# Рекомендації CERT-UA з налаштувань MS Office.

Існує багато ризиків при роботі з програмами MS Office, адже зловмисники або хакери, можуть використовувати не лише вразливості програмного забезпечення, а їх функціональні можливості. Убезпечити себе можна виконавши відповідні налаштувати в категорії **Центр безпеки та конфіденційності**.

Перелік основних елементів програм MS Office, що можуть бути використані зловмисниками або хакерами:

**Надійні розташування** – це розташування в файловій системі, що вважаються надійними джерелами для відкриття файлів. Так як дані розташування встановлюються за замовчуванням і є типовими, зловмисники можуть використовувати їх для реалізації атак.

**Надійні документи** – це файли з активним вмістом (макросами, елементами керування ActiveX, зв'язками даних тощо), які після ввімкнення в них активного вмісту відкриваються без відображення рядка повідомлень (запуск активного змісту проходить без попередження чи індикації). Під час відкриття надійного документа запит не відображається, навіть якщо до документа додано новий активний вміст або внесено зміни до наявного активного вмісту. Проте, якщо після визначення файлу як надійного його було переміщено, то під час відкриття такого файлу з'являється запит. Після визначення документа як надійного він більше не відкривається в безпечному поданні, тому слід довіряти документам лише тоді, коли ви довіряєте джерелу походження файлів.

**Надбудови** (бивш. «програми для Office») – це додаткові розширення чи програми, з якими додаються настроюванні команди та нові функції, що сприяє збільшенню продуктивності роботи із програмами MS Office. Водночас надбудови та веб-надбудови можуть використовуватись зловмисниками.

**Елементи керування ActiveX** – це невеликі стандартні блоки, з яких створюються програми, що працюють в Інтернеті через браузер. Зокрема, це настроюванні програми для збирання даних, перегляду певних типів файлів і відображення анімації. Елементи керування ActiveX зазвичай використовуються у кнопках, списках і діалогових вікнах. Програми Office також дають змогу використовувати елементи керування ActiveX для вдосконалення деяких документів. Елементи керування ActiveX можуть мати необмежений доступ до вашого комп'ютера, отримувати доступ до локальної файлової системи та змінювати параметри реєстру операційної системи. Таким чином, якщо зловмисник вирішить за допомогою елемента керування ActiveX керувати вашим комп'ютером, він може завдати значної шкоди.

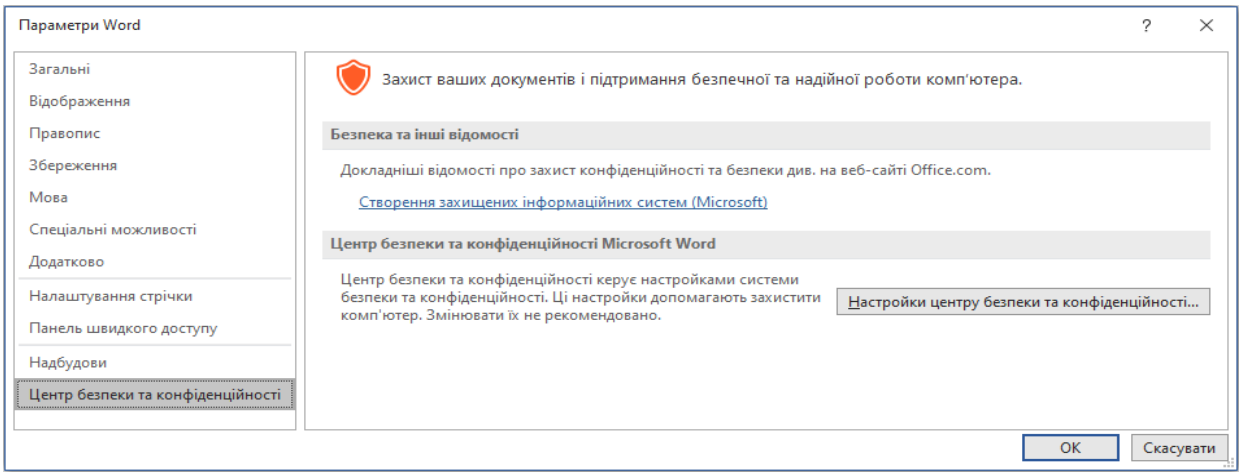
**Макрос** – це набір команд, який можна використовувати для автоматизації повторюваних завдань і запускати для їх виконання. Макроси автоматизують часто виконувані завдання для заощадження часу, який витрачається на натискання клавіш і дії мишею. Багато з них створені за допомогою Microsoft Visual Basic for Applications (VBA) і написані розробниками програмного забезпечення. Проте деякі макроси можуть бути потенційною загрозою для безпеки. Зловмисники або хакери, можуть ввести у файл шкідливі макроси, які можуть поширити вірус на комп'ютері або в мережі установи.

