Комп’ютерні віруси

Інформатика
9клас

Комп'ютерний вірус – це спеціально створена програма для виконання несанкціонованих деструктивних дій на ураженому комп'ютері

Комп'ютерний вірус – це програма, що активізується під час виконання іншої, зараженої нею програми. Після активації вірус самовідтворюється, вражаючи програми на жорсткому диску та на інших носіях

Середовище розповсюдження вірусу

Деструктивні можливості вірусів

Ознаки того, що комп'ютер уражено вірусом:

Троянські коні та хробаки

Окрім комп'ютерних вірусів є ще одна категорія шкідливих програм, які дають змогу зловмисникам збирати інформацію, модифікувати та пошкоджувати її, а також порушувати роботу комп'ютера чи використовувати його ресурси зі зловмисною метою.

Троянський кінь – шкідлива програма (не вірус), що може збирати інформацію, модифікувати та пошкоджувати її, порушувати роботу комп'ютера чи використовувати його ресурси у зловмисних цілях.

Із розвитком мереж з'явилася ще одна категорія шкідливих програм – мережні хробаки. Вони здатні до самовідтворення, але не оселяються в інших програмах.

Мережні хробаки – шкідливі програми, які потрапляють до комп'ютера через мережу, можуть спричинити втрату програм і даних, а також крадення персональних даних користувача.

Способи зараження

- вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення операційної системи до об'єктів зараження і упроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до виключення або перезавантаження комп

Резидентний

- віруси не заражають пам'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус. Такі віруси вважаються нерезидентними

Нерезидентний

- Це віруси, які розмножуються копіюванням себе в службові ділянки гнучких і жорстких магнітних дисків, оптичних дисків та інших зміних носіїв.Копіювання відбувається під час спроби користувача задати дані з ураженого носія.

Дискові віруси

- серед вірусів виділяють ті, що використовують спеціальні способи маскування

Поліморфні (мутанти)

- це віруси, основним завданням яких є виконання несанкціонованих власником комп'ютера дій: збирання і надсилання потрібних зловмиснику даних, знищення або модифікація даних, використання ресурсів комп'ютера для реалізації деструктивних дій над іншими комп'ютерами в мережі та ін.

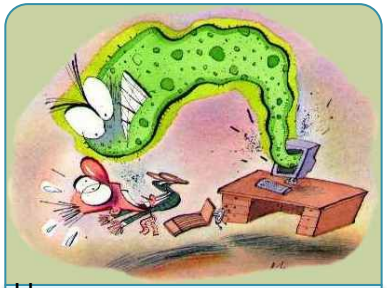
Троянські програми

- це віруси, які розміщують копії своїх кодів у складі файлів різного типу.

Файлові віруси

Боротьба із шкідливими програмами

Профілактичні заходи



Не запускати на виконання незнайомі програми

Не продукористуватися піратськими копіями програмних ктів

Не відкривати одержані через Інтернет документи без перевірки на наявність вірусів

Періодично створювати резервні копії важливих файлів на зовнішніх носіях інформації

Антивірусні програми

Перевіряють файли, диски, пам'ять на наявність вірусів, інформація про які міститься в антивірусній базі сканера

Сканери

Відстежують потенційно небезпечні операції та виводять на екран запити на їх дозвіл

Монітори

Запам'ятовують стан файлової системи, що в подальшому дає змогу відстежувати здійснені в ній зміни

Ревізори

Розрізняють такі антивірусні програми:

- Детектори (сканери)
- Лікарі
- Монітори

Для ефективної боротьби з вірусами розробники антивірусних програм створюють так звані антивірусні бази – сукупність даних про відомі на певний момент часу віруси і способи боротьби з ними.

Існуючі антивірусні програми відомих фірм – це комплексні програми, що мають властивості всіх перерахованих типів програм.

