

**Защита информации
10 класс
(базовый уровень)**

© Тихова Л.В.,
МБОУ «Большехаланская СОШ», 2012

Цифровая информация –

информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

Кража, утечка
прослушивание
информации

ВИДЫ
УГРОЗ

Разрушение,
уничтожение
информации

Физическая защита
каналов,
криптографические
шифры,
цифровая подпись
и сертификаты

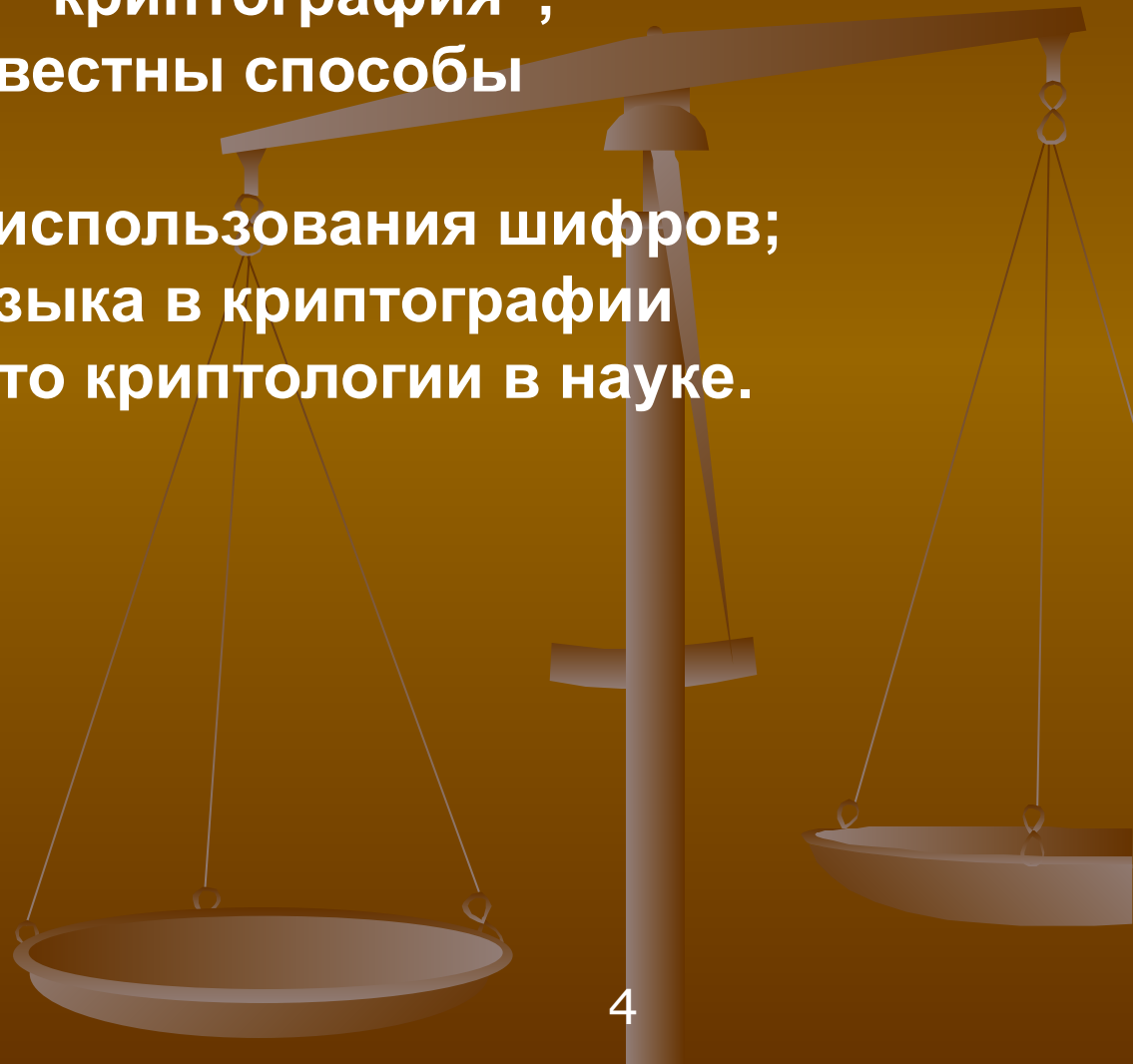
Антивирусные программы,
брандмауэры, межсетевые
экраны, резервное
копирование,
контроль оборудования

