1. **Урок по теме** “Тайнопись – от пирамид до современных компьютеров”.
2. **Возраст** учащихся 13-16 лет.(8-11классы).
3. **Название статьи в журнале, ссылка на источник**: «Тайнопись – от пирамид до компьютеров», <http://publ.lib.ru/ARCHIVES/N/''Nauka_i_jizn'''/_''Nauka_i_jizn'''_1996_.html#9601>
4. **Краткая информация об авторе**: Винничек Татьяна Георгиевна 1970 г.р, учитель информатики ГУО «Русиновская СШ» Барановичского района Брестской области РБ,
5. **Описание идеи из первоисточника**. Тайнопись, сделанная руками человека два века назад не раскрыта до сих пор, несмотря на все могущество современной техники. В статье публикуется некоторые особенности шифров, методах шифрования.
6. **Описание цели и планируемого конечного результата** Урок направлен на расширение знаний и умений учащихся в области защиты информации, способствует профессиональному самоопределению учеников. Актуальность данного урока обусловлена тем, что криптография, которая раньше была засекречена, сейчас касается самых разных сторон жизни, в том числе и бытовых. В итоге планируется ознакомить и научить учащихся основам криптографии и крипто анализа для практического применения, выявить связь криптографии с другими науками.
7. Методика воспроизведения для учителя

**Оборудование:** проектор, экран**.**

**Презентация к уроку.**

**Учитель**:

**Слайд 1** Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные.

Представьте себе, что вы хотите подключится в Internet; в меню средств навигации Сети задается вопрос, нужно ли применить режим шифрования, и если вы ответите "нужен", начинается процедура выработки ключа. Чтобы правильно действовать, мы должны иметь представление об основах криптографии. **Слайд 2**  Где вы встречаетесь в жизни с шифрованием?

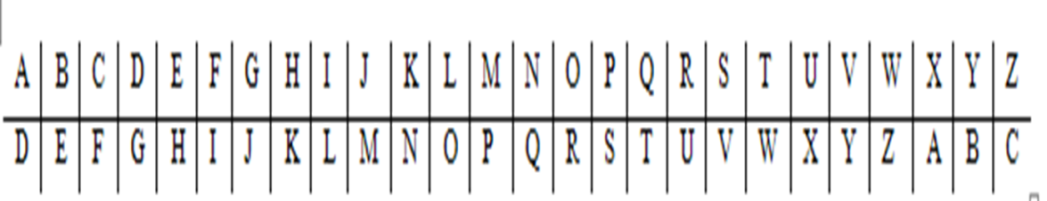
– банковские карточки. Раньше карточки были только магнитными, потом появились интеллектуальные карточки, в них вшит процессор, который выполняет криптографические функции.

 Цифровая подпись – это некоторая криптографическая конструкция, она отличается от шифров, и от нее требуются другие качества: не просто защита открытого текста, защита от отказа от подписи. Именно это имеет исключительное значение во всех делах, связанных с использованием в бизнесе электронных документов.

**Слайд 3** Потребность шифровать сообщения возникла очень давно. В V–VI вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли скиталами. **Слайд 4.** Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полоску папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное он мог, только взяв свою скиталу и намотав на нее без пропусков эту полосу.

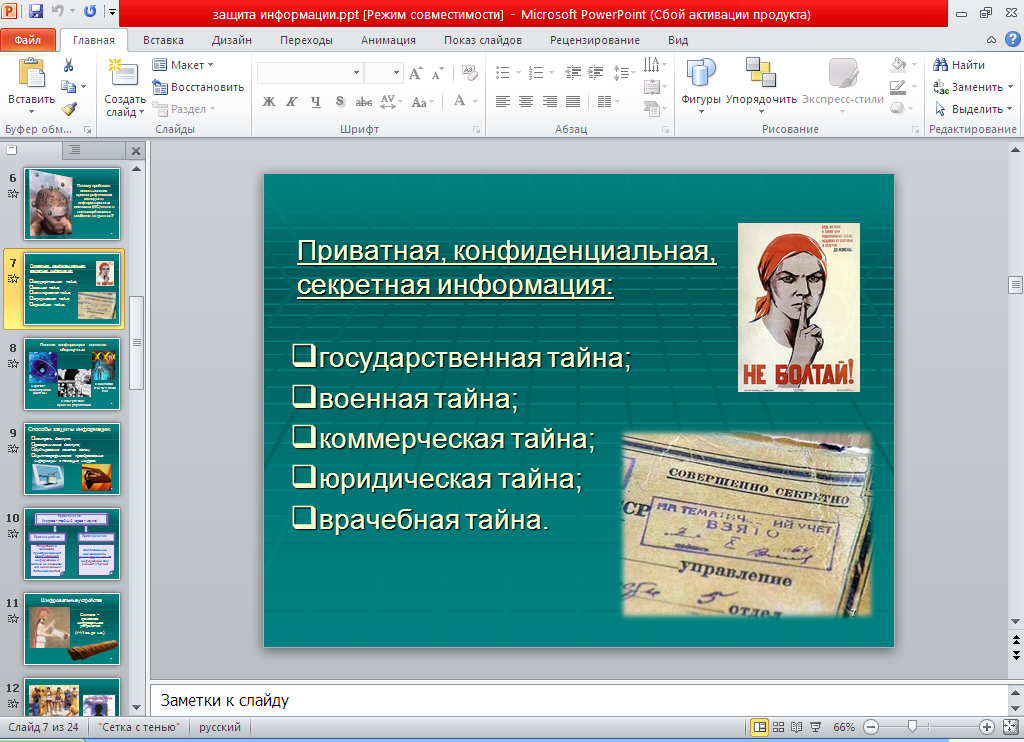
А теперь попробуем зашифровать соседу по парте какое-нибудь сообщение, используя ручку вместо скиталы!

**Слайд 5**

Юлий Цезарь в своем дневнике о войне в Галлии сам изобрел шифр: «сдвинул» алфавит на три буквы вверх, буква «А» стала буквой «Д» и т.д.

