

Тема урока:

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ



Как вы думаете, какая информация может быть защищаемой?

государственная тайна

военная тайна

коммерческая тайна

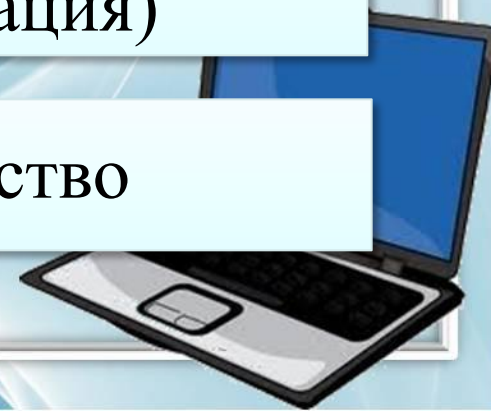
врачебная тайна

персональные данные

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



Любая информация является чьей-то собственностью. Поэтому **защита информации** государственными законами рассматривается как **защита собственности**.



Цифровая информация – это информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

Цели урока:

- рассмотрим виды угроз и меры защиты цифровой информации;
- применим на практике меры защиты личной информации на ПК;
- научимся применять простейшие криптографические шифры для шифрования и дешифрования текста.



Виды угроз для цифровой информации

разрушение,
уничтожение

кража или утечка

несанкционированное

непреднамеренное

- вирусы-разрушители;
- вирусы-шпионы (троянцы)
- деятельность хакеров;
- атака на сервер

- ошибка пользователя;
- сбой оборудования;
- сбой ПО;
- авария электросети, пожар и т.п.

- глобальные сети;
- телефонная
сотовая связь



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

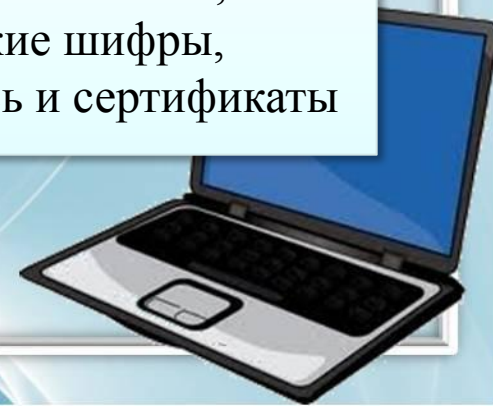
Меры защиты информации

от угрозы разрушения,
уничтожения:

- антивирусные программы,
- брандмауэры, межсетевые экраны,
- резервное копирование,
- контроль оборудования;
- разграничение доступа;
- использование БП

от угрозы кражи
или утечки:

- физическая защита каналов,
- криптографические шифры,
- цифровая подпись и сертификаты



Какие вы знаете антивирусные программы?



Dr.Web



**Kaspersky
Internet Security**



AVIRA



ESET NOD32



**AVG
Anti-Virus**



Avast



**Comodo
Antivirus Free**



Антивирусные программы, брандмауэры, межсетевые экраны

Антивирусные программы предназначены для борьбы с намеренно разработанными программами-вирусами, которые находятся в компьютере.

Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.

Межсетевые экраны - это брандмауэры, защищающие сети, подключенные к другим сетям.



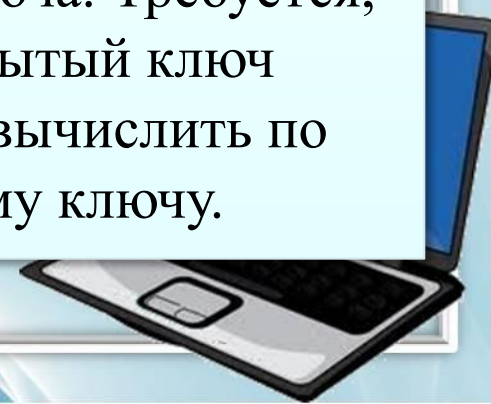
Криптография

Криптография (в переводе с др. греч. – «тайнопись») - наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров.