**Рекомендації щодо налаштувань:**

Для підвищення рівня безпеки рекомендуємо встановити відповідні налаштування в категорії **Центр безпеки та конфіденційності** програм MS Office:

Щоб потрапити до категорії **Центр безпеки та конфіденційності** необхідно:

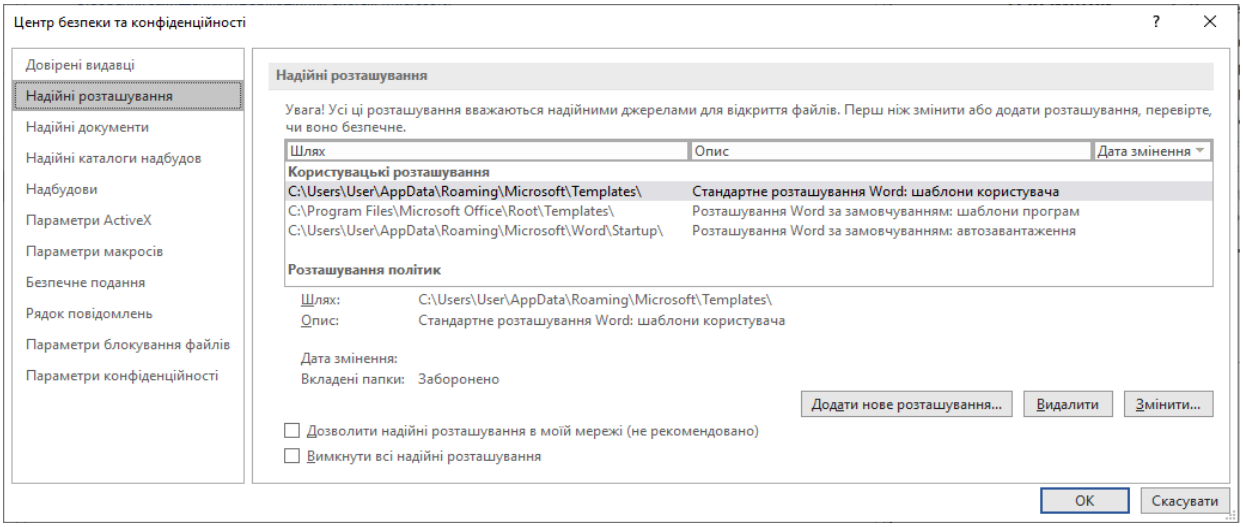
1. Перейти на вкладку **Файл** та вибрати пункт **Параметри**.
2. В **Параметрах** перейти до категорії **Центр безпеки та конфіденційності**.