Основні дії антивірусної програми

- Сканування пам'яті та вмісту дисків за розкладом
- Сканування пам'яті комп'ютера, а також файлів, що записуються та читаються, під час виконання операцій з ними
- Сканування стиснених файлів
- Розпізнавання поведінки, властивої комп'ютерним вірусам
- Автоматичне оновлення антивірусних баз через Інтернет
- Ведення журналів подій, що стосуються антивірусного захисту

Антивірус Касперського

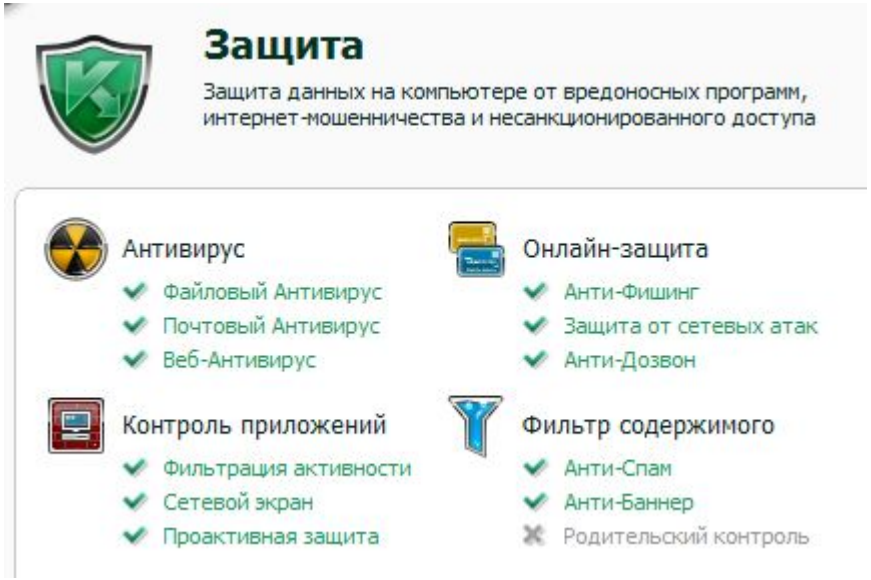
Ця програма не тільки виконує стандартні антивірусні функції, ай здатна відстежувати всі змінення даних на комп'ютері та контролювати "поведінку" документів Microsoft Office.

Головне вікно програми

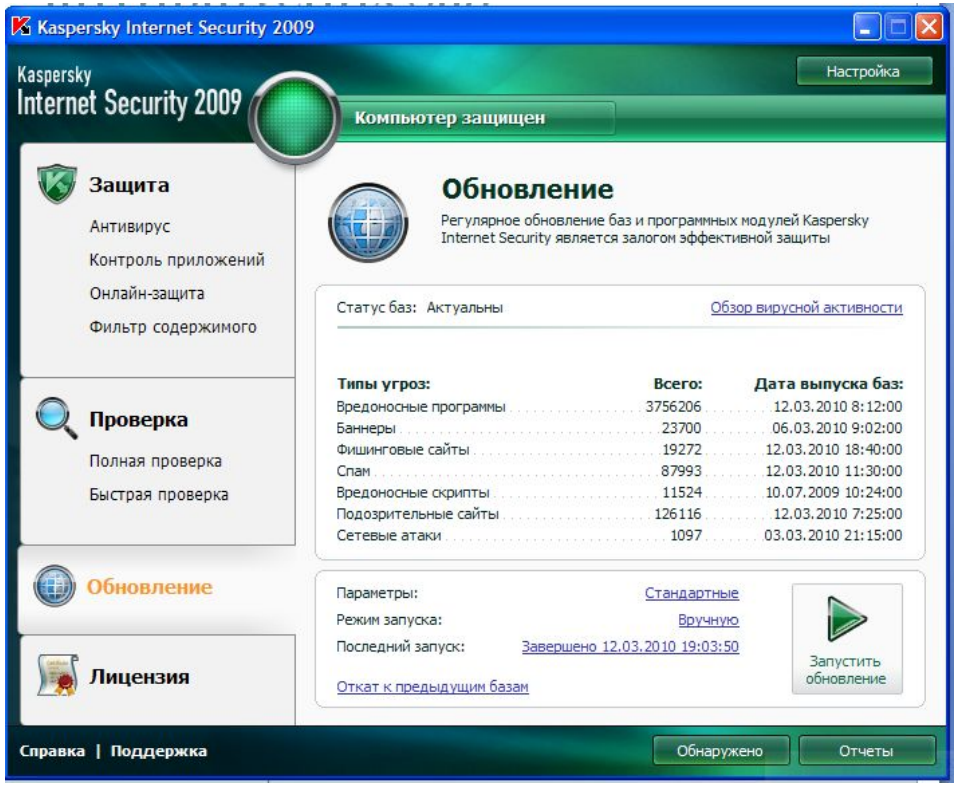
Зверху відображується інформація про поточний стан комп'ютера. Зелений колір свідчить, що захист здійснюється на належному рівні, а жовтий і червоний кольори – про наявність загроз безпеці. За допомогою посилань, розміщених у вікні ліворуч, можна отримати доступ до таких вкладок: **Захист** (Антивірус, Контроль прикладних програм, Онлайн-захист), **Перевірка**, **Оновлення**, **Ліцензія**. Праворуч можна задавати параметри функцій, вибрані у лівій частині, та запускати певні завдання.