Методы шифрования

Закрытый ключ - ключ, которым заранее обмениваются два абонента; единый ключ для шифрования и дешифрования. Основная задача – сохранить ключ втайне от третьих лиц.

Открытый ключ - (асимметричные алгоритмы) – использование шифровального (открытого) и дешифровального (закрытого) ключа. Требуется, чтобы закрытый ключ невозможно вычислить по открытому ключу.



Пример закрытого ключа

Попробуйте догадаться, в чем секрет одного из вариантов ключа Цезаря, с помощью которого зашифровано слово

«К Р И П Т О Г Р А Ф И Я»

в следующем шифрованном сообщении

«Л С Й Р У П Д С Б Х Й А»

Ответ: ключ заключается в циклическом смещении алфавита на 1 позицию.

* Для русского алфавита возможно 32 варианта ключей шифра Цезаря, отличающихся величиной смещения



Цифровые подписи и сертификаты

Цифровая подпись – это индивидуальный секретный шифр, ключ которого известен только владельцу. Алгоритм шифрования с открытым ключом, но иначе, чем обычно: закрытый ключ применяется для шифрования, а открытый для дешифрования.

Цифровой сертификат - это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.

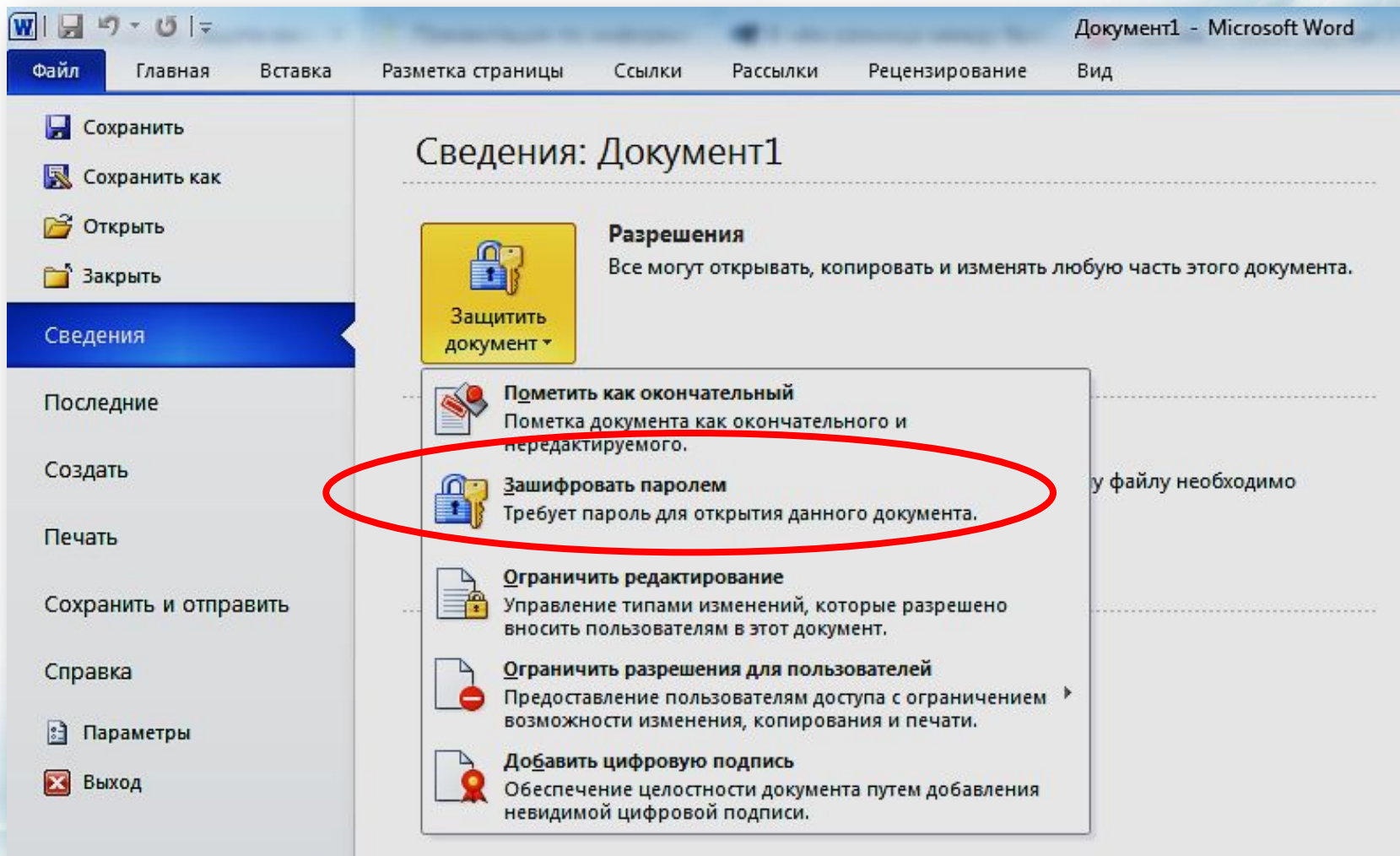


Практическая работа по паролированию и архивированию данных для обеспечения защиты

Задание 1. Защита папки, документа, книги или презентации с помощью паролей, разрешений и других ограничений.
Архивирование данных.



Паролирование в Microsoft Word



The screenshot shows the Microsoft Word interface with the ribbon set to 'Сведения' (Information). The 'Защитить документ' (Protect Document) button is highlighted with a red oval. The ribbon also shows 'Разрешения' (Permissions) and 'Защитить документ' (Protect Document) options. The 'Защитить документ' button is highlighted with a red oval.