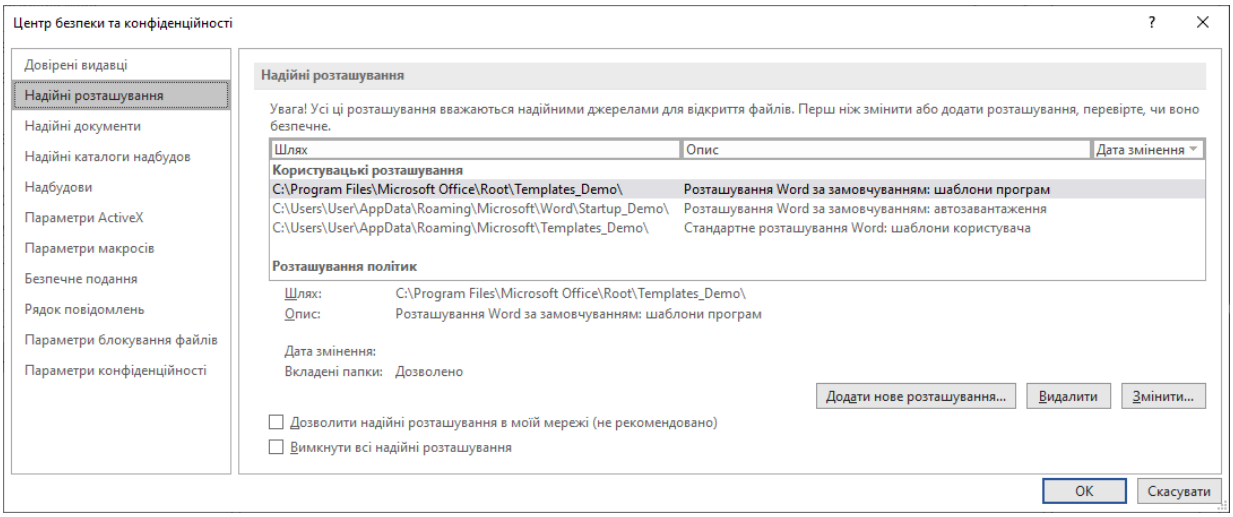

3. В категорії **Центр безпеки та конфіденційності** натиснути кнопку **Настойки центру безпеки та конфіденційності**.

Для встановлення запропонованих налаштувань в **Microsoft Word** необхідно:

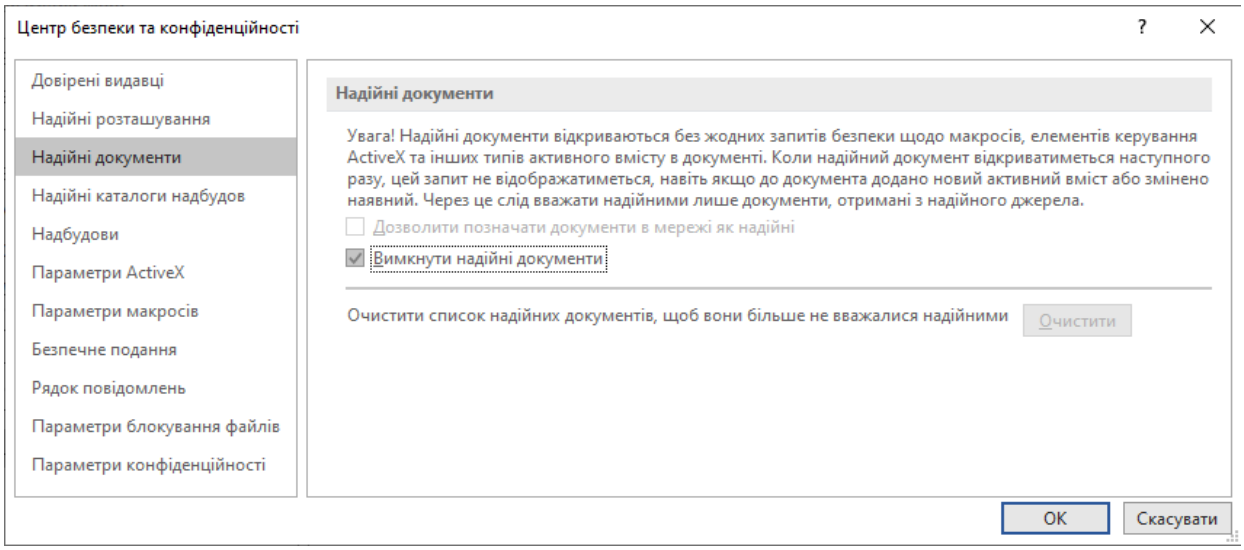
1. В **Центр безпеки та конфіденційності** виберіть пункт **Надійні розташування**.




2. Створіть **нові директорії**, що замінять типові та перевизначте **Надійні розташування**.



3. В **Центр безпеки та конфіденційності** виберіть пункт **Надійні документи**.
4. Натисніть кнопку **Очистити** та оберіть параметр **Вимкнути надійні документи**.




