

## Тема. Антивірусні та антишпигунські програми

### Очікувані результати заняття

Після цього заняття потрібно вміти:

- пояснювати принцип дії антивірусних програм певного типу;
- налаштовувати параметри антивірусної програми.

### Поміркуйте

- Що таке комп'ютерний вірус?
- Які види вірусів ви знаєте?
- Як можна заразити комп'ютер вірусом?
- Які профілактичні заходи можна вжити для захисту від вірусів?

### Ознайомтеся з інформацією

**Антивірус** - це програма, яка виявляє й знешкоджує комп'ютерні віруси. Антивірусні програми можуть виявляти та знищувати лише відомі віруси, при появі нового комп'ютерного вірусу захисту від нього не існує до тих пір, поки для нього не буде розроблено свій антивірус. Однак, багато сучасних антивірусних пакетів мають у своєму складі спеціальний програмний модуль, який називається евристичний аналізатор, і який здатний досліджувати вміст файлів на наявність коду, характерного для комп'ютерних вірусів. Це дає змогу вчасно виявляти та попереджати про небезпеку зараження новим вірусом.

Розрізняють такі **типи антивірусних програм**:

1. **програми-детектори**: призначені для знаходження заражених файлів одним із відомих вірусів. Деякі програми-детектори можуть також лікувати файли від вірусів або знищувати заражені файли. Існують спеціалізовані (тобто призначені для боротьби з одним вірусом) детектори та поліфаги (можуть боротися з багатьма вірусами);
2. **програми-лікарі**: призначені для лікування заражених дисків і програм. Лікування програми полягає у вилученні із зараженої програми тіла вірусу. Також можуть бути як поліфагами, так і спеціалізованими;
3. **програми-ревізори**: призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам'ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп'ютера. В разі невідповідності даних виводиться повідомлення про можливість зараження;
4. **лікарі-ревізори**: призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан.
5. **програми-фільтри**: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження і повідомляють про це користувача. Останній має можливість дозволити або заборонити виконання відповідної операції. Такі програми є резидентними, тобто вони знаходяться в оперативній пам'яті комп'ютера.
6. **програми-вакцини**: використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше).

### Антивірусні програми

- Avira
- Dr.Web
- Kaspersky
- McAfee
- NOD32

- Panda Software
- Symantec CША
- Український Національний Антивірус
- ZoneAlarm AntiVirus

## Методи профілактики зараження комп'ютерними вірусами

Усі існуючі заходи боротьби з комп'ютерними вірусами можна поділити на дві категорії:

- профілактичні заходи, спрямовані на резервне збереження даних та недопущення зараження вірусами через піратське програмне забезпечення;
- заходи щодо знищення комп'ютерних вірусів та лікування заражених програм і даних.

Для профілактики зараження комп'ютера вірусами слід дотримуватись певних правил:

- регулярно оновлювати програми антивірусного захисту;
- систематично перевіряти комп'ютер на наявність вірусів;
- користуватися лише ліцензійним програмним забезпеченням;
- не використовувати для роботи підозрілі й чужі файли, зовнішні носії тощо без попередньої перевірки антивірусними програмами;
- не відкривати приєднані до електронної пошти файли без попередньої їхньої перевірки на наявність вірусів;
- систематично здійснювати резервне копіювання даних на незалежні носії;
- не завантажувати з Інтернету файли з розширенням exe з неперевічених сайтів;
- обмежити коло користувачів вашого комп'ютера, вимагати неухильного дотримання правил антивірусного захисту;
- при використанні ОС Windows працювати під обліковим записом без прав адміністратора.

Основні параметри, які варто враховувати при налаштуванні антивірусного програмного забезпечення:

| Параметр                       | Опис   |
|--------------------------------|--|
| Регулярні оновлення            | Впевніться, що ваша антивірусна програма має актуальну базу даних про віруси. Налаштуйте автоматичні оновлення, щоб ваша програма завжди була оновлена.  |
| Сканування в реальному часі    | Активуйте функцію сканування в реальному часі, щоб антивірусна програма автоматично перевіряла всі файли та програми, які ви використовуєте. Це допоможе виявити і заблокувати потенційно небезпечні файли до того, як вони навмисно або випадково запустяться на вашому комп'ютері. |
| Розклад сканування             | Налаштуйте регулярний розклад сканування вашого комп'ютера. Це дозволить антивірусній програмі автоматично перевіряти всі файли та папки на наявність вірусів за заданим графіком.   |
| Налаштування електронної пошти | Перевірте параметри антивірусної програми для електронної пошти. Деякі віруси можуть поширюватися через електронну пошту, тому важливо встановити фільтри для виявлення та блокування небезпечних вкладень або посилань.   |
| Парольний захист               | Встановіть пароль для антивірусної програми, щоб запобігти несанкціонованому доступу до її налаштувань або вимкненню захисту.  |

## Дізнайтеся більше

- <https://zillya.ua/zillya-total-security-maksimalnii-zakhist-koristuvachiv>
- <https://mediacom.com.ua/prosta-bezpeka-yak-nalashtuvati-parametri-vashoi-antivirusnoi-programi/>
- [wizcase.com](http://wizcase.com)

## Виконайте вправу

<https://wordwall.net/resource/53305425>

## Завдання

Пройдіть тестування <https://vseosvita.ua/test/start/aqj411>

## Джерела

- [Мій клас](#)
- [wizcase.com](http://wizcase.com)
- [mediacom](http://mediacom)