**Слайд 6**

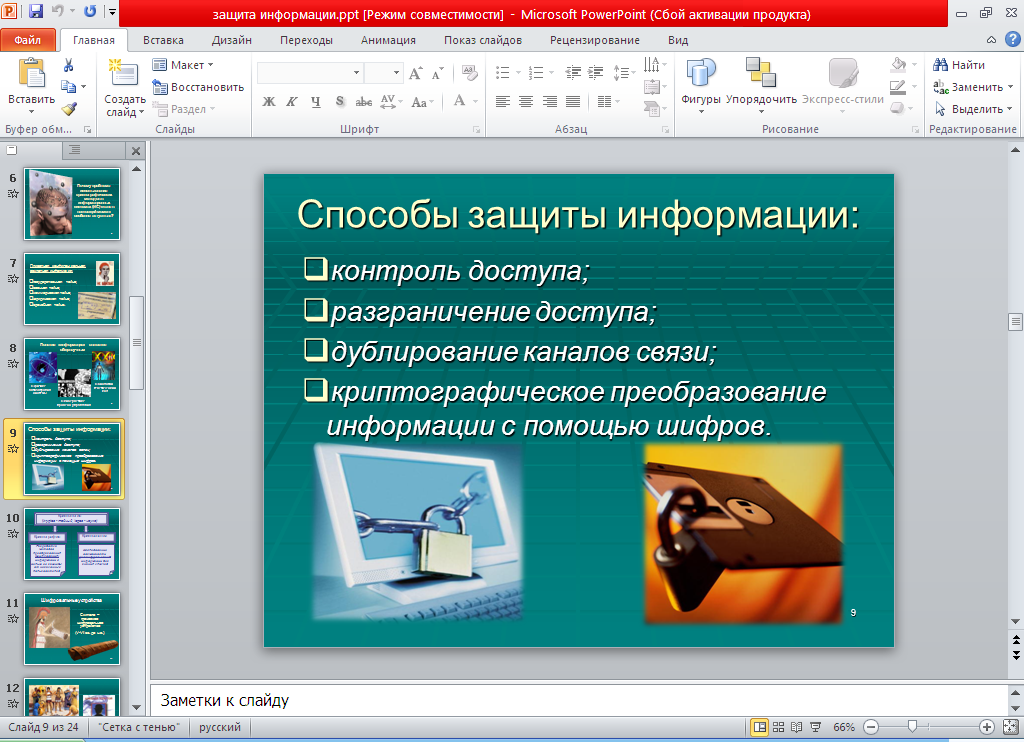
В 1945 году в статье «Теория связи в секретных системах», разработанной американским математиком Шонненом криптография получила статус науки.

Шифровать необходимо только ту информацию, которая нуждается в защите. Обычно в таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

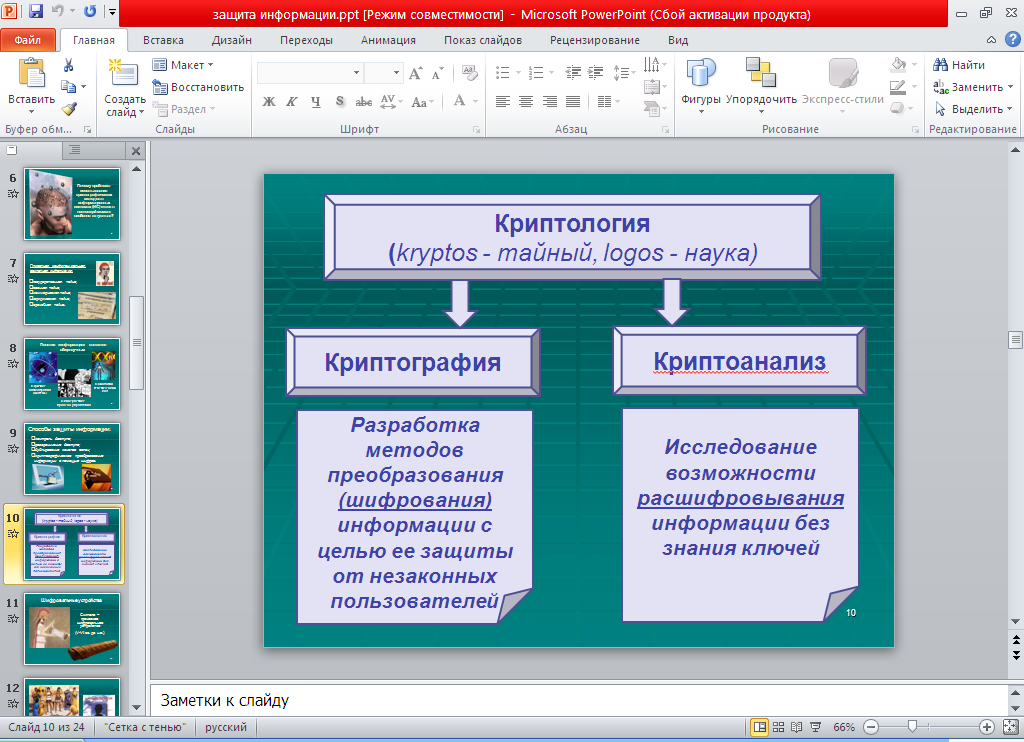
Расширилось использование глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

Появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющие число этих методов может быть успешно использовано и для закрытия информации.

Для предотвращения потери информации разрабатываются различные механизмы ее защиты, которые используются на всех этапах работы с ней.