**Інформація для ознайомлення**

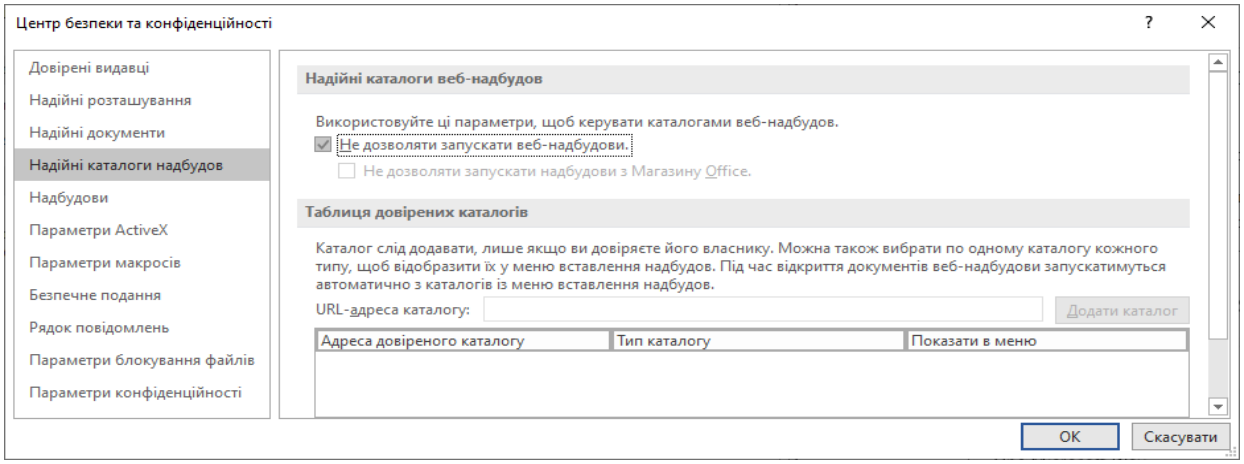
Докладніше про можливості налаштування надійних документів:

*Дозволити призначати документи в мережі як надійні*. Діалогове вікно Попередження системи безпеки більше не відображатиметься для файлів у мережевих розташуваннях.

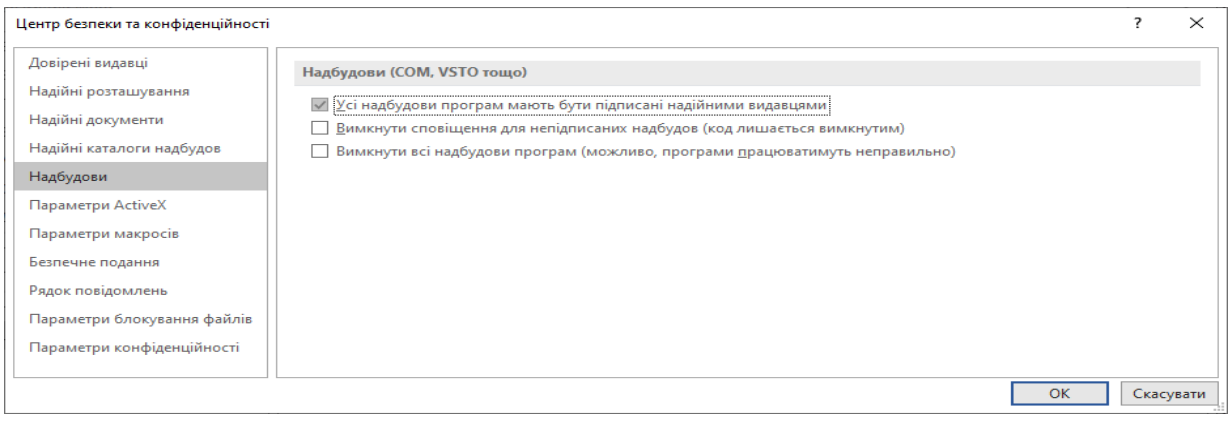
*Заборонити надійні документи.* Діалогове вікно Попередження системи безпеки відображатиметься кожного разу під час відкриття файлів.