Документ1 - Microsoft Word

Файл Главная Вставка Разметка страницы Ссылки Рассылки Рецензирование Вид

Сохранить
Сохранить как
Открыть
Закрыть

Сведения

Последние
Создать
Печать
Сохранить и отправить
Справка
Параметры
Выход

Сведения: Документ1

Разрешения

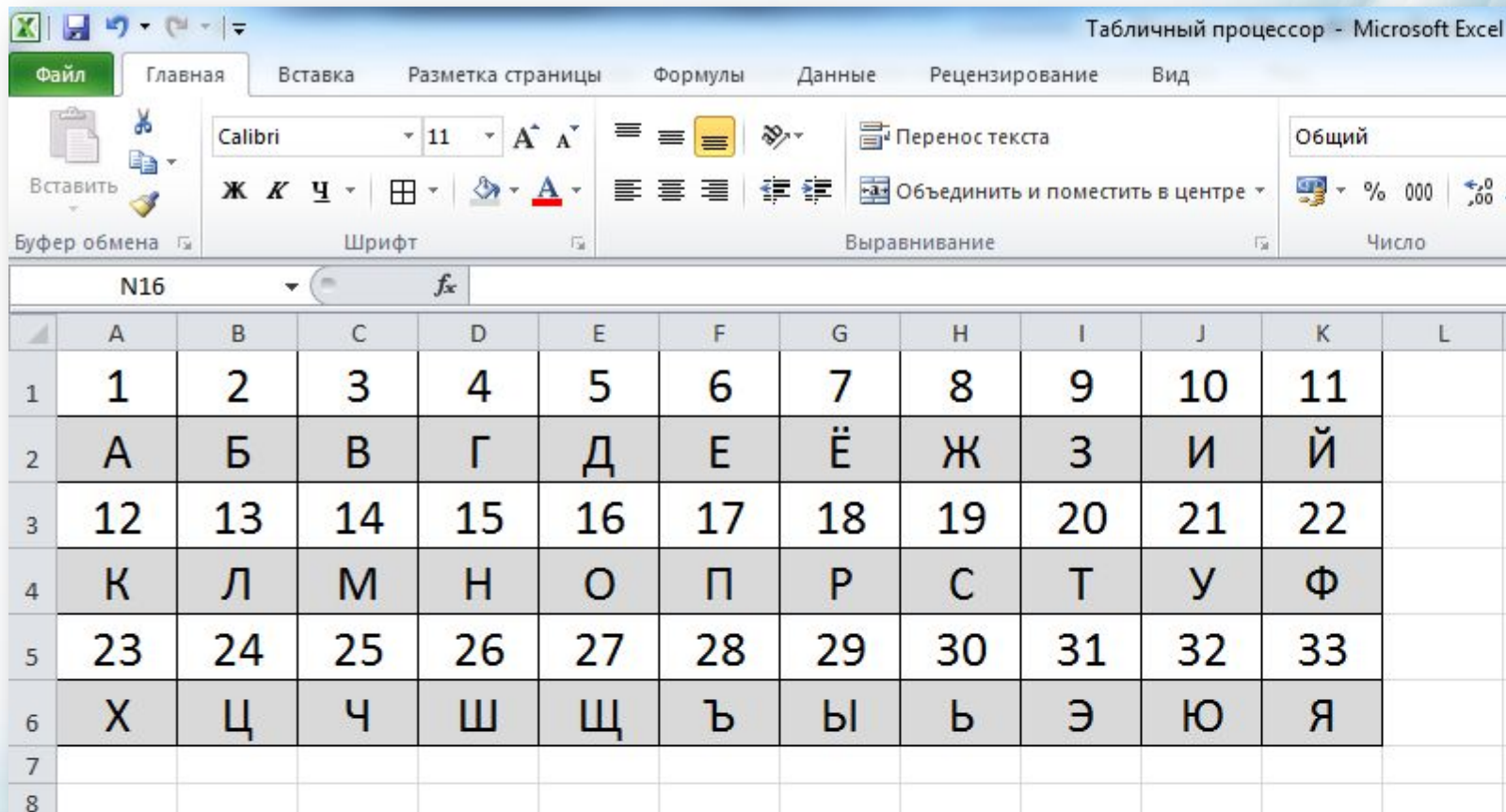
Все могут открывать, копировать и изменять любую часть этого документа.

Защитить документ

- Пометить как окончательный**
Пометка документа как окончательного и неотредактируемого.
- Зашифровать паролем**
Требует пароль для открытия данного документа.
- Ограничить редактирование**
Управление типами изменений, которые разрешено вносить пользователям в этот документ.
- Ограничить разрешения для пользователей**
Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.
- Добавить цифровую подпись**
Обеспечение целостности документа путем добавления невидимой цифровой подписи.