Цель урока:

- **Обучающая** – сформировать у учащихся понятия цифровой и защищаемой информации, виды угроз для информации и методы ее защиты, криптографии;
- **Развивающая** – способствовать развитию познавательной деятельности учащихся, умению анализировать полученную информацию;
- **Воспитывающая** – способствовать формированию недопустимости действий, нарушающих правовые и этические нормы работы с информацией.

Задачи урока

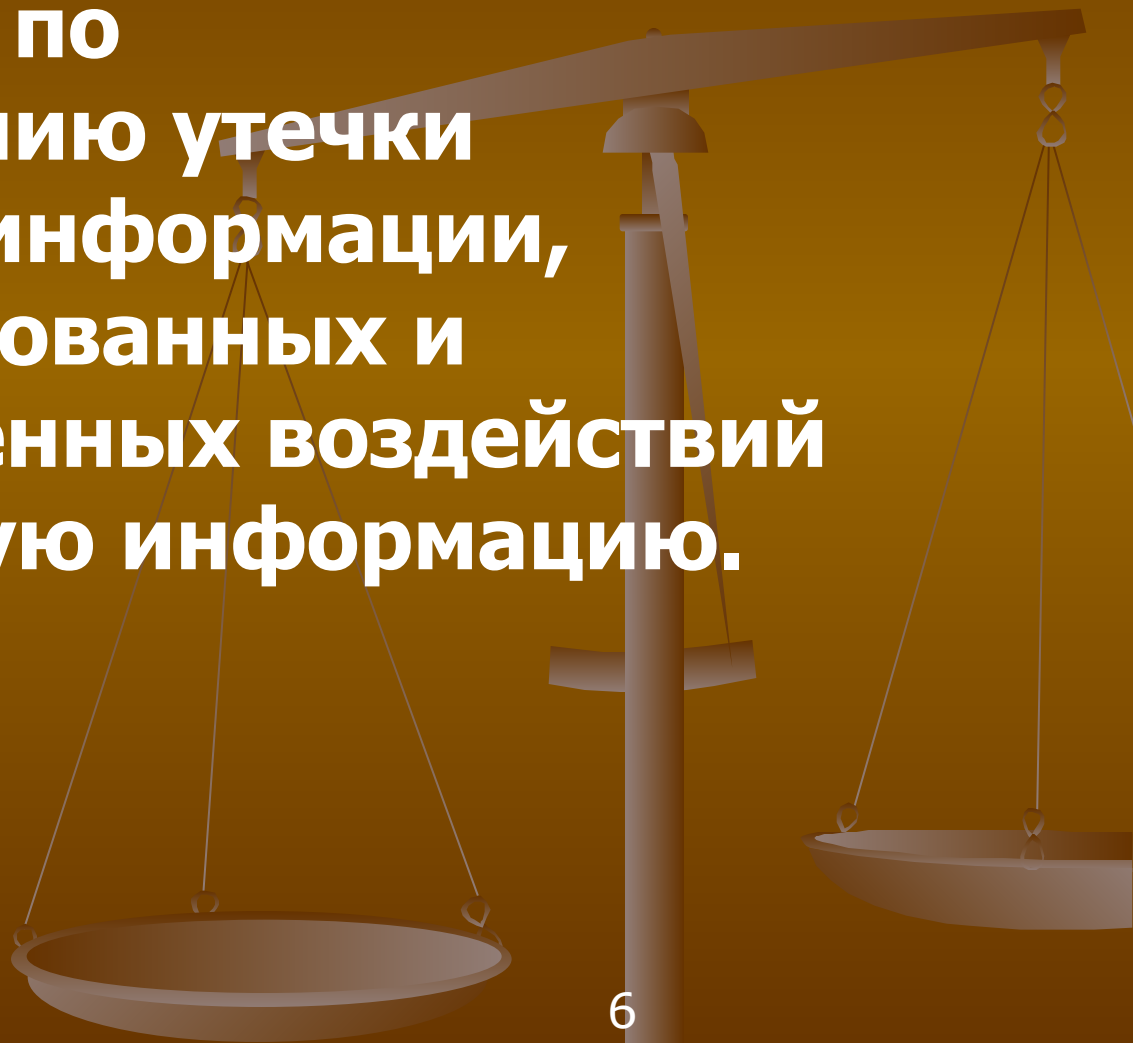
выяснить, что включают в себя понятия “криптология” и “криптография”;
узнать, какие известны способы шифрования;
изучить сферы использования шифров;
выявить роль языка в криптографии
определить место криптологии в науке.