*Скинути всі надійні документи, щоб вони більше не вважалися надійними*. Щоб видалити список надійних документів, яким ви довіряли раніше, натисніть кнопку Скинути. Для документів, яким ви довіряли раніше, знову відображатиметься рядок повідомлень.

5. В **Центр безпеки та конфіденційності** виберіть пункт **Надійні каталоги надбудов**.
   5.1. В разі, якщо веб-надбудови не використовуються встановіть прапорець **Не дозволяти запускати веб-надбудови**.




6. В **Центр безпеки та конфіденційності** виберіть пункт **Надбудови** та виберіть потрібні параметри.



**Інформація для ознайомлення**

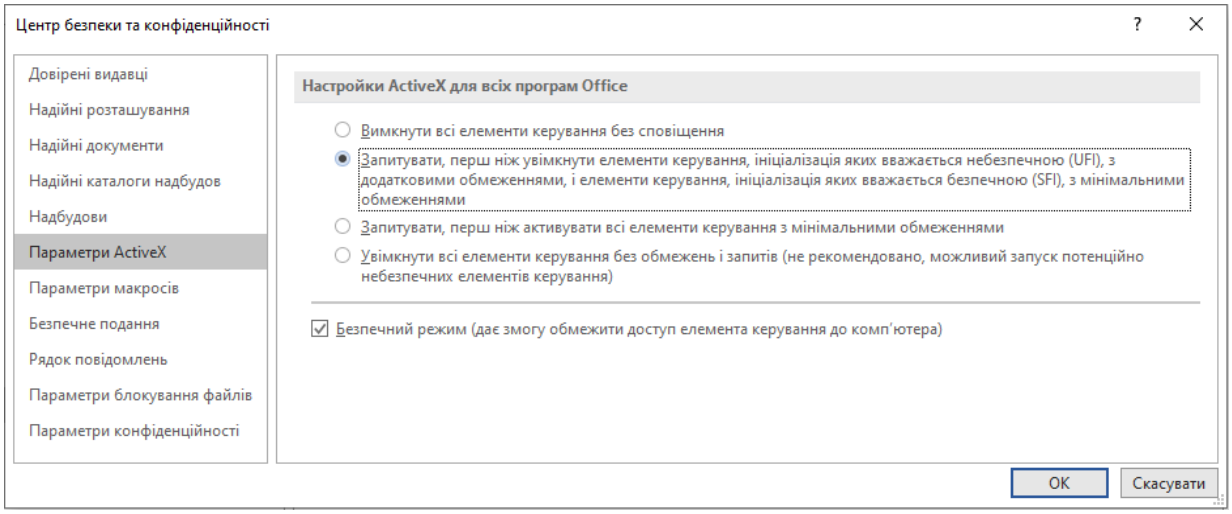
Докладніше про можливості налаштування надбудов:

*Усі надбудови програм мають бути підписані надійними видавцями*. Установіть цей прапорець, щоб Центр безпеки та конфіденційності перевіряв, чи надбудова використовує надійний підпис видавця. Якщо підпис видавця не надійний, офісна програма не завантажуватиме надбудову, а на Панелі безпеки відобразиться сповіщення про те, що надбудову вимкнуто.

*Вимкнути сповіщення для непідписаних надбудов* (*код лишається вимкнутим)*. Цей параметр активується, коли ви встановите прапорець Усі надбудови програм мають бути підписані надійними видавцями. Надбудови, підписані надійним видавцем, буде ввімкнуто, а непідписані – вимкнуто.

*Вимкнути всі надбудови програм* (*можливе порушення функціональних можливостей*). Установіть цей прапорець, якщо ви не довіряєте жодній надбудові. Усі надбудови буде вимкнуто без жодного сповіщення, а інші прапорці в розділі "Надбудови" стануть неактивні.

7. В **Центр безпеки та конфіденційності** виберіть пункт **Параметри ActiveX** та виберіть відповідні параметри.




**Інформація для ознайомлення**

Докладніше про налаштування ActiveX:

*Вимкнути всі елементи керування без сповіщення*. Усі елементи керування ActiveX у документах вимкнуто.