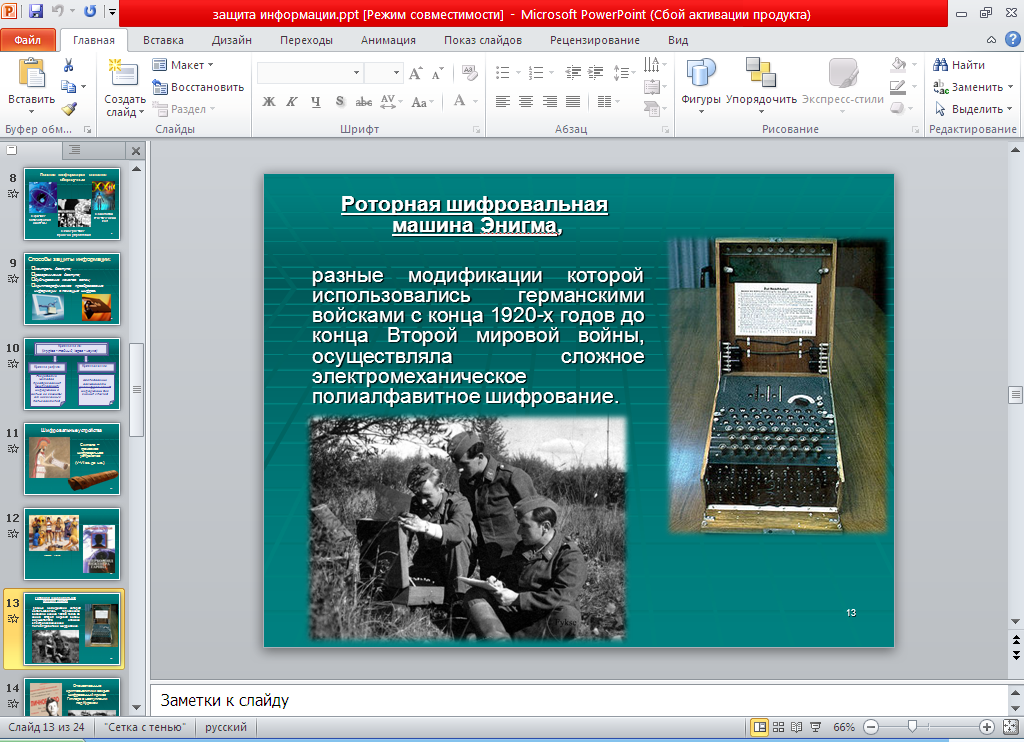
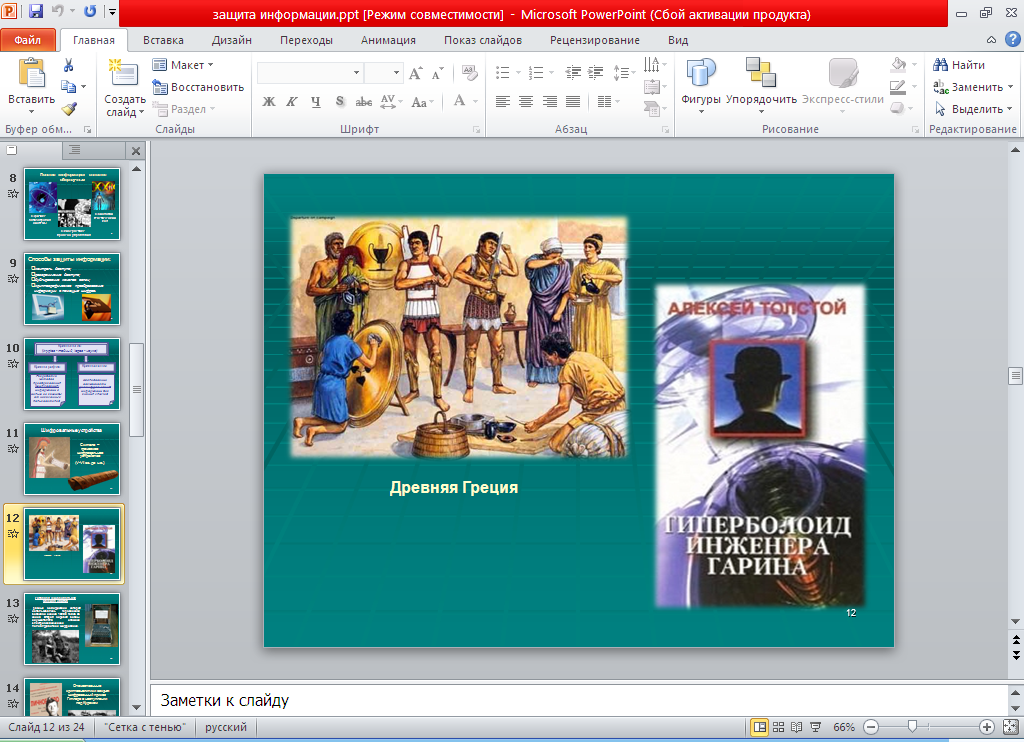
**Слайд 7** Для защиты информации используют различные способы защиты:

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука). Криптология разделяется на два направления – криптографию и криптоанализ. Цели этих направлений прямо противоположны.

**Слайд 8** Разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей занимается **криптография**. Такие методы и способы преобразования информации называются шифрами.

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.