Перевірка на наявність вірусів та оновлення антивірусних баз

Параметри захисту можна задати на вкладці **Захист**.



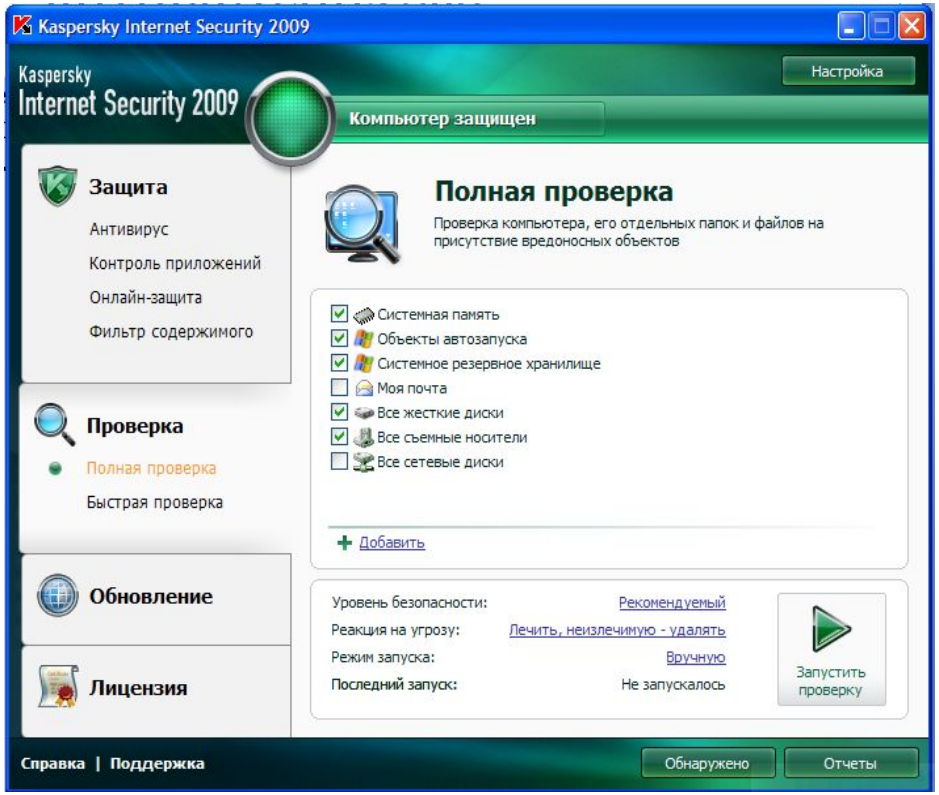
Щоб оновити базу антивірусу, клацнути посилання Оновлення, після чого відкриється онлайнова вкладка.

