

Лабораторна робота 5

ДОСЛІДЖЕННЯ ПРОЦЕСІВ КІБЕРЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Мета: дослідження процесів захисту інформації від несанкціонованого доступу шляхом накладання паролів на документи, створених засобами Microsoft Office 2016, архівних документів.

ТЕОРЕТИЧНІ ВІДОМОСТІ ТА ХІД РОБОТИ

1. Методи та засоби накладання паролів на офісні документи Microsoft Office:

1.1. Методи та засоби накладання паролів на документи текстового редактора Microsoft Word;

Для захисту текстових документів створених засобами Microsoft Word використовується наступна послідовність дій:

1. Пуск→Програми→ Microsoft Office→ Microsoft Word, рисунок 1.



Рисунок 1

2. Створюємо будь-який документ (може містити фразу, малюнок, таблицю), рисунок 2 та зберігаємо його під наступною назвою: **номер групи_Прізвище студента. Наприклад, КБ 20 1 Лобанчикова.**

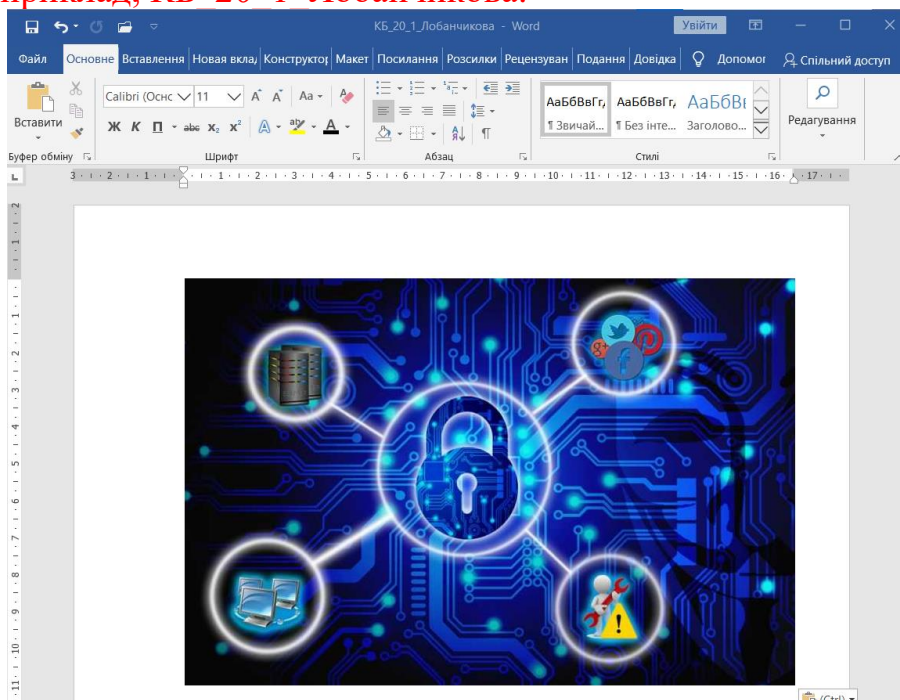


Рисунок 2

3. Відкриваємо:

Рецензування→Захист.

Я видно з вікна, що представлено на рисунку 3-5 пропонується декілька варіантів використання параметрів безпеки.