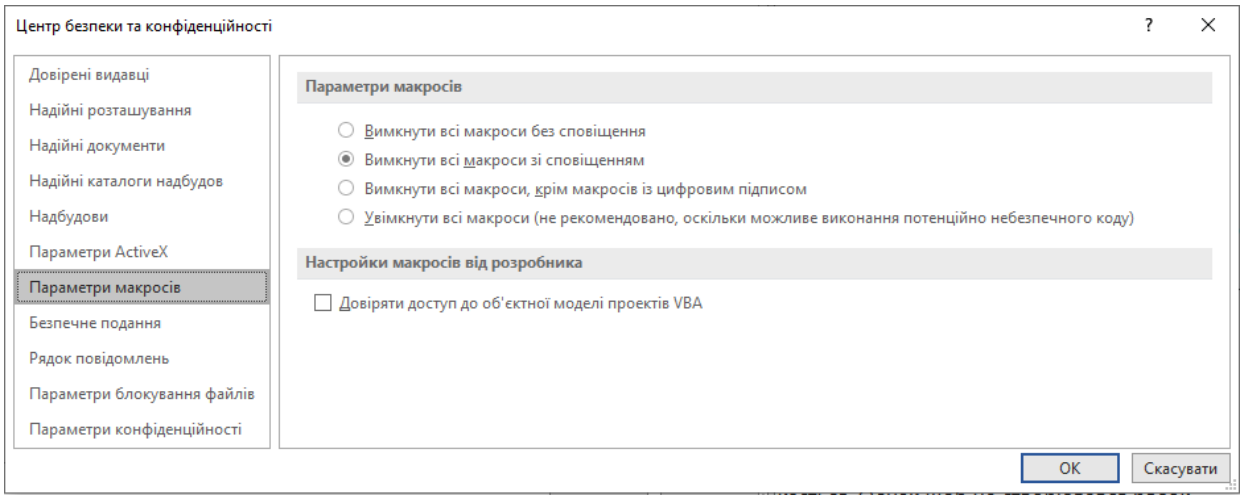
*Запит перед увімкненням елементів керування, ініціалізація яких вважається небезпечною* (*UFI*), *з додатковими обмеженнями та елементів керування, ініціалізація яких вважається безпечною* (*SFI*), *з мінімальними обмеженнями*. Існує два типи настройок на основі наявності проектів VBA:
*У разі наявності проекту VBA*. Усі елементи керування ActiveX вимкнуто й відображається рядок повідомлень. Натисніть кнопку Увімкнути вміст, щоб увімкнути елементи керування.
*У разі відсутності проекту VBA*. Елементи керування SFI ActiveX увімкнуто з мінімальними обмеженнями, а рядок повідомлень не відображається. Однак щоб не створювався рядок повідомлень, усі елементи керування ActiveX мають бути позначені як SFI. Елементи керування UFI ActiveX вимкнуто. Проте коли користувач увімкне елементи керування UFI, вони ініціалізуються з додатковими обмеженнями (наприклад, значеннями за промовчанням). Усі набуті дані, які є частиною елемента керування UFI, буде втрачено.

*Запит перед увімкненням усіх елементів керування з мінімальними обмеженнями*. Це значення встановлено за промовчанням. Існує два типи настройок на основі наявності проектів VBA:
*У разі наявності проекту VBA*. Усі елементи керування ActiveX вимкнуто й відображається рядок повідомлень. Натисніть кнопку Увімкнути вміст, щоб увімкнути елементи керування.
*У разі відсутності проекту VBA*. Елементи керування SFI ActiveX увімкнуто з мінімальними обмеженнями, а рядок повідомлень не відображається. Однак, щоб не створювати рядок повідомлень, усі елементи керування ActiveX мають бути позначені як "SFI". Елементи керування UFI ActiveX вимкнуто. Проте, коли користувач увімкне елементи керування UFI, вони ініціалізуються з мінімальними обмеженнями (наприклад, зі збереженими значеннями або значеннями за промовчанням, якщо збережені дані не наявні).

*Увімкнути всі елементи керування без обмежень і запитів* (*не рекомендовано*). Вмикає всі елементи керування ActiveX у документах із мінімальними обмеженнями.