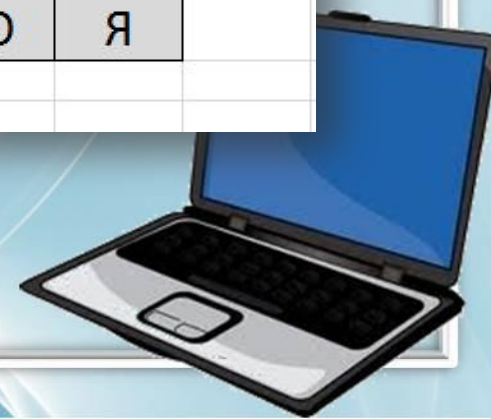
у файлу необходимо

Паролирование в Microsoft Excel

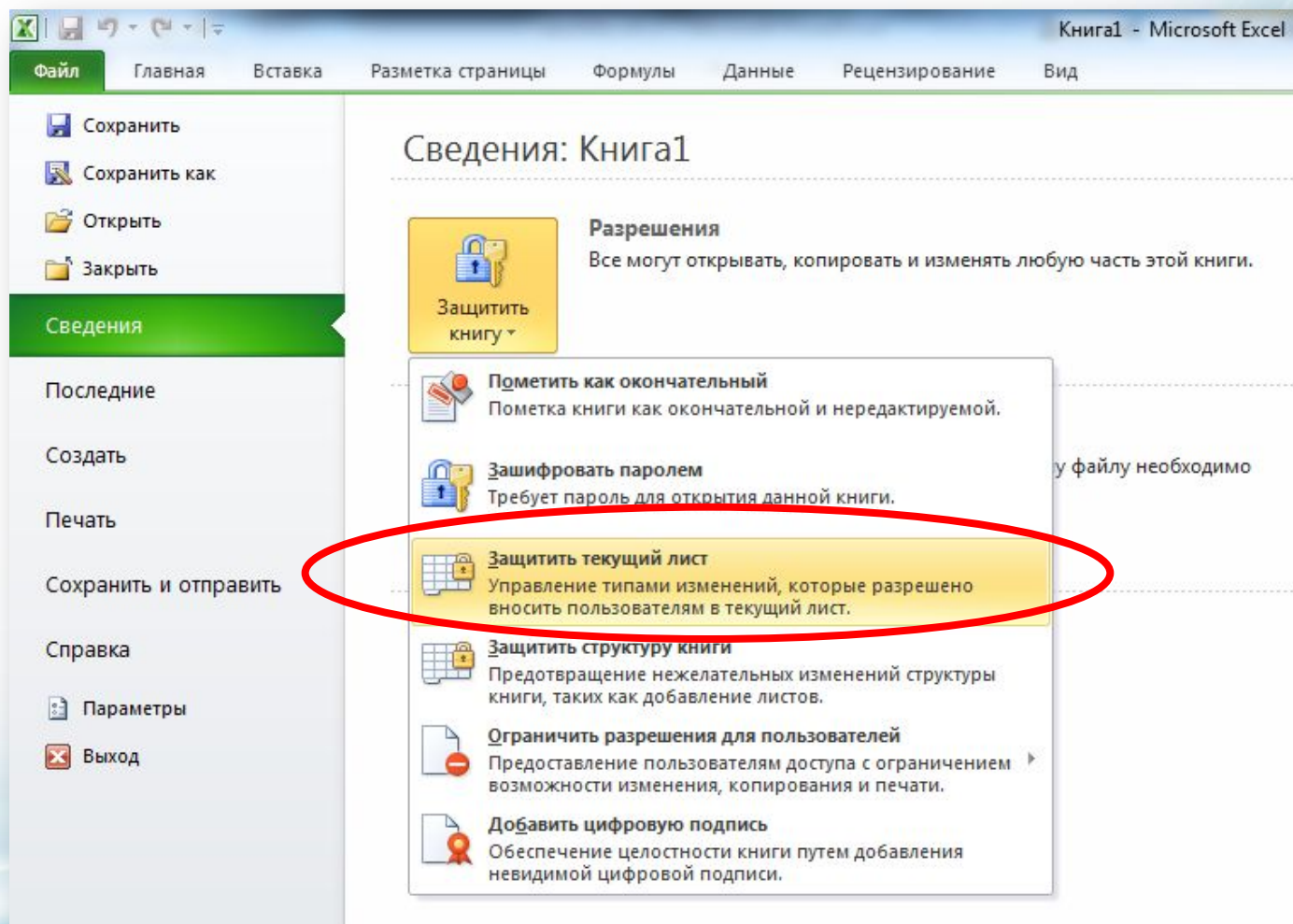


The screenshot displays the Microsoft Excel interface. The title bar reads "Табличный процессор - Microsoft Excel". The ribbon includes "Файл", "Главная", "Вставка", "Разметка страницы", "Формулы", "Данные", "Рецензирование", and "Вид". The "Главная" ribbon is active, showing options for font (Calibri, size 11), alignment, and number formatting. The formula bar shows "N16". The grid contains the following data:

	A	B	C	D	E	F	G	H	I	J	K	L
1	1	2	3	4	5	6	7	8	9	10	11	
2	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	
3	12	13	14	15	16	17	18	19	20	21	22	
4	К	Л	М	Н	О	П	Р	С	Т	У	Ф	
5	23	24	25	26	27	28	29	30	31	32	33	
6	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
7												
8												



Паролирование в Microsoft Excel



Книга1 - Microsoft Excel

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид

Сохранить
Сохранить как
Открыть
Закрыть

Сведения

Последние
Создать
Печать
Сохранить и отправить
Справка
Параметры
Выход

Сведения: Книга1

Разрешения
Все могут открывать, копировать и изменять любую часть этой книги.

