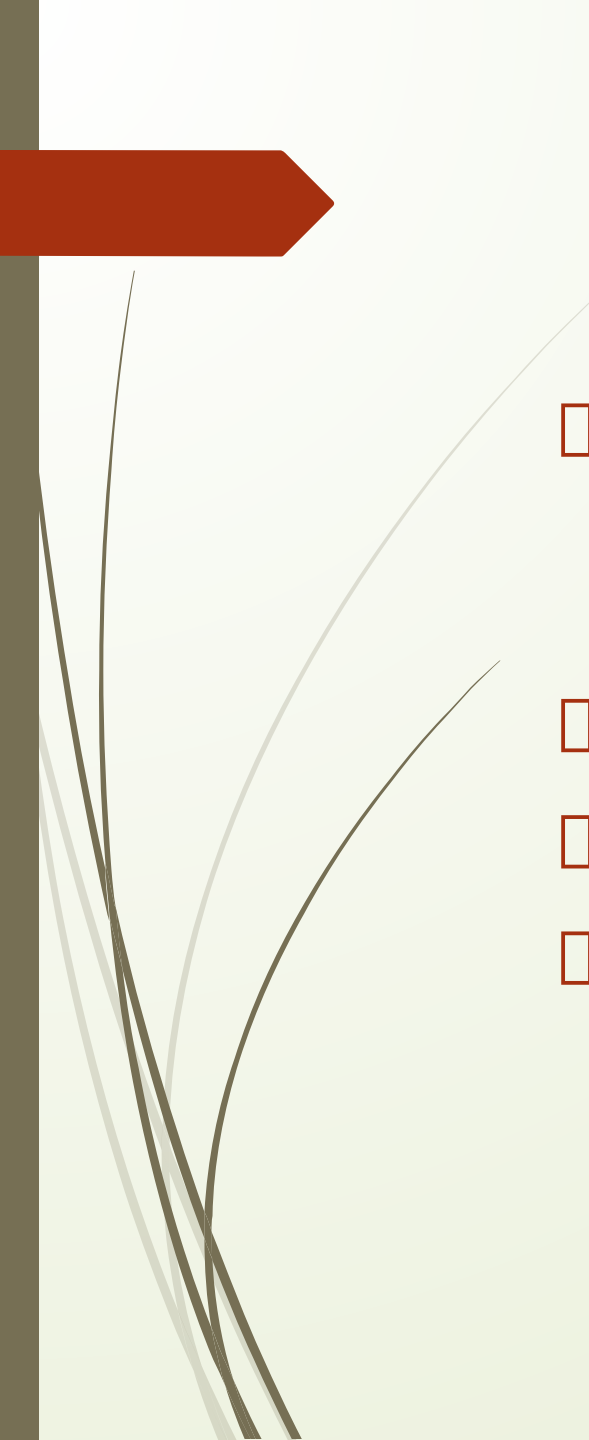
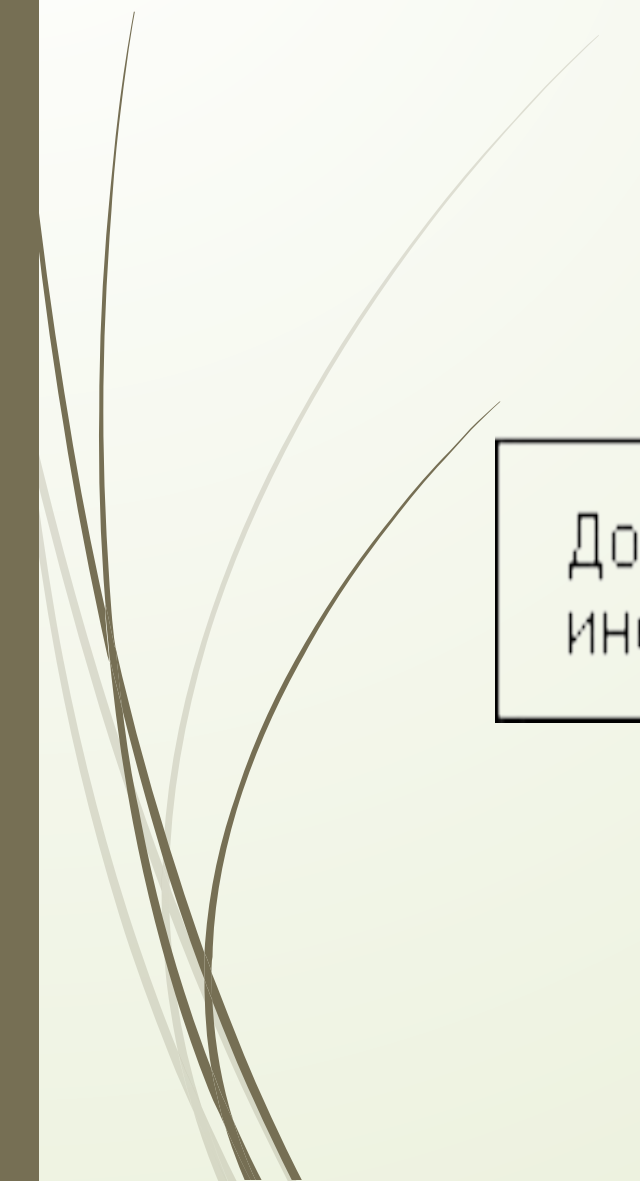




Тема 2: Составляющие информационной безопасности

- 
- Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:
 - Обеспечением доступности информации.
 - Обеспечением целостности информации.
 - Обеспечением конфиденциальности информации.



```
graph TD; A[Содержание информационной безопасности] --> B[Доступность информации]; A --> C[Конфиденциальность информации]; A --> D[Целостность информации];
```

Содержание
информационной безопасности

Доступность
информации

Конфиденциальность
информации

Целостность
информации

- 
- 
- **Доступность** – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.
 - Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени.

- 
- **Целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.
 - Целостность информации условно подразделяется на статическую и динамическую. **Статическая** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. **Динамическая** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.
 - Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами

- 
- 
- **Конфиденциальность** – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.
 - Практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.



Домашнее задание