*Безпечний режим*. Вмикає елементи керування SFI ActiveX у безпечному режимі, що означає, що розробник позначив елемент керування як безпечний.

8. В **Центр безпеки та конфіденційності** виберіть пункт **Параметри макросів** та виберіть відповідні параметри.




**Інформація для ознайомлення**

Докладніше про налаштування макросів:

*Вимкнути всі макроси без сповіщення*. Макроси й оповіщення від системи безпеки про макроси вимикаються.

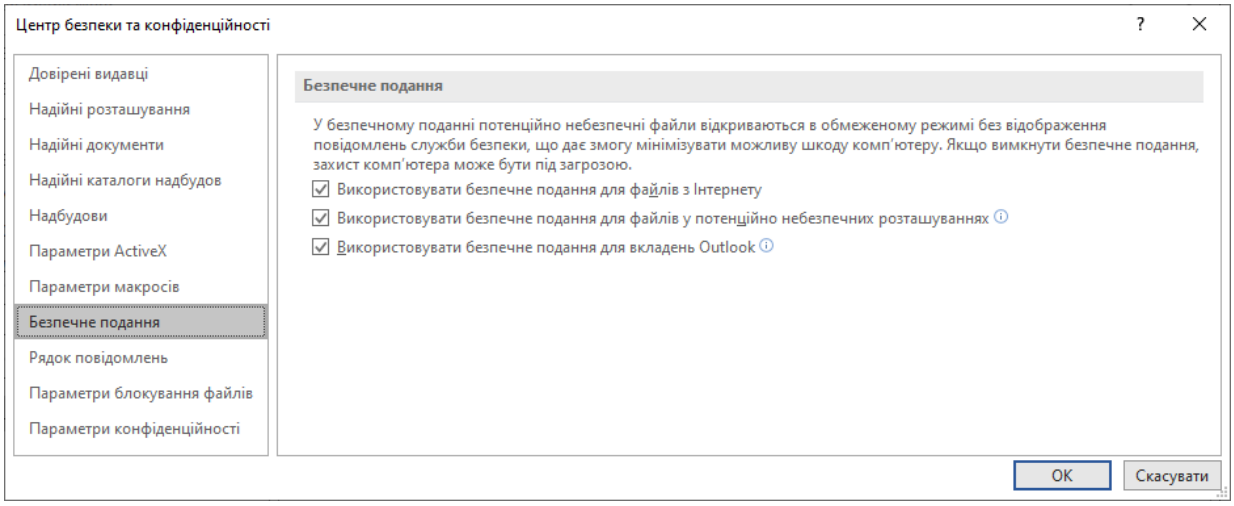
*Вимкнути всі макроси зі сповіщенням*. Макроси вимкнуто, але за наявності макросів сповіщення системи безпеки будуть відображатися. Існує можливість ввімкнути окремий макрос в файлі.

*Вимкнути всі макроси, крім макросів із цифровим підписом*. Макроси вимкнуто, але за наявності макросів сповіщення системи безпеки будуть відображатися. Проте якщо макрос підписано надійним видавцем, макрос запускатиметься за умови, що користувач довіряє цьому видавцю. Якщо видавець не надійний, відображається сповіщення про ввімкнення вмісту або довіру видавцеві.