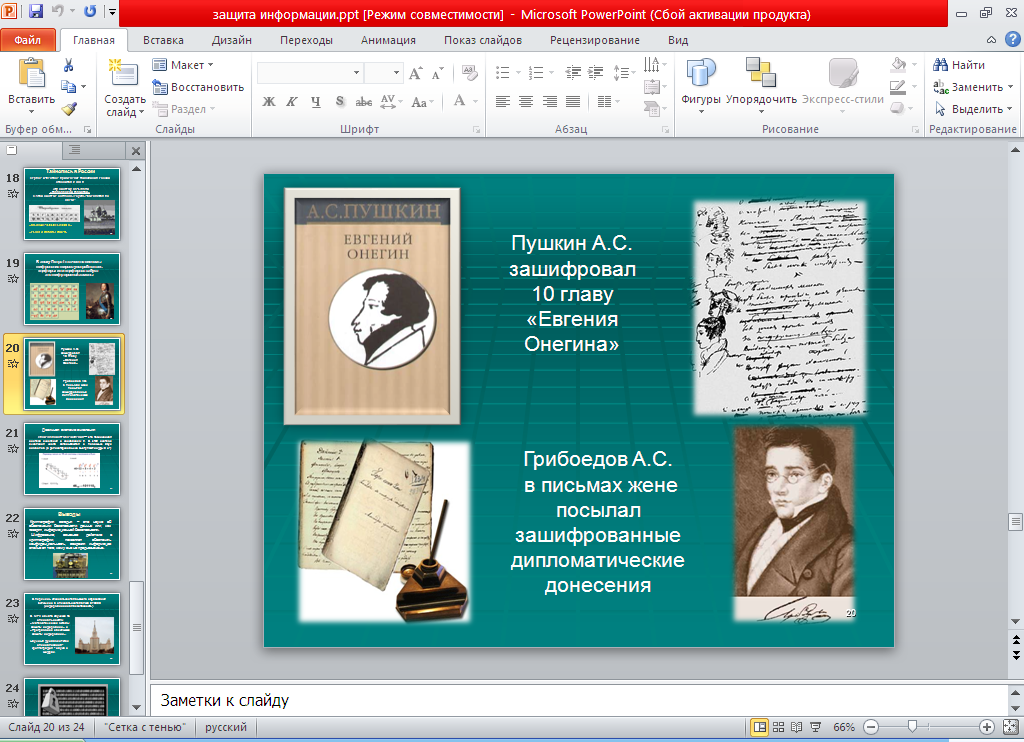
Дешифрование – процесс, обратный шифрованию, т.е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

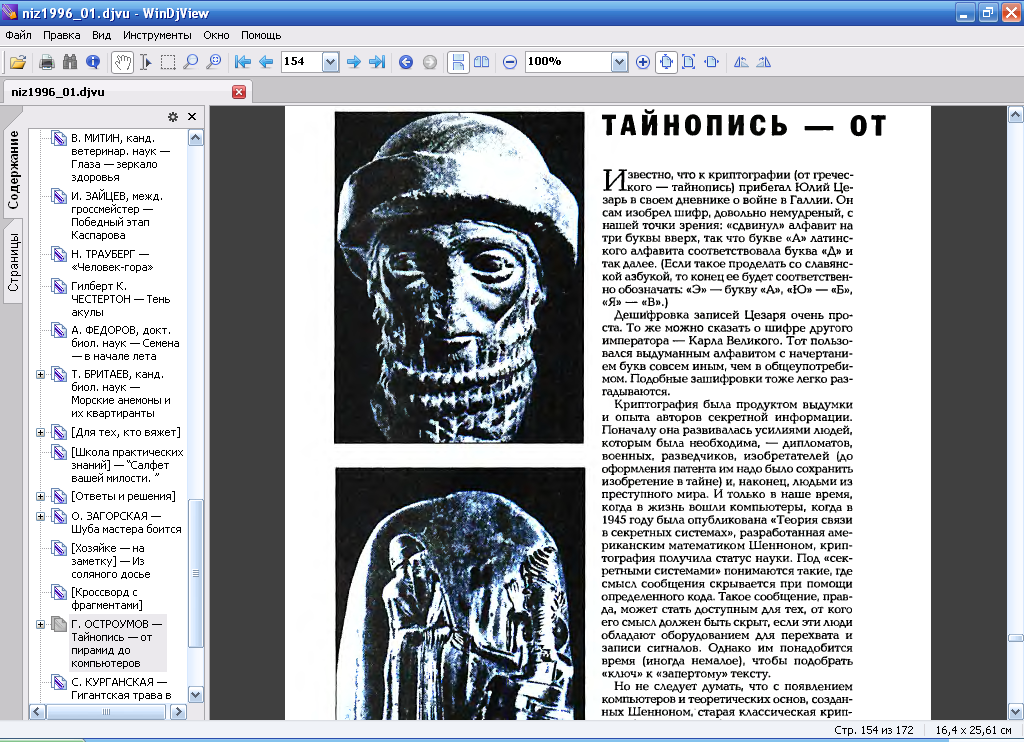
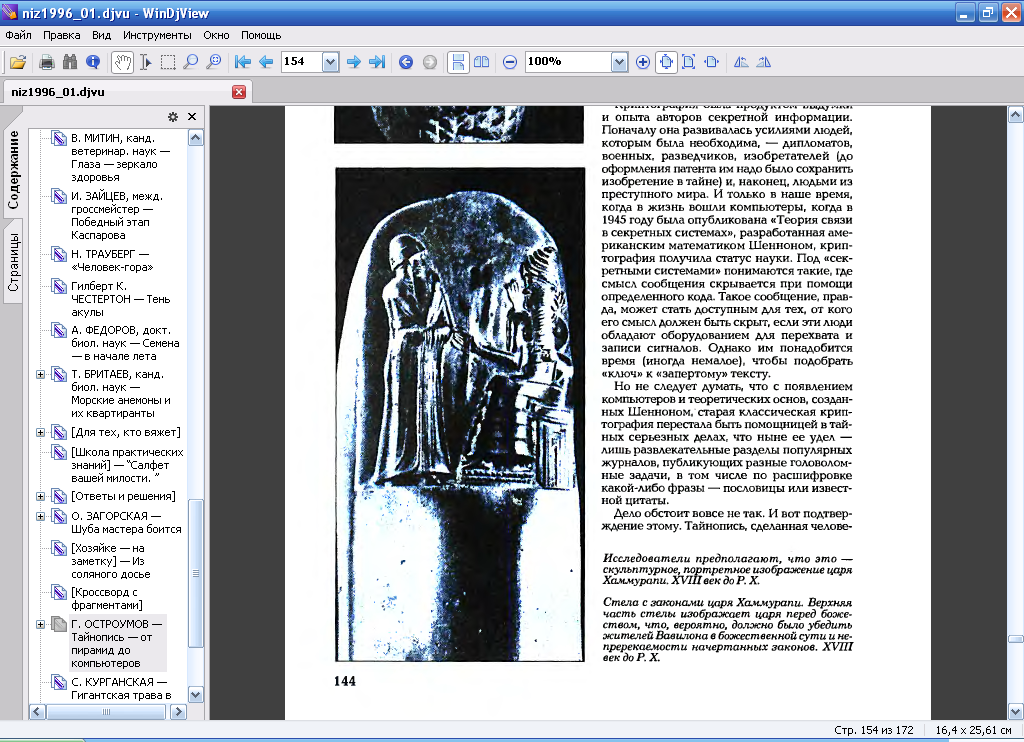
**Слайд 8** В древней Греции однажды обрили раба, написали на его голове, и, когда волосы отросли, отправили с поручением к адресату. Отзвук этой истории можно встретить в "Гиперболоиде инженера Гарина" Алексея Толстого, где текст нанесли на спину мальчика. Если же гонец был надежен и даже под пытками не выдал бы послания, то его изложение могло быть изустным.