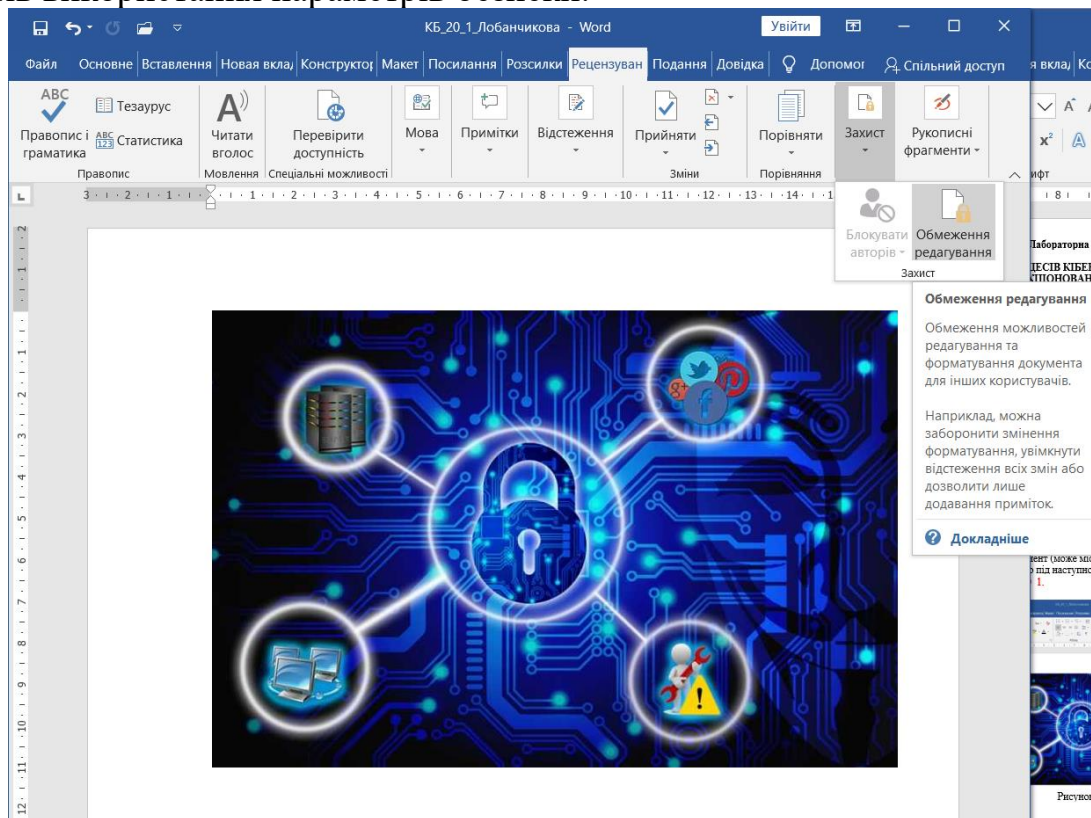


Рисунок 3

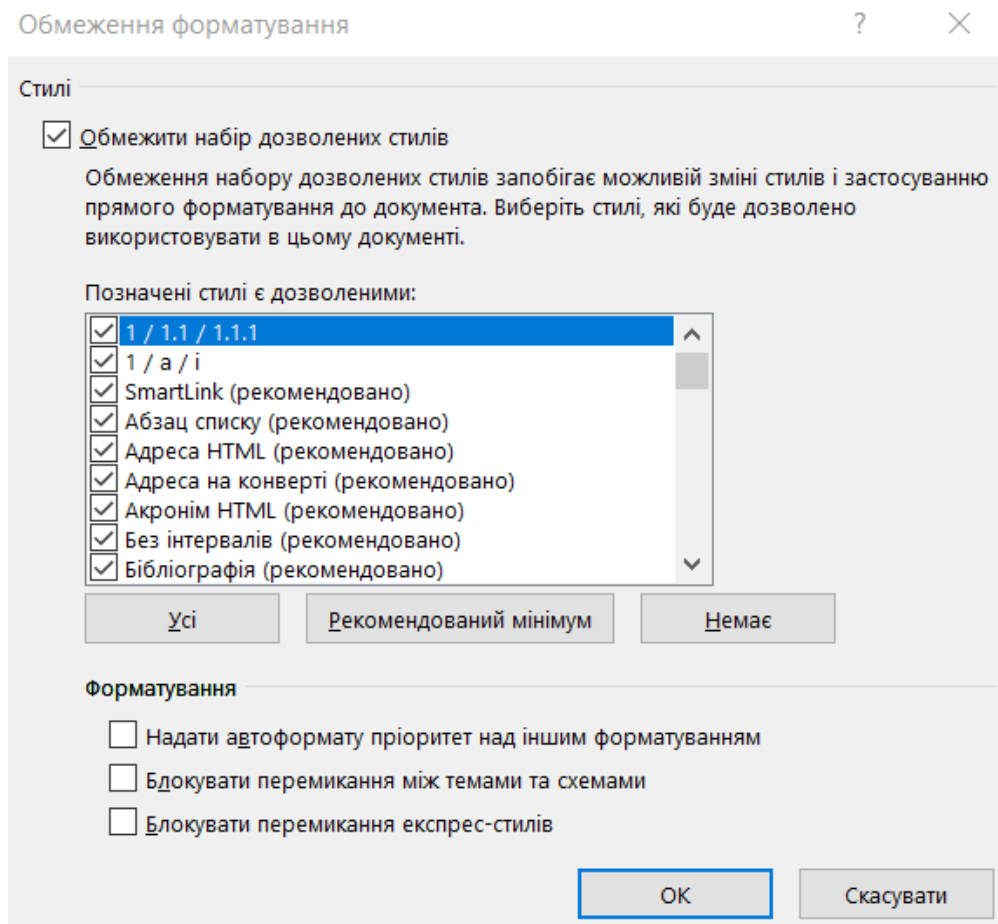


Рисунок 4

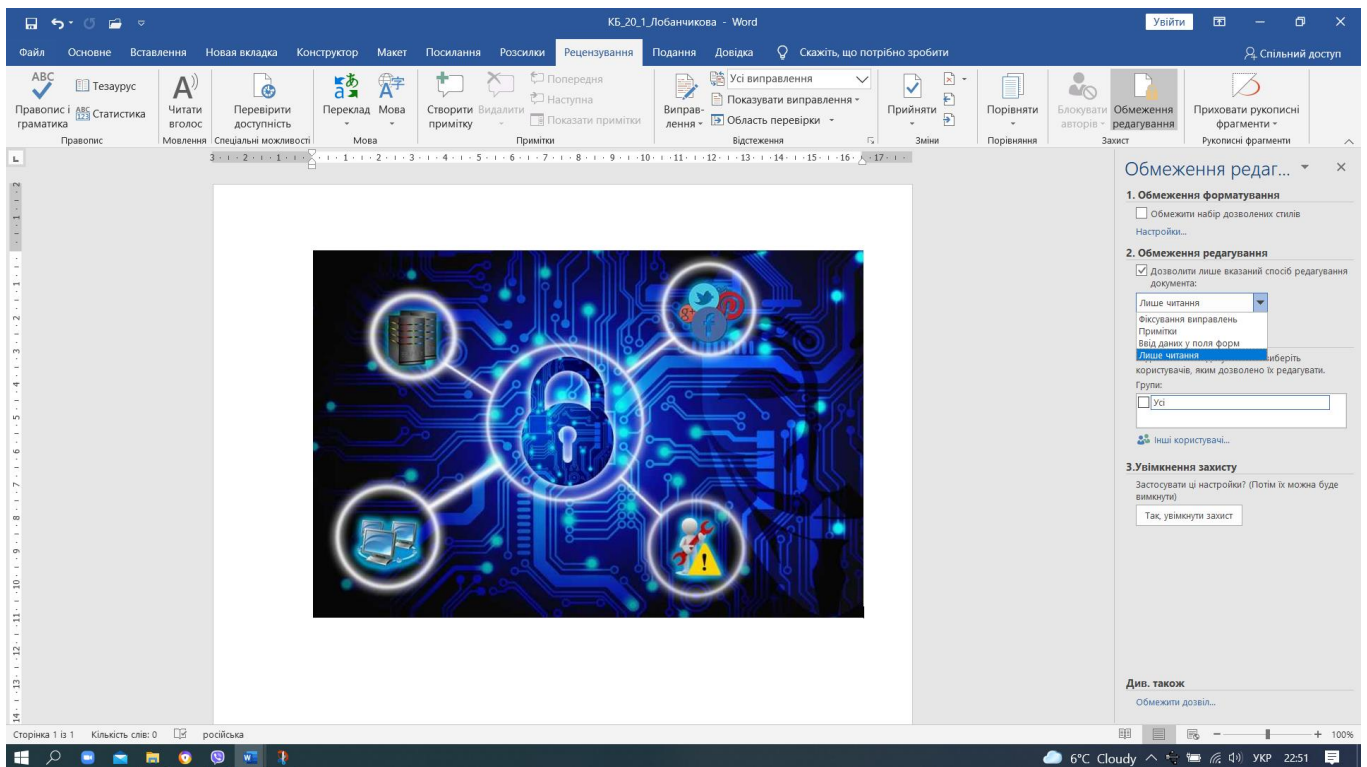


Рисунок 5

Завдання: дослідити процедуру «обмеження на форматування», рисунок 4, «обмеження на редагування», рисунок 5. Представити у звіті послідовність процедур та описати значення параметрів.

4. Встановлення паролю

Рецензування → Захист → 3. Увімкнення захисту → Так, увімкнути захист, рисунок 6.