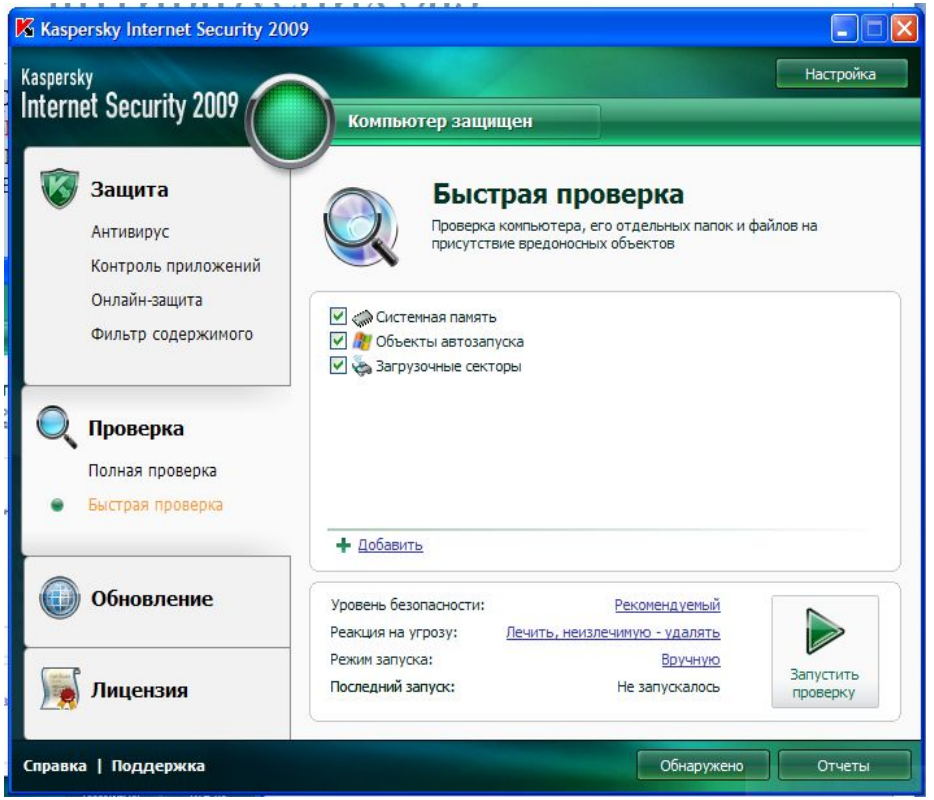


Перевірка на наявність вірусів та оновлення антивірусних баз

Виконати повну перевірку комп'ютера – перейти на вкладку **Повна перевірка** в головному вікні програми і клацнути кнопку Запустити перевірку.

Із вкладки **Швидка перевірка** можна запустити перевірку системної пам'яті, програм, що запускаються автоматично, та областей диска, де записано файли ОС