**Слайд 9**

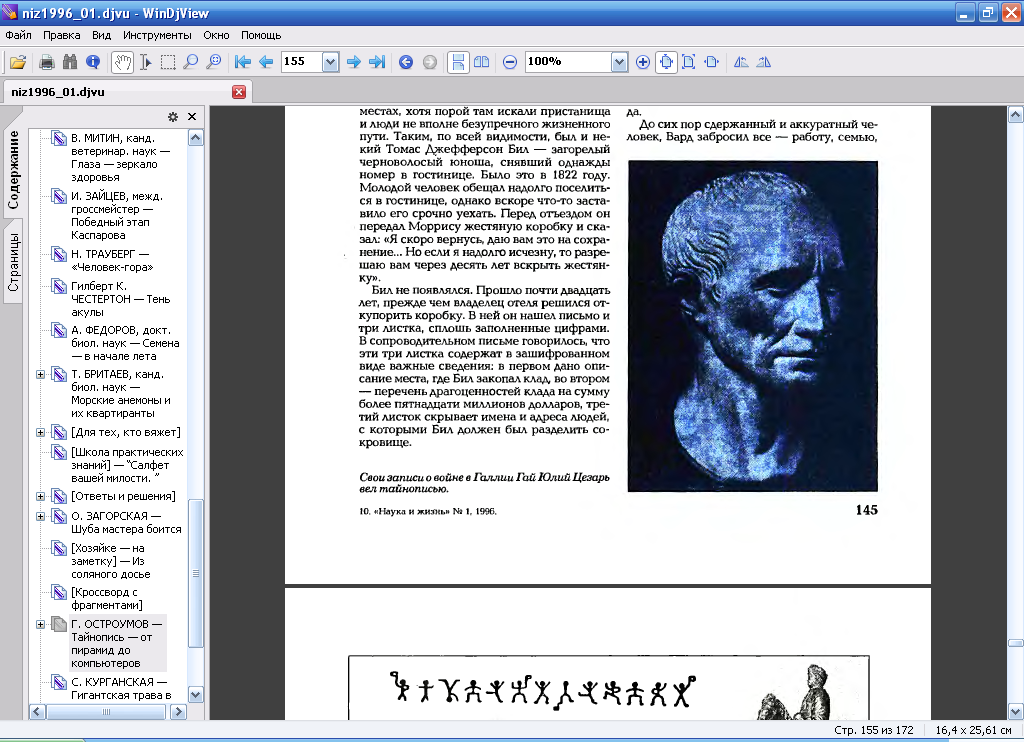
С конца 1920-х годов до конца Второй мировой войны Роторная шифровальная машина Энигма, разные модификации которой использовались германскими войсками, осуществляла сложное электро-механическое полиалфавитное шифрование.

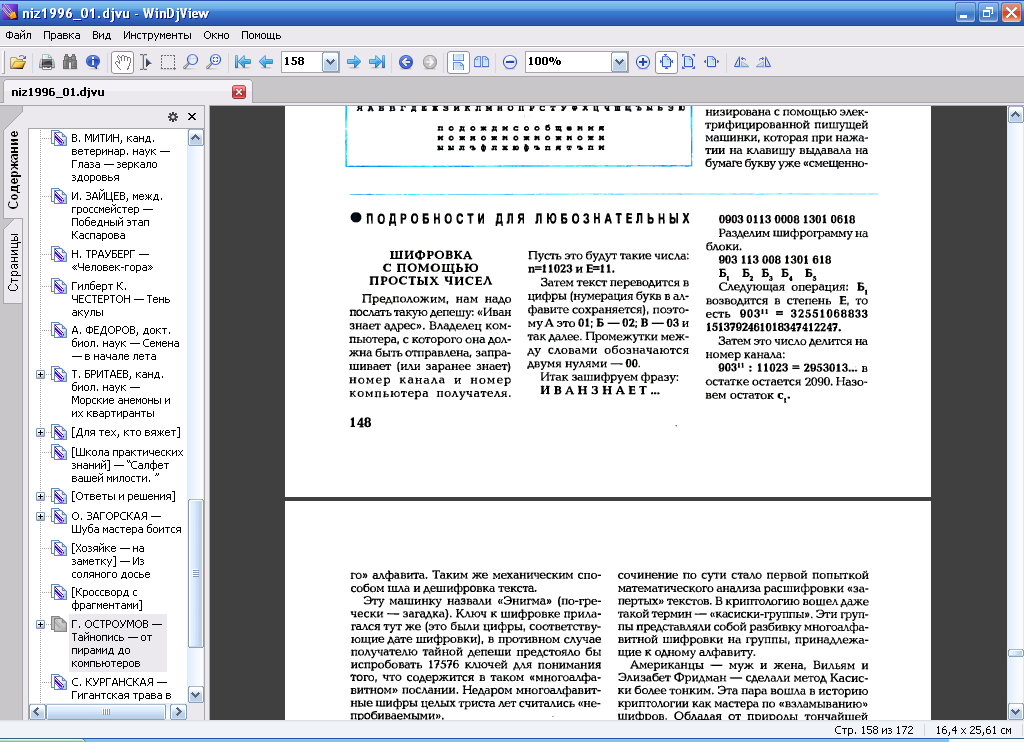
С появлением специальных крупных криптографических подразделений, привлечением талантливых ученых и инженеров криптография в России вышла на передовые позиции, что пригодилось в годы Второй мировой войны. Мы знаем знаменитого разведчика Кузнецова, который назвал дату наступления немецких войск под Курском. Окончательное решение об этой битве было принято после того, как буквально за сутки отечественные криптоаналитики вскрыли шифрованный приказ Гитлера о наступлении.

