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 відповіднні 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.

Параметри Word		?	\times
Загальні	问 Захист ваших документів і підтримання безпечної та надійної роботи комп'ютера.		
Відображення			
Правопис	Безпека та інші відомості		
Збереження	Докладніші відомості про захист конфіденційності та безпеки див. на веб-сайті Office.com.		
Мова	Створення захищених інформаційних систем (Microsoft)		
Спеціальні можливості	Центо безпеки та конфіденційності Microsoft Word		
Додатково			
Налаштування стрічки	безпеки та конфіденційності. Ці настройки допомагають захистити <u>Н</u> астройки центру безпеки та конфіден	ційност	ri
Панель швидкого доступу	комп ютер. Змінювати іх не рекомендовано.		
Надбудови			
Центр безпеки та конфіденційності			
	OK	Скасу	/вати

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.

Центр безпеки та конфіденційності		1	? ×
Довірені видавці	Надійні розташування		
Надійні розташування	Увага! Усі ці розташування вважаються надійними джерелами для відкриття файлів. Перш ніж змінити або дода	ти розташування, п	еревірте,
Надійні документи	чи воно безпечне.		
Надійні каталоги надбудов	Шлях Опис	Дата змін	нення 🔻
	Користувацькі розташування		
Надбудови	C:\Users\User\AppData\Roaming\Microsoft\Templates\ Стандартне розташування Word: шаблони користу	/вача	
Параметри ActiveX	C:\Program Files\Microsoft Office\Root\Templates\ C:\Users\User\AppData\Roaminq\Microsoft\Word\Startup\ Pозташування Word за замовчуванням: автозавант	програм гаження	
Параметри макросів			
Безпечне подання	Розташування політик		
	<u>Ш</u> лях: C:\Users\User\AppData\Roaming\Microsoft\Templates\		
Рядок повідомлень	<u>О</u> пис: Стандартне розташування Word: шаблони користувача		
Параметри блокування файлів	Дата змінення:		
Параметри конфіденційності	Вкладені папки: Заборонено		
	До <u>да</u> ти нове розташування	<u>В</u> идалити <u>З</u> м	інити
	🗌 Дозволити надійні розташування в моїй мережі (не рекомендовано)		
	<u>В</u> имкнути всі надійні розташування		
		OK	Скасувати

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

Центр безпеки та конфіденційності		? ×
Довірені видавці	Налійні розташування	
Надійні розташування	увага! Усі ці розташування вважаються надійними джерелами для відкриття файлів. Перш ніж змінити або д	одати розташування, перевірте, чи воно
Надійні документи	безпечне.	
Надійні каталоги надбудов	Шлях Опис	Дата змінення 👻
Наябулови	Користувацькі розташування	
падоудови	C:\Program Files\Wicrosoft Office\Root\Templates_Demo\ PostauyBahha Word sa saMoB4yBahham: ua	олони програм
Параметри ActiveX	C:\Users\User\AppData\Koaming\Microsoft\Word\Startup_Demo\ Розташування Word за замовчуванням: авт C:\Users\User\AppData\Roaming\Microsoft\Templates Demo\ Стандартне розташування Word: шаблони	озавантаження користувача
Параметри макросів		
Eastering Desaying	Розташування політик	
везпечне подання	Шлях: C:\Program Files\Microsoft Office\Root\Templates Demo\	
Рядок повідомлень	Опис: Розташування Word за замовчуванням: шаблони програм	
Параметри блокування файлів	Лата зміненно	
Параметри конфіденційності	Вкладені папки: Дозволено	
	Додати нове розташ	ування Видалити <u>З</u> мінити
	🗌 Дозволити надійні розташування в моїй мережі (не рекомендовано)	
	<u>В</u> имкнути всі надійні розташування	
		ОК Скасувати

3. В Центр безпеки та конфіденційності виберіть пункт Надійні документи.

4. Натисніть кнопку Очистити та оберіть параметр Вимкнути надійні документи.

Центр безпеки та конфіденційності		?	×
Довірені видавці	Надійні документи		
Надійні розташування	Уваса! Навійні заминици візкондароть са без жодних заритів безреки шодо макросів, еденентів		
Надійні документи	Эвага: надини документи відкриваються ов жодних запить безпеки щодо макрось, елементь Астічех та інших типета активного вмісту ве документі. Коли надійний документ відкриватиметься	наступ	ного
Надійні каталоги надбудов	разу, цей запит не відображатиметася, навта якщо до документа додано новий активний вміст а наявний. Через це слід вважати надійними лише документи, отримані з надійного джерела.	100 SMIR	ieno
Надбудови	Дозволити позначати документи в мережі як надійні		
Параметри ActiveX	Вимкнути надійні документи		
Параметри макросів	Очистити список надійних документів, щоб вони більше не вважалися надійними Очистити		
Безпечне подання			
Рядок повідомлень			
Параметри блокування файлів			
Параметри конфіденційності			
L	ОК	Скас	увати

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.

