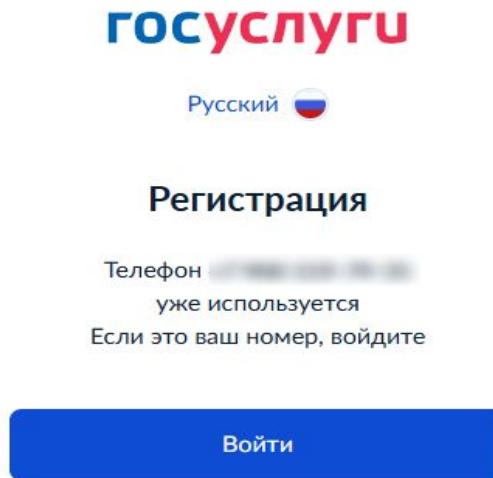


Рис. 1. Ошибка идентификации
(телефон уже используется)

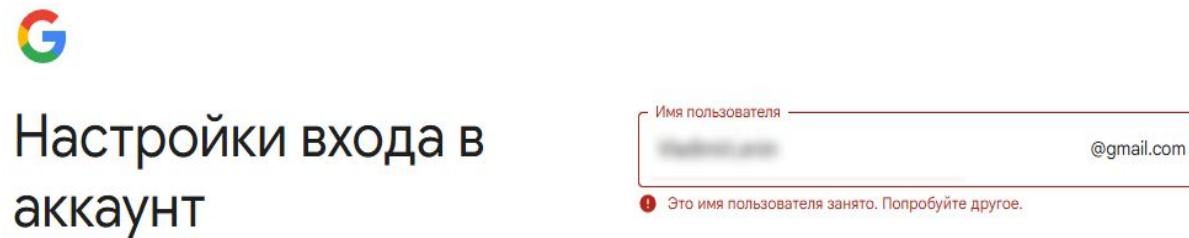


Рис. 2. Ошибка идентификации (имя пользователя занято)

Таблица 1. Плюсы и минусы идентификации

Плюсы идентификации	Минусы идентификации
Упрощение взаимодействия: Пользователю не нужно запоминать сложные комбинации для входа в разные сервисы.	Проблемы с конфиденциальностью: Email и телефон — это персональные данные . Их утечка из базы данных сервиса может привести к спаму, фишинговым атакам и даже взлому других аккаунтов пользователя.
Уникальность: Логин, email и номер телефона гарантированно уникальны для каждого пользователя в рамках одной системы.	Уязвимости для атак: Сканирование и подбор (Enumeration Attack): Злоумышленник может автоматически проверять, зарегистрирован ли в системе тот или иной email/логин.
Гибкость для пользователя: Предоставление выбора (войти по логину, email или телефону) повышает удобство.	Социальная инженерия: Знание идентификатора (например, email) — это первый шаг для целевой фишинговой атаки.
Интеграция и персонализация: Использование email позволяет сервису связывать данные пользователя (например, автоматически подставлять имя из почты), а телефон — для интеграции с мессенджерами или звонками.	Потеря доступа к идентификатору: Если пользователь потерял доступ к email или SIM карте, процесс восстановления доступа к аккаунту становится крайне сложным, а иногда и невозможным.
	Устаревание данных: Люди меняют email-адреса и номера телефонов. Если не обновить их в сервисе, аккаунт может быть навсегда утерян.

Аутентификация

Определение

Это процесс проверки подлинности субъекта, который перед этим прошёл идентификацию.

Аутентификация может быть:

- Односторонней — личность подтверждает только пользователь, пытающийся получить доступ к системе.
- Взаимной — подлинность доказывают и пользователь, и сервер. Такой тип проверки используется при доступе к засекреченным данным.

Также аутентификация может быть:

Однофакторной — использование одного элемента проверки, чаще всего пароля.

Многофакторной — для доступа требуется подтвердить личность несколькими способами (например, пароль и одноразовый код)



Рис. 3. Основные элементы многофакторной аутентификации

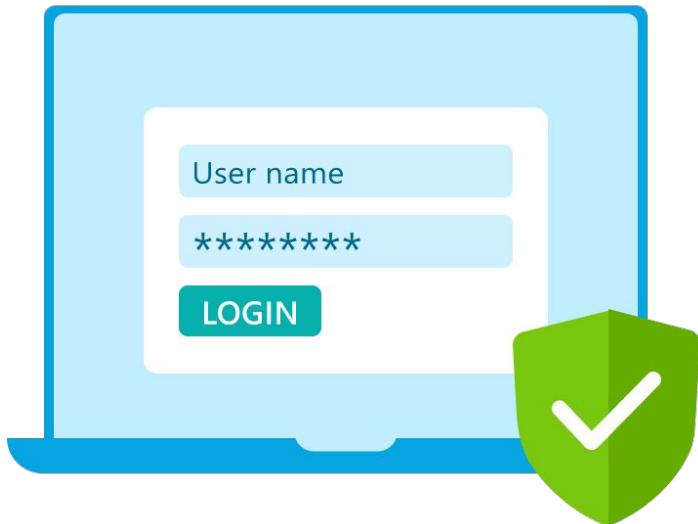
Многофакторная аутентификация удобна, потому что:

- если злоумышленник узнал пароль, без второго фактора он не сможет войти;
- современные способы — пуш-уведомление или код в приложении — занимают несколько секунд;
- можно выбрать удобный для себя способ, например звонок или код из приложения

Авторизация

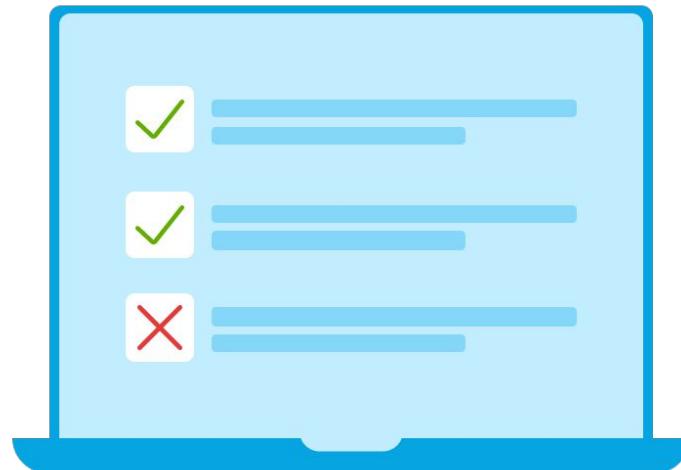
Определение: это процесс, который предоставляет пользователю права на выполнение определённых действий, а также проверяет эти права при попытке получить доступ к ресурсам или выполнить действие

Аутентификация



Является ли пользователь тем,
за кого себя выдаёт?

Авторизация



Есть ли у пользователя разрешение
на доступ к данным?

Рис. 4. Аутентификация и Авторизация

Примеры авторизации:

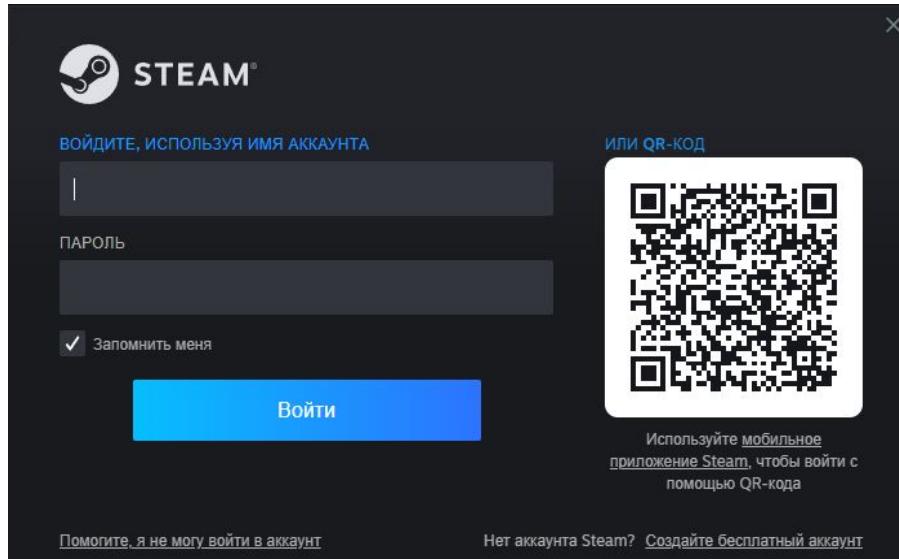


Рис. 5. Вход в аккаунт

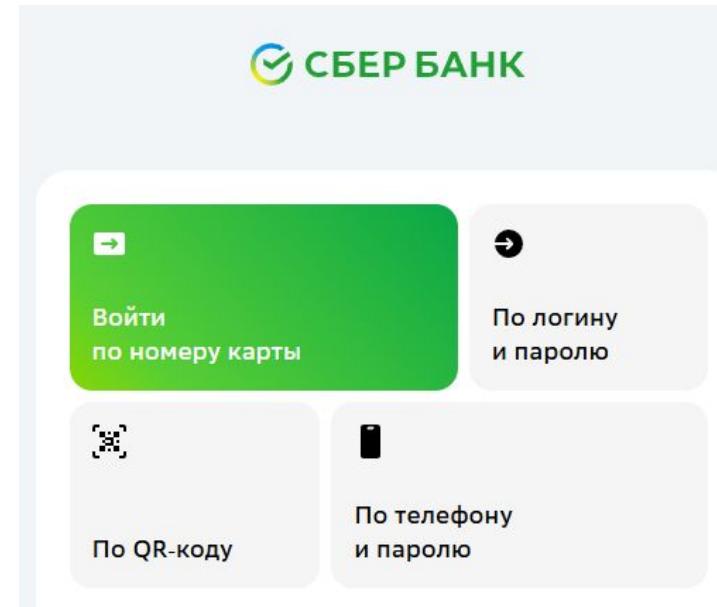


Рис. 6. Авторизация банковской карты

Как работает авторизация технически?