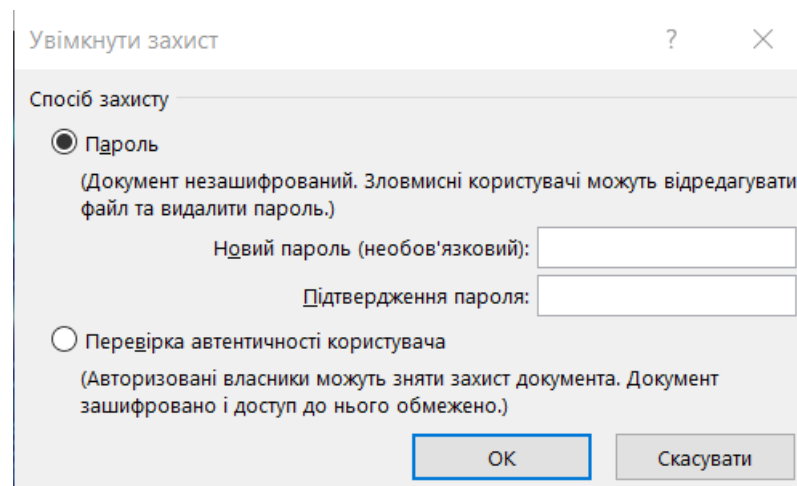


Рисунок 6

Другий варіант: Для того, щоб встановити пароль, необхідно виконати наступні дії (рисунок 6):

1. Вибрати команду *Файл* → *Зберегти як...* і у вікні, що відкрилося вибрати команду *Сервіс* → *Загальні параметри*, рис. 7.

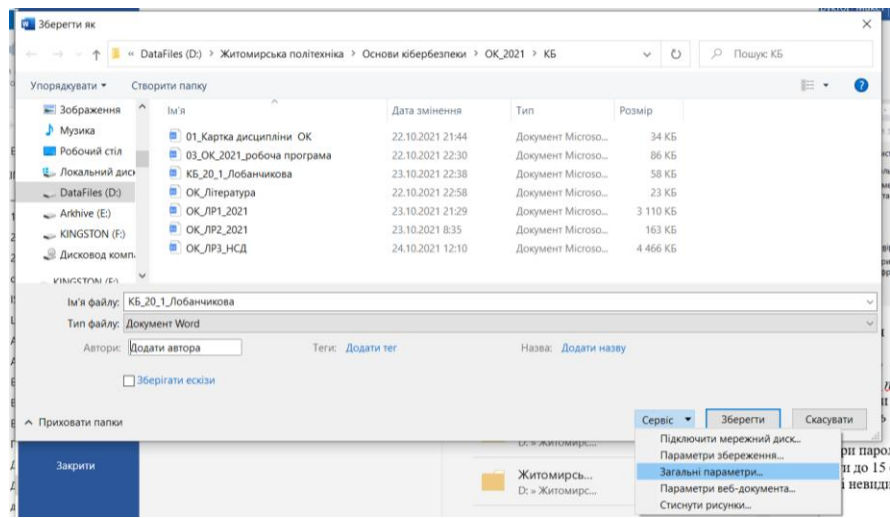


Рисунок 7

У нижній частині вкладки *Збереження* знаходяться поля введення: *Пароль для відкриття файлу*, *Пароль дозволу запису* і прапорець *Рекомендувати доступ тільки для читання*, рис. 8