**Слайд 10** Великий русский поэт А.С. Пушкин также применял знания о криптологии, так десятая глава "Евгения Онегина" отчасти была сожжена поэтом, а остатки дошли до нас в виде фрагментов, большей частью зашифрованных. Интересно использование шифров в письмах Грибоедова к своей жене из Персии. При исследовании, сделанном криптоаналитиками, оказалось, что эти письма содержали дипломатические послания Грибоедова. Написав донесение через трафарет, Грибоедов дописывал разбросанные по листу буквы в связный текст так, чтобы он содержал письмо жене и отправлял его с обычной почтой. Российские секретные службы перехватывали это письмо, расшифровывали, а затем доставляли адресату.

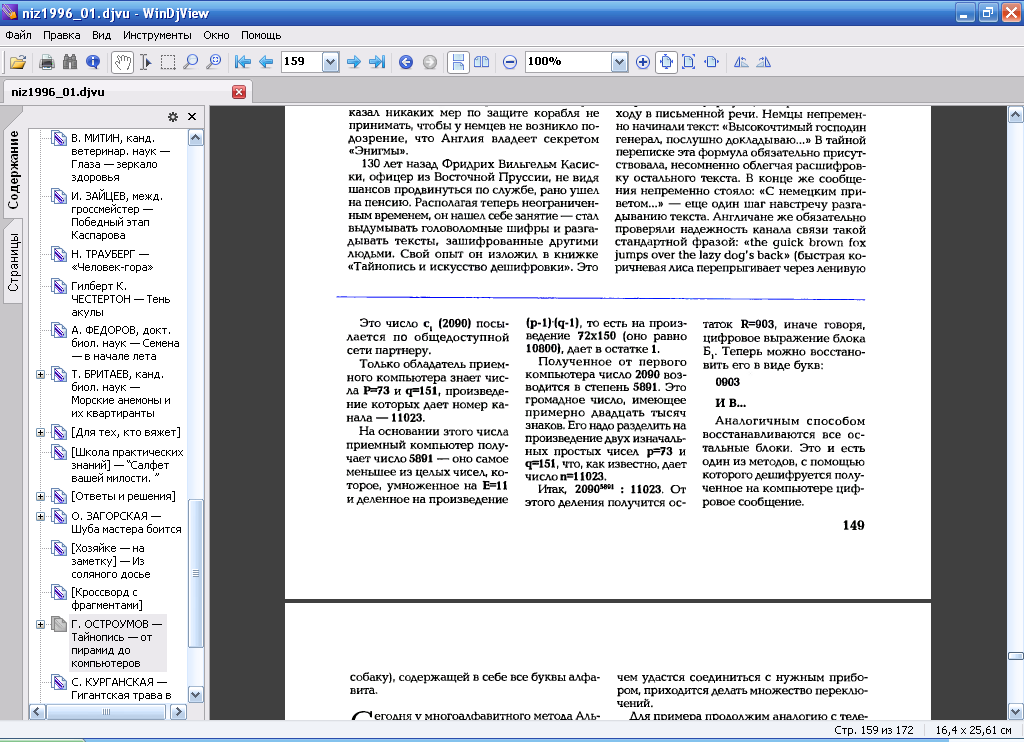
**Слайд 11** Исследователи предполагают, что это скульптурное, портретное изображение царя Хаммурапи.