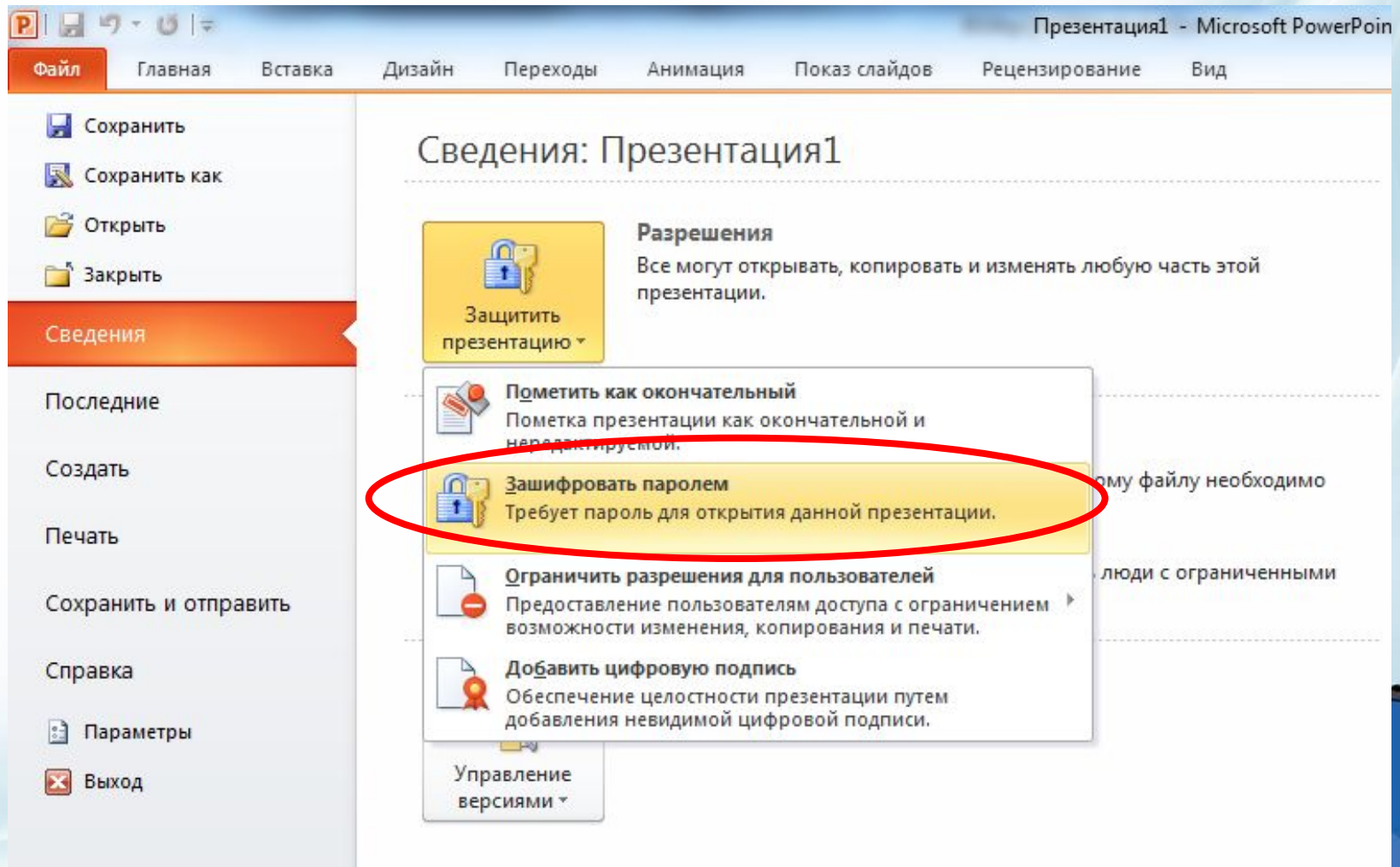
Защитить книгу

- Пометить как окончательный**
Пометка книги как окончательной и нередактируемой.
- Зашифровать паролем**
Требует пароль для открытия данной книги.
- Защитить текущий лист**
Управление типами изменений, которые разрешено вносить пользователям в текущий лист.
- Защитить структуру книги**
Предотвращение нежелательных изменений структуры книги, таких как добавление листов.
- Ограничить разрешения для пользователей**
Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.
- Добавить цифровую подпись**
Обеспечение целостности книги путем добавления невидимой цифровой подписи.

у файлу необходимо



Паролирование в Microsoft PowerPoint



The screenshot shows the Microsoft PowerPoint interface. The title bar reads 'Презентация1 - Microsoft PowerPoint'. The ribbon includes 'Файл', 'Главная', 'Вставка', 'Дизайн', 'Переходы', 'Анимация', 'Показ слайдов', 'Рецензирование', and 'Вид'. The 'Файл' (File) tab is active, showing a sidebar with options: Сохранить, Сохранить как, Открыть, and Закреть. Below these are 'Сведения' (highlighted in orange), 'Последние', 'Создать', 'Печать', 'Сохранить и отправить', 'Справка', 'Параметры', and 'Выход'. The main area displays 'Сведения: Презентация1' with a 'Защитить презентацию' button. A dropdown menu is open, listing: 'Пометить как окончательный', 'Зашифровать паролем' (circled in red), 'Ограничить разрешения для пользователей', and 'Добавить цифровую подпись'. A 'Управление версиями' button is at the bottom of the dropdown.