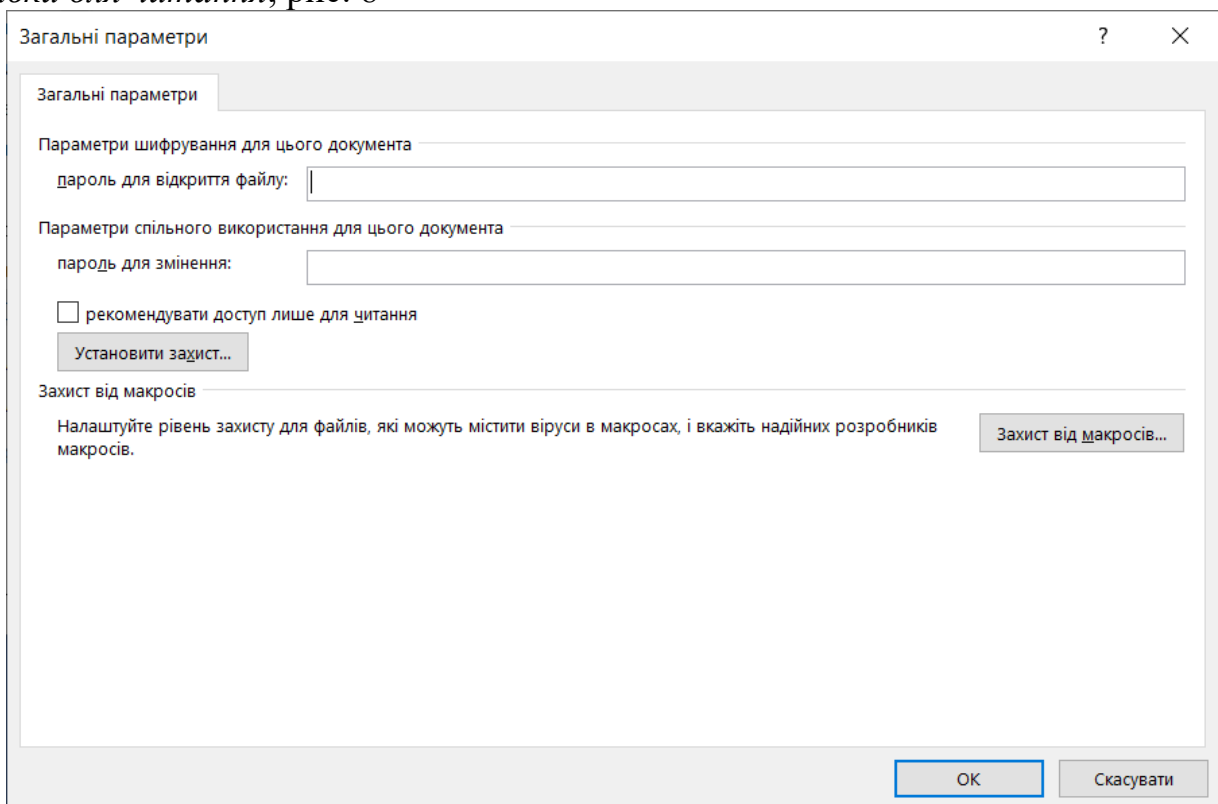


Рисунок 8

2. Ввести з клавіатури пароль.

Пароль може містити до 15 символів, включаючи букви, цифри, значки і пропуски. Пароль в цьому полі невидимий (головне, його запам'ятати).

3. Натиснути *ОК*. З'явиться вікно діалогу *Підтвердження пароля*.

4. Повторно ввести пароль і знову натиснути *ОК*.

5. Зберегти документ із внесеними змінами, натиснувши клавішу *Сохранить*.

Завдання: дослідити процедуру встановлення паролю на відкриття документів, процедуру встановлення паролю на дозвіл запису, параметри налаштування захисту конфіденційності інформації та захисту від макросів. Представити у звіті послідовність процедур та описати значення параметрів. Визначити поняття «макросу» та необхідності захисту від макросів.

5. Шифрування документів

У відкритому документі послідовно виберіть елементи *Файл* → *Відомості* → *Захист документа*, рисунок 9.