Когда пользователь пытается выполнить какое-либо действие, система:

- 1) Перехватывает запрос (например, "удалить файл")
- 2) Проверяет контекст:

Кто пользователь (его ID, роли, атрибуты)

Что он пытается сделать (действие)

С каким ресурсом работает

- 3) Сверяется с правилами доступа
- 4) Выдает/не выдает токен/права доступа

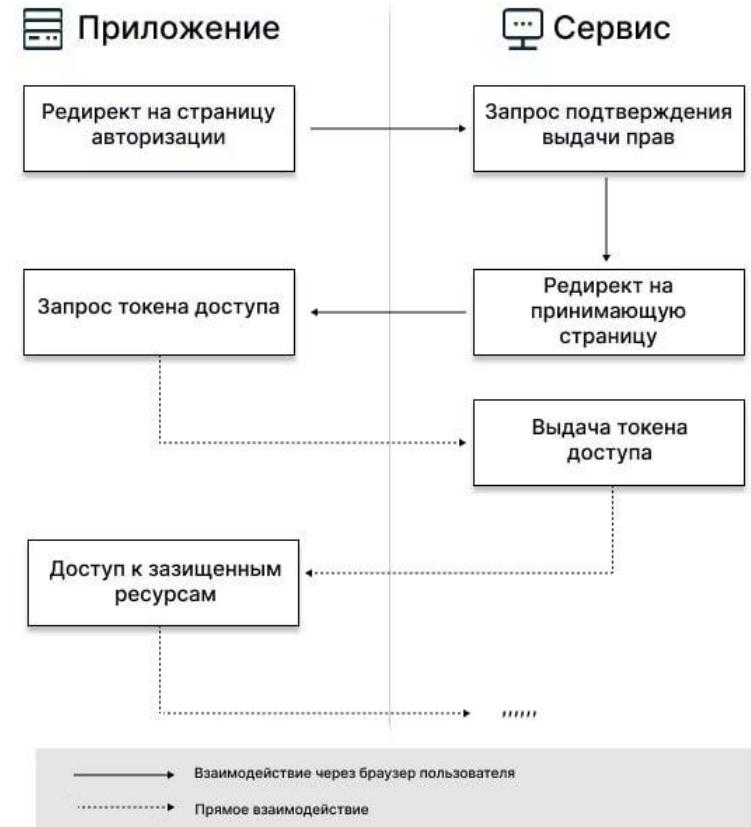


Схема 1. Принцип работы авторизации

Основные модели авторизации:

1. RBAC (Role-Based Access Control) : Права

выдаются на основе ролей . Пример: Роль “Менеджер” : просмотр отчетов, редактирование заказов; Роль “гость” : только просмотр каталога.

2. ABAC (Attribute-Based Access Control) : доступ

определяется атрибутами и политиками. Пример : “Сотрудник отдела финансов может получить доступ к бюджет только с рабочего компьютера в рабочее время”.

3. DAC (Discretionary Access Control) :

владелец ресурса сам решает, кому дать доступ. Пример: Вы создали файл в Google Docs и сами выбираете ,кому дать права доступа на редактирование.

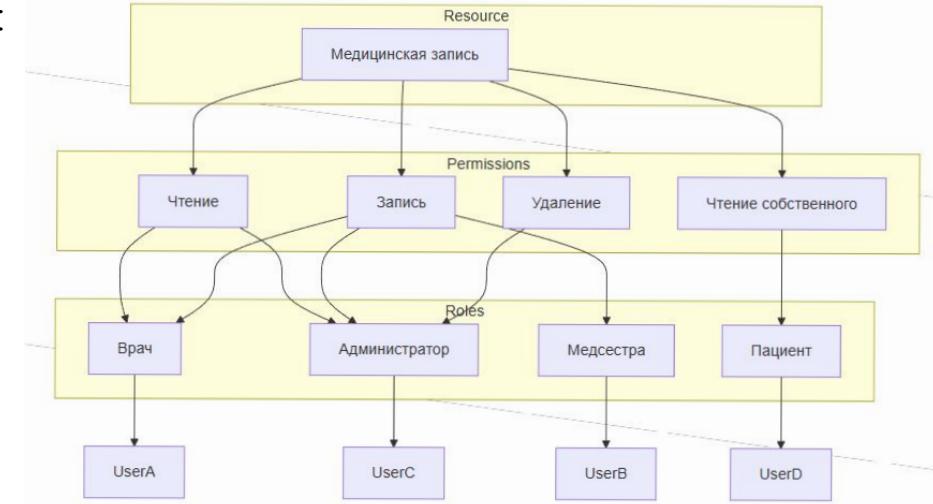


Рис.7. Модель RBAC

Выводы:

- 1) Объяснили разницу между идентификацией, аутентификацией и авторизацией
- 2) Проанализировали плюсы и минусы современных способов идентификации
- 3) Раскрыли многофакторную аутентификацию как стандарт безопасности
- 4) Продемонстрировали модели авторизации на практических примерах

Таким образом, цель изучения теоретических основ и практических аспектов процессов идентификации, аутентификации и авторизации достигнута. В результате проведенного анализа сформирована комплексная картина функционирования ключевых механизмов обеспечения информационной безопасности