Защищаемая информация –

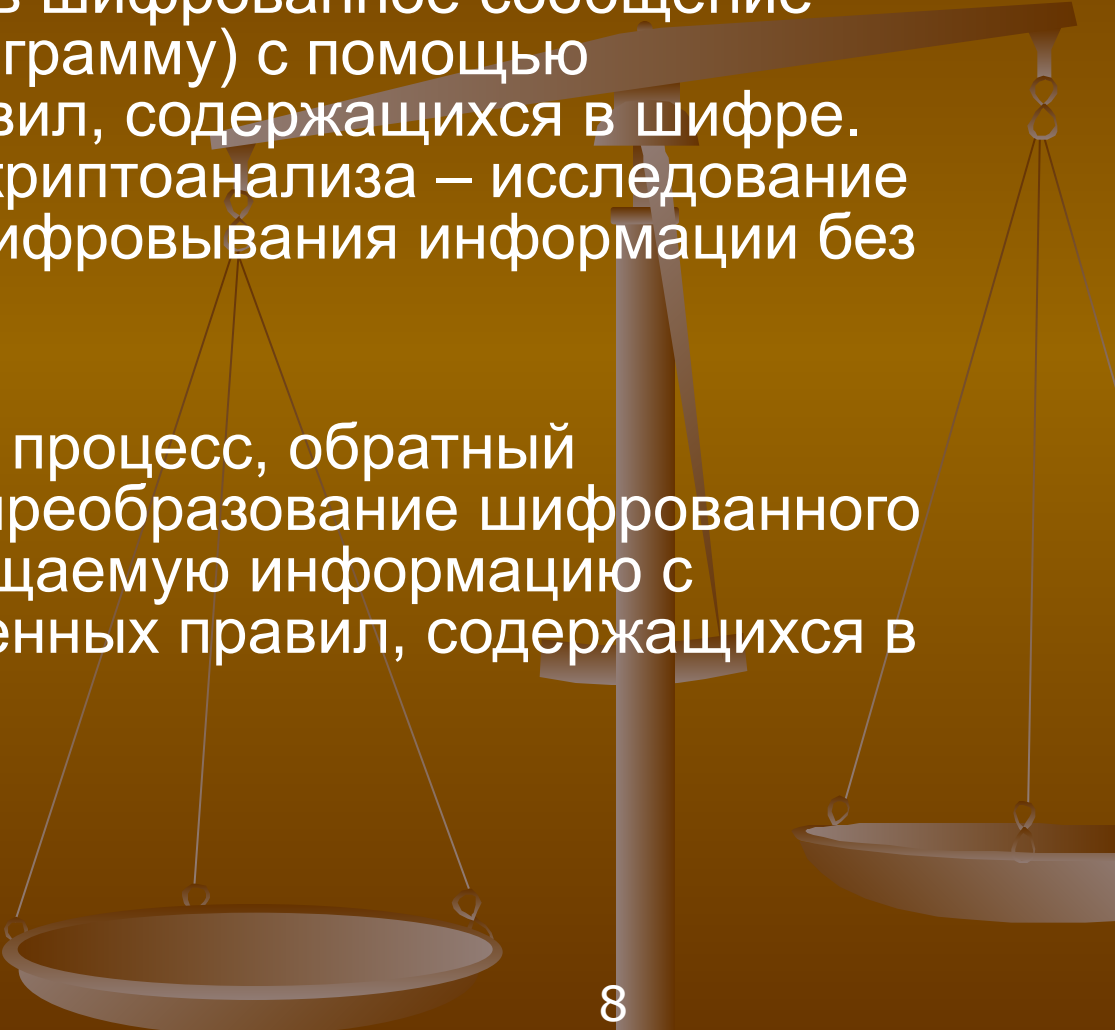
информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации –
деятельность по
предотвращению утечки
защищаемой информации,
несанкционированных и
непреднамеренных воздействий
на защищаемую информацию.