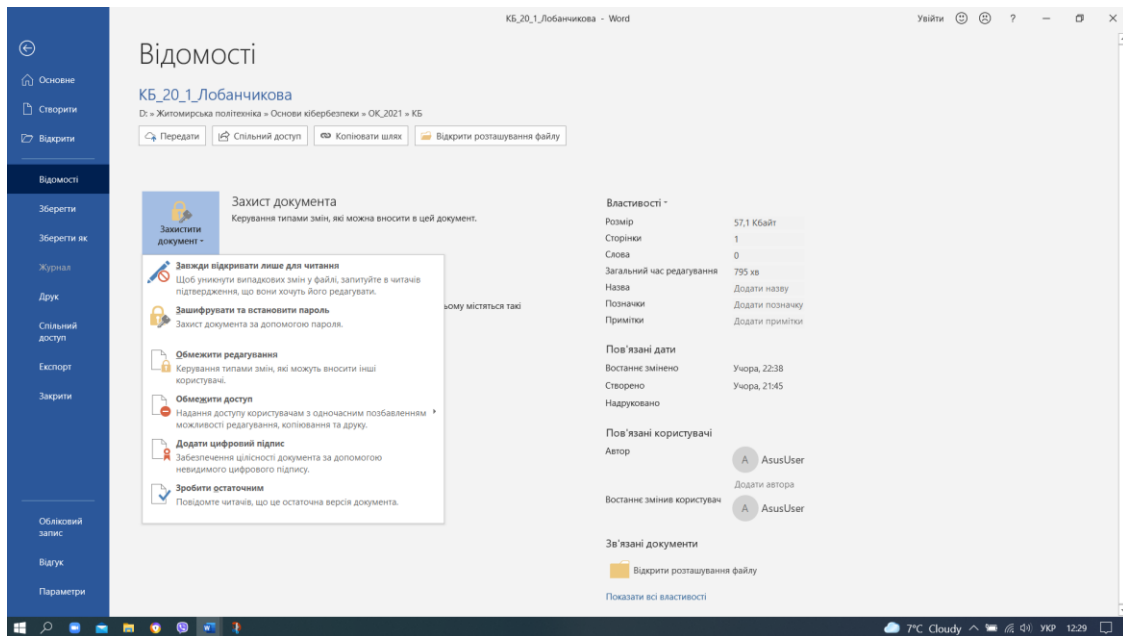


Рисунок 9

Відобразяться такі параметри:

Завжди відкривати лише для читання. Встановлення даного параметру дозволяє уникнути випадкових змін у файлі, шляхом запиту у читача підтвердження внесених змін.

Зашифрувати та встановити пароль. Відбувається процедура шифрування файлу із встановленням паролю. У разі вибору параметра *Шифрувати паролем* відображається діалогове вікно *Зашифрувати документ*. У полі *Пароль* введіть пароль. **Увага!** Корпорація Майкрософт не може відновити втрачені або забуті паролі, тому зберігайте список паролів і відповідних імен файлів у безпечному місці.

Обмежити редагування. Керування типами змін, які можна внести в документ. Якщо вибрати команду *Обмежити редагування*, відобразяться три параметри. *Обмеження форматування* Завдяки цьому обмежуються параметри форматування та зберігається зовнішній вигляд. Щоб вибрати, які стилі дозволено, виберіть елемент *Налаштування*. *Обмеження редагування.* Можна контролювати, як можна редагувати файл або вимкнути редагування. Щоб керувати тим, хто може редагувати, виберіть елемент *Винятки* або *Інші користувачі*.

Увімкнення захисту. Щоб вибрати захист паролем або автентифікація користувача, виберіть команду *Так, увімкнути захист*. Щоб додати або видалити редакторів з обмеженими дозволами, можна також вибрати команду *Обмежити дозвіл*. *Обмежити дозвіл за користувачем.* Використання ідентифікатора Windows Live ID для обмеження дозволів. Щоб обмежити дозволи, використовуйте ідентифікатор Windows Live ID або обліковий запис Microsoft Windows. Дозволи можна застосовувати через шаблон, який використовується в організації або можна додати дозволи вибравши команду

Обмежити доступ. Докладні відомості про керування правами доступу до інформації див. у статті [Керування правами доступу до інформації в системі Office](#).

Додати цифровий підпис. Додавання видимого або невидимого цифрового підпису. Цифрові підписи дають змогу автентифікувати цифрові відомості, зокрема документи, повідомлення електронної пошти й макроси, за допомогою комп'ютерної криптографії. Цифрові підписи створюються шляхом введення підпису або додавання зображення підпису, щоб установити автентичність, цілісність і неможливість зречення.

Зробити остаточною. Перетворення документа лише для читання з повідомлення читачів про те, що документ є остаточною. Коли документ позначається як остаточною, функція введення тексту, команди редагування та перевірки правопису вимикаються, а документ стає доступний лише для читання. За допомогою команди *Позначити як остаточною* можна повідомити, що надається доступ до остаточної версії документа. Вона також допомагає уникнути внесення випадкових змін у документ редакторами або читачами.

Завдання: дослідити процедуру «позначити як остаточною», «шифрування паролем», «обмежити редагування», «обмежити форматування», «обмеження редагування». Представити у звіті послідовність процедур та описати значення параметрів. Визначити поняття «цифровий підпис».