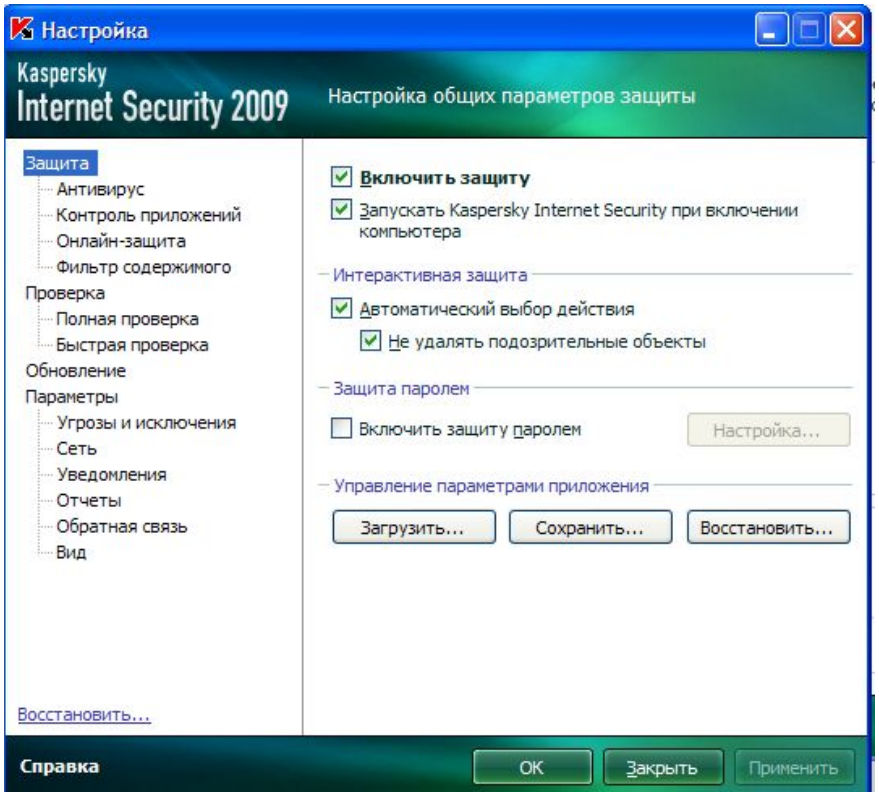
Робота з програмою

Виявивши заражений або підозрілий об'єкт, що не піддається лікуванню, програма повідомить про це й запропонує обрати певну дію:

- Перемістити об'єкт, що становить загрозу, до карантину (спеціальної папки, об'єкти з якої не можуть бути використані);
- Видалити об'єкт;
- Пропустити об'єкт, якщо ви цілком впевнені, що він нешкідливий.

Настроювання програми

Якщо клацнути кнопку настройка в головному вікні програми, то відкриється вікно настроювання її параметрів.



Цікаві новини

В інтернеті з'явився новий вірус, який викрадає паролі

Десятки тисяч інтернет-користувачів в усьому світі постраждали від нової епідемії комп'ютерних вірусів, які викрадають паролі, сказано в повідомленні дослідницької лабораторії Trendlabs компанії Trend Micro.

Виробник мережевих антивірусних програм, програмного забезпечення і послуг для захисту контенту зазначає, що спочатку епідемія торкнулася тисячі популярних італійських сайтів, а потім атака "дуже швидко" розповсюдилася по всьому світу.

"Протягом 48 годин після початку епідемії було зламано більше двох тисяч італійських сайтів. Trend Micro реєструвала подвоєння числа жертв кожні 6-8 годин", сказано в повідомленні.

Шкідливий код, що знаходиться на заражених сайтах, встановлює на комп'ютер користувача програму, здатну викрадати паролі і перетворювати комп'ютер на сервер, призначений для здійснення атак на інші комп'ютери.

За словами старшого дослідника інтернет-загроз Trendlabs Івана Макалінтала, - зловмисники використовують декілька шкідливих програм для того, щоб залишитися непоміченими і встановити програму, призначену для крадіжки такої персональної інформації, як банківські дані і паролі.

Пам'ятайте!

Комп'ютерні віруси - це програми, які заважають нормальній роботі комп'ютера.
Віруси перезаписують, ушкоджують або видаляють дані. Вони також поширюються між комп'ютерами в мережі і через інтернет, часто уповільнюючи їх роботу і викликаючи інші збої.

З підключенням до мережі Інтернет Ваш комп'ютер стає більш схильним до небезпеки зараження вірусами, мережевими черв'яками, рекламними і шпигунськими програмами. Нові шкідливі програми з'являються щодня і розташовуються на самих різних ресурсах мережі, зайшовши на які, вони непомітно проникають до Вашої системи. Ми зможемо правильно видалити віруси і попередити повторне зараження, встановивши і налагодити необхідні антивірусні продукти.

Віруси можуть:
- викликати перезавантаження або виключення комп'ютера;
- гальмувати роботу комп'ютера;
- знищувати і псувати дані (файли);
- розсилати самого себе через інтернет і в локальній мережі (втрата трафіку, проблеми з провайдером);
- операційна система може перестати працювати;
- виробляють розсилку по Інтернету, що наводить до втрати трафіку;
- і безліч інших всіляких проблем.