Криптография - наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров.

馬 羊 狗



■ **Шифрование** (зашифрование) – процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре. Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.

■ **Дешифрование** – процесс, обратный шифрованию, т.е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

- **Криптосистемы** разделяются на симметричные (с секретным ключом) и с открытым ключом.
- **Закрытый ключ** – ключ, которым заранее обмениваются два абонента.
- **Открытый ключ (асимметричные алгоритмы)** – использование шифровального (открытого) и дешифровального (закрытого) ключа.

Физкультминутка

1. Посмотреть на кончик носа, на счет 1- 4, а потом перевести взгляд вдаль на счет 1-6. Повторить 4-5 раз.
2. Не поворачивая головы (голова прямо), делать медленно круговые движения глазами вверх -вправо – вниз -влево и в обратную сторону: вверх –влево – вниз –вправо. Затем посмотреть вдаль прямо на счет 1-6. Повторить 4-5 раз.
3. И.п. - руки на поясе. Повернуться направо, локтем правой руки достать до спинки сиденья, вернуться в и.п. То же в другую сторону.
4. И.п. - руки над головой, локти вперед. Развести локти в стороны, прогнуться, вернуться в и.п.

Шифрование данных



Цель работы: знакомство с простейшими приемами шифрования и дешифрования текстовой информации

Задание 1

Шифр Цезаря. Этот шифр реализует следующие преобразования текста: каждая буква исходного текста заменяется следующей после нее буквой в алфавите, который считается написанным по кругу.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Шифр Виженера. Это шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов исходного текста: 31913191 и т.д.

Так например КОМПЬЮТЕР – НПХТЭЖХЁЩ
319319319

Домашнее задание

- Повторить §§5-12 учебника

- Задание №9 к §12.

Расшифровать текст

ВУАЈНУFNBRF – К.,ВУSQ GHTLVТN DCT[

EXFOBRJD!



Литература

- Семакин И.Г.
Информатика и ИКТ. Базовый уровень: учебник для 10-11 классов / И.Г. Семакин, Е.К. Хеннер. – 4-е изд., испр. - М.: БИНОМ. Лаборатория знаний, 2008. – 246 с.: ил.
- Семакин И.Г.
Информатика и ИКТ. Базовый уровень: практикум для 10-11 классов / И.Г. Семакин, Е.К. Хеннер, Т.Ю. Шеина– 3-е изд., испр.– М.: БИНОМ. Лаборатория знаний, 2008. – 120 с.: ил.
- Семакин И.Г.
Информатика и ИКТ. Базовый уровень. 10-11 классы: методическое пособие / И.Г. Семакин, Е.К. Хеннер. – М.: БИНОМ. Лаборатория знаний, 2008. – 102 с.: ил.