1.2. Методи та засоби накладання паролів на документи програми обробки електронних таблиць Microsoft Excel

Для захисту документів, створених засобами Microsoft Excel виконується наступна послідовність дій:

1. Запускаємо програму обробки електронних таблиць Microsoft Excel.
2. Створюємо будь-яку таблицю (може містити особисті надії, форми звітності, рейтинг студентів, тощо) та зберігаємо її під наступною назвою: **номер групи_Прізвище студента. Наприклад, КБ_20_1_Лобанчикова.**
3. Для того, щоб встановити пароль, необхідно виконати наступні дії (рисунок 8):

1. Вибрати команду *Файл* → *Зберегти як...* і у вікні, що відкрилося вибрати команду *Сервіс* → *Загальні параметри*.

У нижній частині вкладки *Збереження* знаходяться поля введення: *Пароль для відкриття файлу*, *Пароль для зміни* і прапорець *Рекомендувати доступ тільки для читання та Завжди створювати резервну копію*.

2. Ввести з клавіатури пароль, рис. 10.

Пароль може містити до 15 символів, включаючи букви, цифри, значки і пропуски. Пароль в цьому полі невидимий (головне, його запам'ятати).

3. Натиснути *ОК*. З'явиться вікно діалогу *Підтвердження пароля*.
4. Повторно ввести пароль і знову натиснути *ОК*.
5. Зберегти документ із внесеними змінами, натиснувши клавішу *Зберегти*.

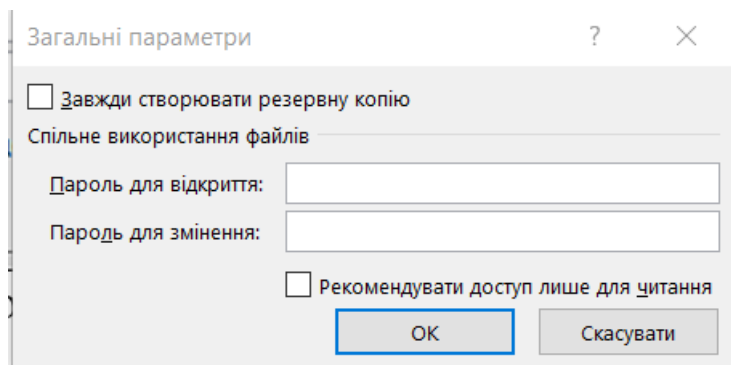


Рисунок 10

Завдання: дослідити процедуру встановлення паролю на відкриття документів, процедуру встановлення паролю на дозвіл запису. Представити у звіті послідовність процедур та описати значення параметрів.

4. Захист аркуша Excel

На відкритому аркуші послідовно виберіть елементи *Файл* → *Відомості* → *Захист книги*, рисунок 9.

Відобразяться такі параметри, рис. 11, що ідентичні до Word, однак є відмінності у застосуванні, зокрема захистити можна поточний аркуш або захистити структуру книги.

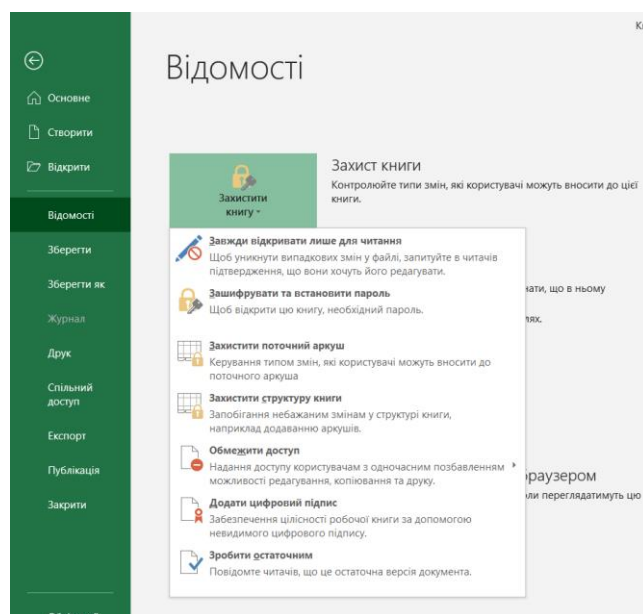


Рисунок 11

Завдання: Провести дослідження процедури кожного виду захисту, навести у звіті порядок виконання операції та представити результати роботи в вигляді скріншотів та коротких нотацій.

