

Григорьев Александр Сергеевич

[t.me/iu7zi2022](https://t.me/iu7zi2022)

Зачет (допуск - все лабы (х6))

Два вопроса:

- 1) Можно снять (если отвечать на лекции)
- 2) Можно снять (сдать все лабы до начала зачетной недели)

# Введение

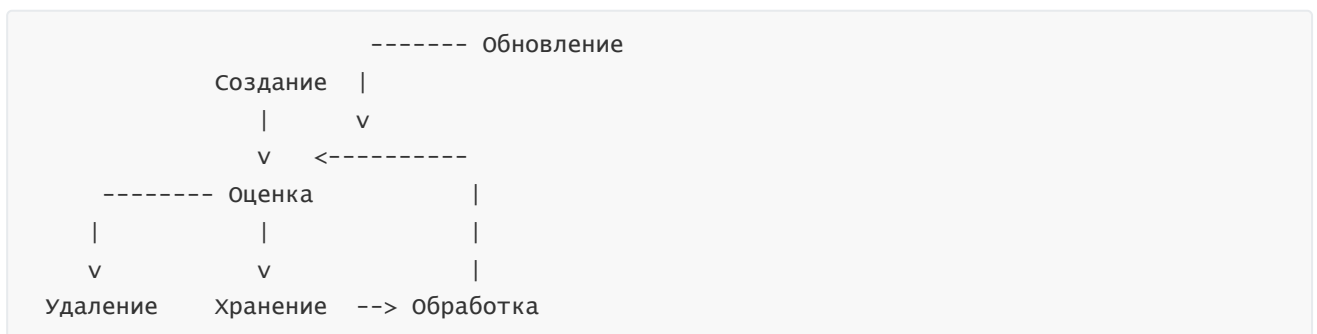
## Периоды

- древние времена (сдвиги, замены);
- средние века (многоалфавитность, криптоанализ);
- математическая криптография (открытость);
- стандартизация и государственное регулирование;
- децентрализация (блокчейны).

**Информация** - сведения, сообщения, данные независимо от формы их представления.

149-ФЗ

## Жизненный цикл информации



**Документ** - информация, зафиксированная на материальном носителе (+ реквизиты).

**Электронный документ** - документированная информация, представленная в электронной форме.

**Защита информации** - включает в себе три группы мер:

- нормативные меры (законы),
  - организационные меры (организации),
  - технические меры (программно-аппаратные),
- направленные на:

1. предотвращение неправомерных действий в отношении информации:

- передача,

- распространение,
- доступ (кража),
- уничтожение,
- искажение,
- копирование,
- блокирование,

2. соблюдение конфиденциальности информации ограниченного доступа,

3. реализация права на доступ к информации.

Одна из самых развитых сфер в защите информации - *банковская*.

Стандарт банка России информационной безопасности банковской системы Российской Федерации.

СТО БР ИББС РФ 1.0 - 2014

Актив - все, что имеет ценность для субъекта и находится в его распоряжении.

## Информационная сфера

- информация (что?),	---	
- информационная инфраструктура (где?),		
- субъекты (кто?),		Система регулирования
- процедуры (как?)	---	

**Угроза** - опасность, предполагающая возможность потери, ущерба.

**Безопасность** - состояние защищенности в условиях угроз.

**Информационная безопасность** - состояние безопасности в информационной сфере.

## Задачи

(обязательные)

- доступность (availability),
- целостность (integrity),
- конфиденциальность (confidentiality)

(вспомогательные)

- авторство,
- подотчетность,
- аутентичность (подлинность),
- достоверность.

## **Стадии работы пользователя в системе**

1. Идентификация - присвоение и последующая проверка уникального имени субъекта (логин);
2. Аутентификация - проверка подлинности идентификатора, предоставленного субъектом (пароль и тд);
3. Авторизация - предоставление прав доступа.

## **Информация по уровню ценности**

- жизненно-важная,
- важная,
- служебная,
- незначительная.

Обоснованность доступа - доступ должен быть достаточным для выполнения обязанностей.

Глубина контроля доступа - разграничение потоков информации.

Чистота повторного использования ресурсов (на всех стадиях).

Персональная ответственность - каждый пользователь должен проходить все стадии.