Презентация1 - Microsoft PowerPoint

Файл Главная Вставка Дизайн Переходы Анимация Показ слайдов Рецензирование Вид

Сохранить
Сохранить как
Открыть
Закреть

Сведения

Последние
Создать
Печать
Сохранить и отправить
Справка
Параметры
Выход

Сведения: Презентация1

Защитить презентацию

Разрешения
Все могут открывать, копировать и изменять любую часть этой презентации.

Пометить как окончательный
Пометка презентации как окончательной и нередactable.

Зашифровать паролем
Требует пароль для открытия данной презентации.

Ограничить разрешения для пользователей
Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.

Добавить цифровую подпись
Обеспечение целостности презентации путем добавления невидимой цифровой подписи.

Управление версиями



Архивирование и паролирование данных

1. Выделить папку «Защита информации».
2. Правой кнопкой мыши вызвать контекстное меню Windows.
3. Выберите пункт «**Add to archive...**» («**Добавить в архив...**»).
4. Откроется меню архивации WinRar.
5. Вкладка «Общие» нажать на кнопку «**Установить пароль**».
6. Ввести пароль и нажать «**ОК**».



Практическая работа по шифрованию данных

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.

Пример:

	A	B	C	D	E	F	G	H	I	J
1	Шифр Виженера									
2	ключ	В	А	З	А	В	А	З	А	В
3	сдвиг	З	1	9	1	З	1	9	1	З
4	текст	К	О	М	П	Ь	Ю	Т	Е	Р
5	шифр	Н	П	Х	Т	Э	Ж	Х	Ё	Щ
6										



Практическая работа по шифрованию данных

Задание 2. Шифр Виженера. Используя в качестве ключевого слова **ЗИМА**, закодировать слова:

- КОМПЬЮТЕР

УШЪРЕЗАЁЩ

- ИНТЕРНЕТ

СЧАЁЩЧТУ

- БЕЗОПАСНОСТЬ

ЙОХПШЙЯОЧЫАЭ