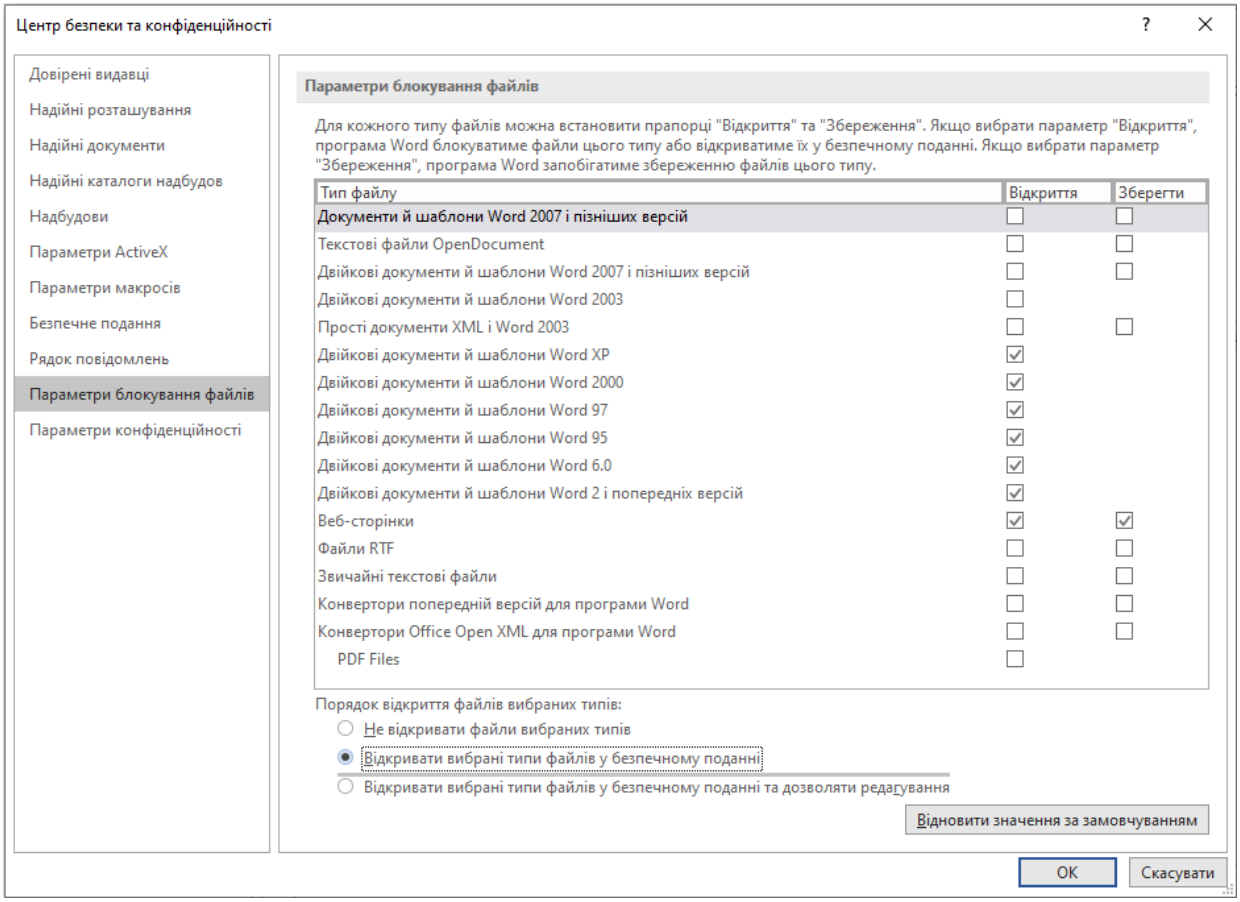
*Увімкнути всі макроси* (*не рекомендовано, потенційно небезпечний код може виконуватися*). Усі макроси будуть працювати. Цей параметр робить комп'ютер вразливим для потенційно небезпечного коду.

*Довіряти доступ до об'єктної моделі проектів VBA*. Заборонити або дозволити програмний доступ до об'єктної моделі Visual Basic для застосунків (VBA) із клієнта автоматизації. Цей параметр безпеки призначений для автоматизації програми Office і маніпулювання середовищем VBA та об'єктної моделі. Цей параметр для кожного користувача та для кожного окремого застосунку, і заперечує доступ за замовчуванням, перешкоджає несанкціонованому програмам створювати шкідливі самореплікації коду. Щоб клієнти автоматизації могли отримати доступ до об'єктної моделі VBA, користувач, який працює в коді, має надати доступ. Щоб дозволити доступ клієнтам, установіть цей прапорець.

9. В **Центр безпеки та конфіденційності** виберіть пункт **Безпечне подання** та виберіть усі можливі параметри.



10. В **Центр безпеки та конфіденційності** виберіть пункт **Параметри блокування файлів** та виберіть відповідні параметри.




**Для іншої продукції MS Office налаштування відбуваються аналогічно.**

**Також наголошуємо, що слід використовувати лише ліцензійне програмне забезпечення з офіційних ресурсів та регулярно його оновлювати.**