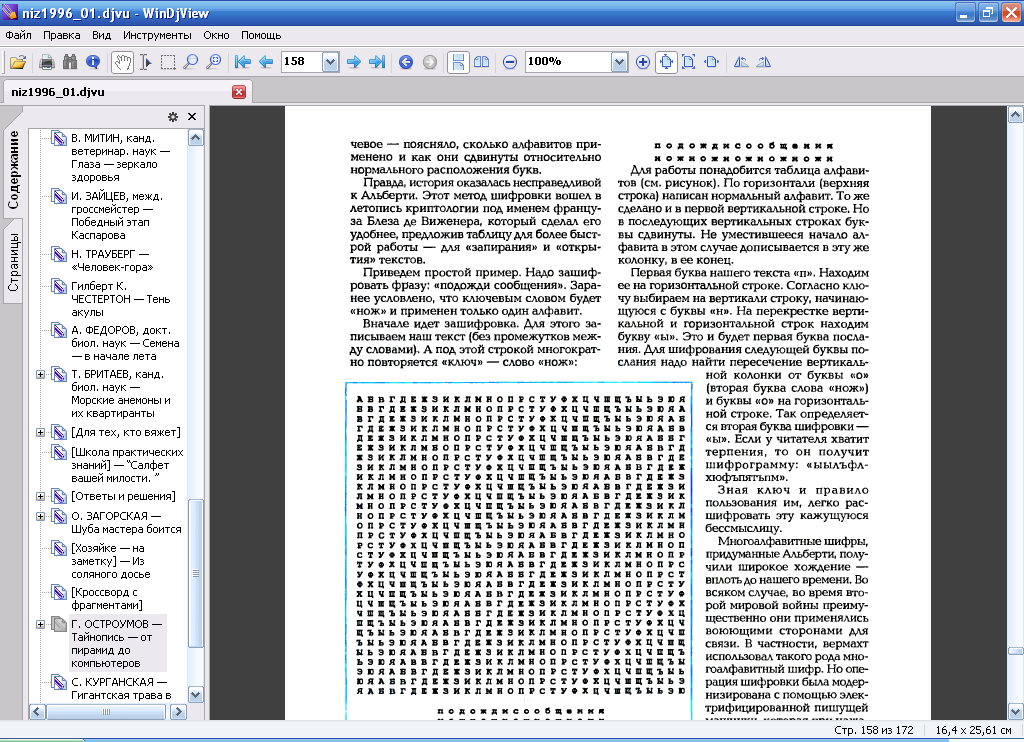
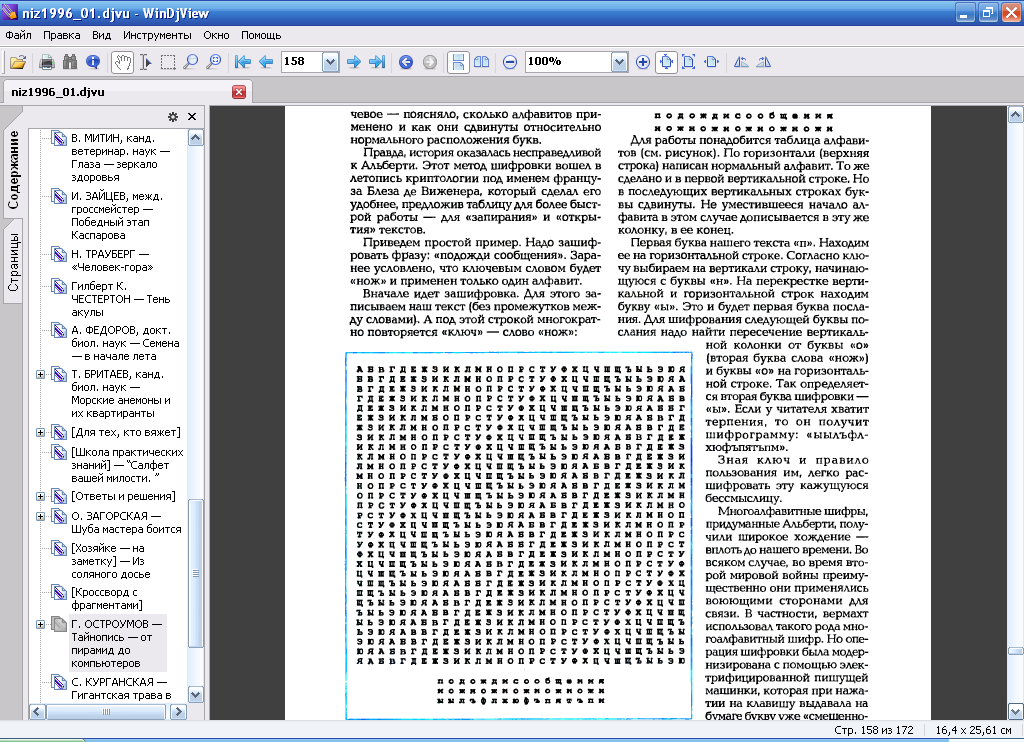
Стела с законами царя Хаммурапи. Верхняя часть стелы изображает царя перед божеством, что вероятней всего должно было убедить жителей Вавилона в божественной сути и непререкаемости начертанных законов XVIII векдо Р.Х.

**Слайд 12** В истории криптографии хорошо известен пример с Томом Джефферсоном Биллом, который остановился в гостинице и вскоре исчез передав жестяную коробку владельцу гостинницы и попросив его открыть ее только в том случае, если он исчезнет. После 20 лет отсутствия владелец гостинницы Вард в сопроводительном письме этой коробки прочитал о кладе в 15млн долларов Сдержаный и аккуратный забросил семью, работу и до конца своих дней он расшифровал лишь один лист из трех, в котором было описание клада, пронумеровав все буквы «декларации».

****130 лет назад фицер Восточной Пруссии Фридрих Вильгельм Касиски уйдя рано на пенсию стал придумывать головоломки и разгадыать тексты других людей. Свой опыт он изложил в книге « Тайнопись и исксство дешифровки». Это сочинение стало первой попыткой математического анализа расшифровки «запертых» текстов.В криптологию вошел термин «касиски-группы». Эти группы представляли собой разбику многоалфавитной шифровки на буквы, принадлежащие одному алфавиту. Этот метод разработан независимо Фридрихом Касиски и Чарльзом Бэббиджем. Метод Касиски позволяет криптоаналитику найти длину ключевого слова.