Центр безпеки та конфіденційності		?	×
Довірені видавці	Надійні каталоги веб-надбудов		^
Надійні розташування	Використовуйте ці параметри, щоб керувати каталогами веб-налбулов.		
Надійні документи	✓ Не дозволяти запускати веб-надбудови.		
Надійні каталоги надбудов	🗌 Не дозволяти запускати надбудови з Магазину <u>O</u> ffice.		
Надбудови	Tafanung napinguny yatanarip		
Параметри ActiveX	таолиця довретия каталотъ		11
Параметри макросів	Каталог слід додавати, лише якщо ви довіряєте його власнику. Можна також вибрати по одному каталогу кож типу, щоб відобразити їх у меню вставлення надбудов. Під час відкриття документів веб-надбудови запускатик автоматично з каталогів із менно вставлення надбудов.	иуться	
Безпечне подання	URL-адреса каталогу: Додати	каталог	11
Рядок повідомлень	Адреса довіреного каталогу Тип каталогу Показати в меню		j 🗆
Параметри блокування файлів			
Параметри конфіденційності			•
	ОК	Скасу	вати

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

Центр безпеки та конфіденційності			?	\times
Довірені видавці Надійні розташування Надійні документи	Надбудови (СОМ, VSTO тощо) Усі надбудови програм мають бути підписані надійними видавцями Вимкнути сповіщення для непідписаних надбудов (код лишається вимкнутим)			
Надбудови	Вимкнути всі надбудови програм (можливо, програми працюватимуть неправильно)			
Параметри ActiveX				
Параметри макросів				
Безпечне подання				
Рядок повідомлень				
Параметри блокування файлів				
Параметри конфіденційності				
		ОК	Ска	сувати

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.

Центр безпеки та конфіденційності		?	×
Довірені видавці	Настройки ActiveX для всіх програм Office		
Надійні розташування Надійні документи Надійні каталоги надбудов Надбудови Параметри ActiveX	 Вимкнути всі елементи керування без сповіщення Запитувати, перш ніж увімкнути елементи керування, ініціалізація яких вважається небезпечною (UFI), з додатковими обмеженнями, і елементи керування, ініціалізація яких вважається безпечною (SFI), з мініма обмеженнями Запитувати, перш ніж активувати всі елементи керування з мінімальними обмеженнями Увімкнути всі елементи керування без обмежень і запитів (не рекомендовано, можливий запуск потенцій небезпечних елементів керування) 	альним	ли
Параметри макросів Безпечне подання Рядок повідомлень Параметри блокування файлів	✓ Безпечний режим (дає змогу обмежити доступ елемента керування до комп'ютера)		
Параметри конфіденційності	ОК	Скасу	/вати

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.

Центр безпеки та конфіденційності		?	×
Довірені видавці	Параметри макросів		
Надійні розташування			
Надійні документи	 <u>В</u>имкнути всі макроси без сповіщення Вимкнути всі макроси зі сповіщенням 		
Надійні каталоги надбудов	 Вимкнути всі макроси, крім макросів із цифровим підписом 		
Надбудови	🔘 Увімкнути всі макроси (не рекомендовано, оскільки можливе виконання потенційно небезпечного коду)		
Параметри ActiveX	Настройки макросів від розробника		
Параметри макросів	П Довіряти доступ до об'єктної моделі проектів VBA		
Безпечне подання			
Рядок повідомлень			
Параметри блокування файлів			
Параметри конфіденційності			
	ОК	Скасу	вати

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.

Центр безпеки та конфіденційності		?	\times
Довірені видавці	Безпечне подання		
Надійні розташування Надійні документи	У безпечному поданні потенційно небезпечні файли відкриваються в обмеженому режимі без відображення повідомлень служби безпеки, що дає змогу мінімізувати можливу шкоду комп'ютеру. Якщо вимкнути безпечни захист комп'ютера може бути під загрозою.	е подан	іня,
Надійні каталоги надбудов	☑ Використовувати безпечне подання для файлів з Інтернету		
Надбудови	✓ Використовувати безпечне подання для файлів у потенційно небезпечних розташуваннях ⁽¹⁾ ✓ Використовувати безпечне подання для вкладень Outlook ⁽¹⁾		
Параметри макросів			
Безпечне подання			
Рядок повідомлень			
Параметри блокування файлів			
Параметри конфіденційності			
	ОК	Скасу	вати

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

нтр безпеки та конфіденційності			?
Іовірені видавці	Параметри блокування файлів		
łадійні розташування łадійні документи	Для кожного типу файлів можна встановити прапорці "Відкриття" та "Збереження". Як програма Word блокуватиме файли цього типу або відкриватиме їх у безпечному под "Збереження", програма Word запобігатиме збереженню файлів цього типу.	що вибрати параме анні. Якщо вибрати	тр "Відкриття параметр
Тадійні каталоги надбудов	Тип файлу	Відкриття	Зберегти
Тадбудови	Документи й шаблони Word 2007 і пізніших версій		
араметри ActiveX	Текстові файли OpenDocument		
	Двійкові документи й шаблони Word 2007 і пізніших версій		
араметри макросів	Двійкові документи й шаблони Word 2003		
зпечне подання	Прості документи XML і Word 2003		
док повідомлень	Двійкові документи й шаблони Word XP	\checkmark	
	Двійкові документи й шаблони Word 2000	\checkmark	
раметри олокування фаилів	Двійкові документи й шаблони Word 97	\checkmark	
раметри конфіденційності	Двійкові документи й шаблони Word 95	\checkmark	
	Двійкові документи й шаблони Word 6.0	\checkmark	
	Двійкові документи й шаблони Word 2 і попередніх версій	\checkmark	
	Веб-сторінки	\checkmark	\checkmark
	Файли RTF		
	Звичайні текстові файли		
	Конвертори попередній версій для програми Word		
	Конвертори Office Open XML для програми Word		
	PDF Files		
	Порядок відкриття файлів вибраних типів:		
	 пе ыдкривати фаили виораних типів Па по по		
	 Відкривати вибрані типи файлів у безпечному поданні 		
	 Бідкривати вибрані типи файлів у безпечному поданні та дозволяти редагування 	1	
	<u>B</u> iAH	ювити значення за з	амовчування
		OK	Cracy

Для іншої продукції MS Office налаштування відбуваються аналогічно.

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