Завдання: Аналогічним чином провести дослідження методів та засобів захисту документів, створених за допомогою програми PowerPoint, Access. Представити скіншоти послідовності операцій та результатів ваших дій. Коротко описати процедури та параметри захисту документів у різних програмах.

1.3. Методи та засоби накладання паролів на відкриття архівних документів

Для дослідження процедури захисту архівних документів від відкриття при їх пересиланні засобами електронної пошти та Інтернет необхідно:

1. Вибрати будь-яких документ та запустити програму створення архівів, рисунок 12:

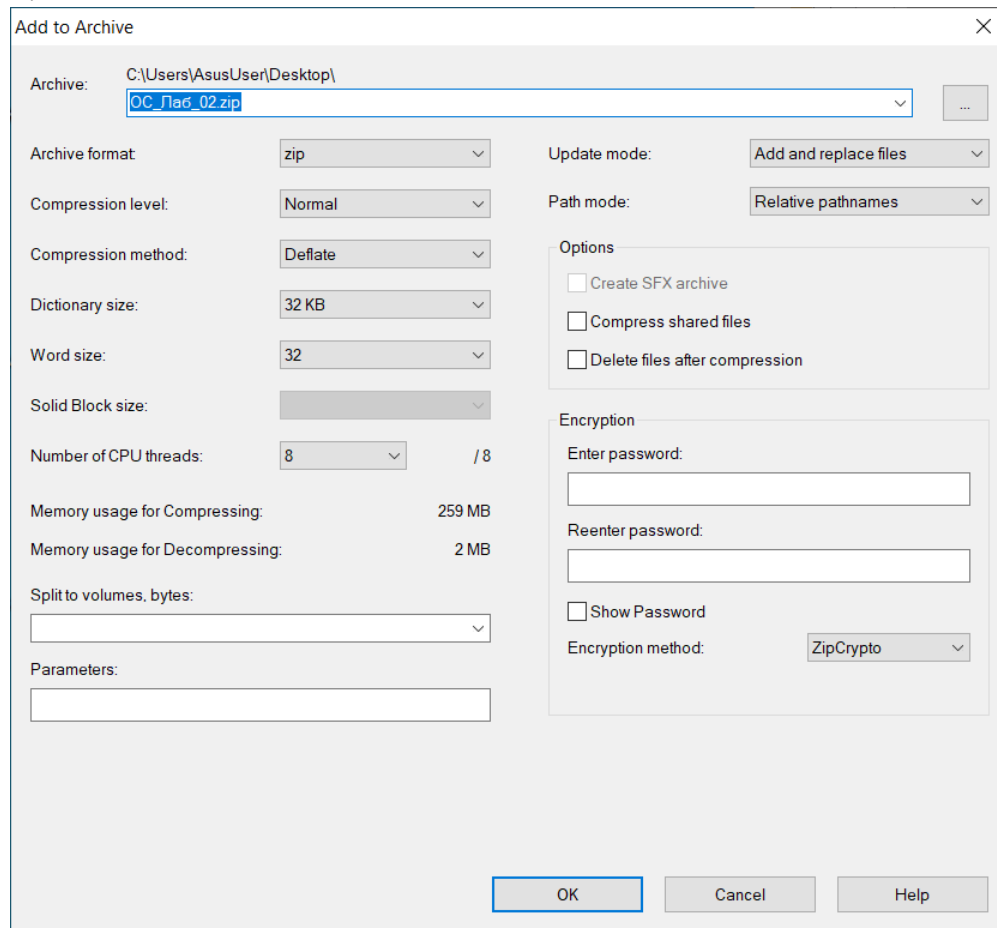


Рисунок 12

2. Далі, зазвичай вибирається метод стиснення даних, обмеження розміру (при необхідності). Праворуч міститься розділ вікна Encryption, де можна ввести пароль на шифрування, його підтвердження та вибрати метод шифрування: ZipCrypto або AES-256.

Завдання: вибрати будь-який доступний документ, запустити процедуру архівування, встановити пароль на відкриття документу та перевірити його дію. Навести скріншоти виконання операції.

Всі результати проведених досліджень представити викладачу у порядку їх виконання. Підготувати звіт з лабораторної роботи в установленому порядку. Всі результати проведених дій та операцій в звіті відобразити у вигляді скріншотів та нотацій.