**Слайд 13**



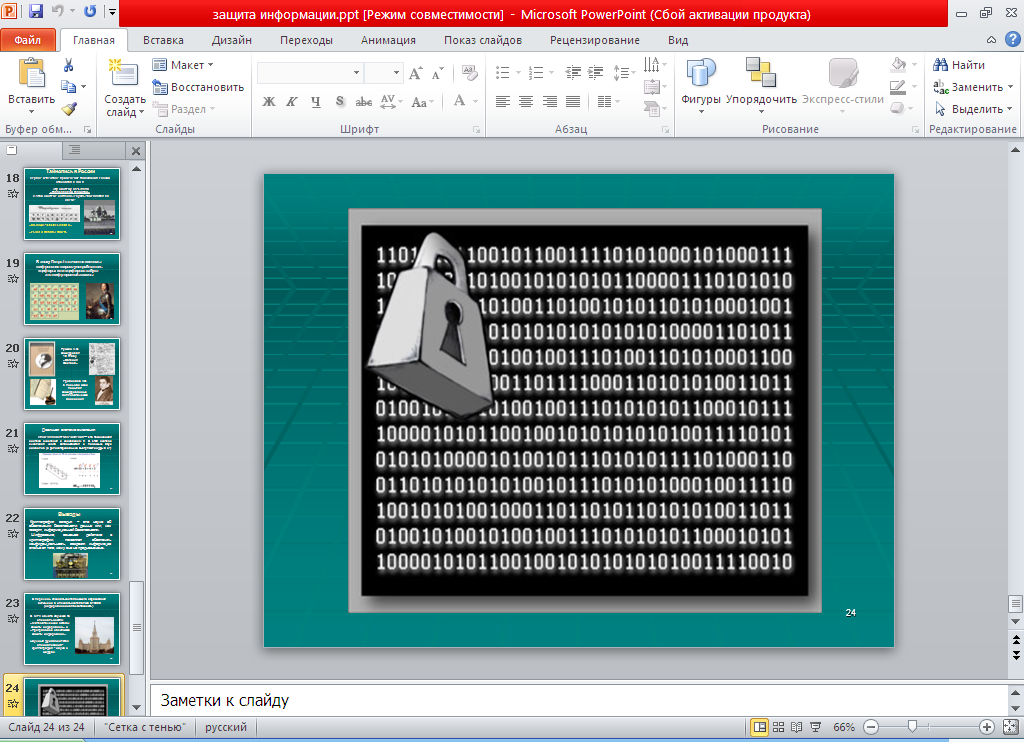


Идем дальше метод шифровки француза Блеза де Виженера. Пример:

**Слайд 14.** Надо зашифровать фразу «**подожди сообщения**» Заранее установлено, что ключевым словом будет слово «нож».

первая буква «п» ищем в таблице по горизонтали «н» по вертикали

Выдающийся математик Алан Тьюринг соорудил Англии первую электронно-счетную машину, как мы называем теперь **компьютер!**

Сегодня эти методы для компьютера не актуальны и криптологи обратились к математике. Разложение больших чисел на множители, переводят не знаки в слове, а слоги.

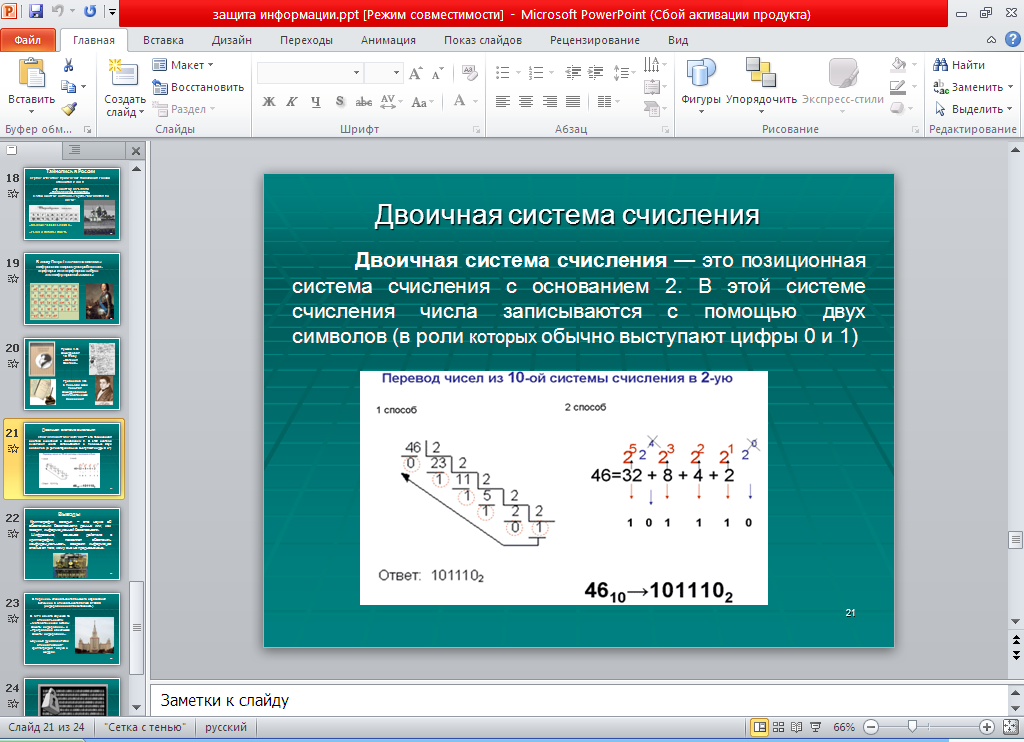
**Слайд 15 Заключение:**

Мы рассмотрели различные типы шифров от древности до

наших дней.

**Это интересно**!!!:

Великий русский поэт А.С. Пушкин также применял знания о криптологии, так десятая глава "Евгения Онегина" отчасти была сожжена поэтом, а остатки дошли до нас в виде фрагментов, большей частью зашифрованных. Интересно использование шифров в письмах Грибоедова к своей жене из Персии. При исследовании, сделанном криптоаналитиками, оказалось, что эти письма содержали дипломатические послания Грибоедова. Написав донесение через трафарет, Грибоедов дописывал разбросанные по листу буквы в связный текст так, чтобы он содержал письмо жене и отправлял его с обычной почтой.

**Слайд 1****6** Как представить текстовую информацию на ЭВМ, если для компьютера вся система счисления представлена в виде двоичного кода? В этом опять помогает криптография с ее возможностью кодировать и декодировать информацию разными методами.

С точки зрения криптологии, живой организм является сложной криптосистемой (зашифрованная информация содержится в генах). Примером применения методов дешифровки и современных технологий создания искусственного интеллекта является метод криптоанализа с помощью генетических алгоритмов.

Состязанию шифровальщиков и тех, кто стремится прочесть запретный текст, кажется, не видно конца.

**Для учащихся предлагается домашнее задание**: придумать свои способы кодирования и декодирования информации. На последующих уроках планируется написание программ , которые будут осуществлять полученные способы шифрования.

**Выводы**: Криптология в наши дни приобрела значимость и нашла новые сферы применения, она нужна не только для защиты государственных интересов, но и необходима для защиты частной жизни каждого современного человека.