

***Комп'ютерні  
віруси та  
антивірусний  
захист***

# Історія комп'ютерних вірусів

*Перша «епідемія» комп'ютерного вірусу сталася в 1986 році, коли вірус на ім'я Brain (англ. «мозок») «заражав» дискети персональних комп'ютерів. В даний час відомо кілька десятків тисяч вірусів, що заражають комп'ютери і розповсюджуються по комп'ютерних мережах.*



# Що таке комп'ютерний вірус?

**Комп'ютерний вірус** - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.



# Історія комп'ютерних вірусів

Перший прототип вірусу з'явився ще в 1971р .. Програміст Боб Томас, намагаючись вирішити завдання передачі інформації з одного комп'ютера на інший, створив програму Creeper, мимовільно «перестрибує» з однієї машини на іншу в мережі комп'ютерного центру.

Правда ця програма не саморозмножується, не завдавала шкоди.



# Історія комп'ютерних вірусів

Перші дослідження саморозмно-лишнього штучних конструкцій проводилася в середині минулого сторіччя вченими фон Нейманом і Вінером.



*Норберт Вінер  
(1894 - 1964)*



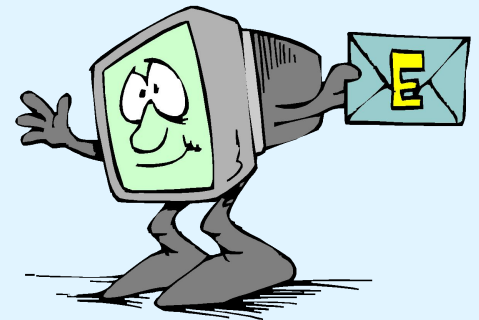
*Джон фон Нейман  
(1903 - 1957)*

# Чим небезпечний комп'ютерний вірус?

Після зараження комп'ютера вірус може активізуватися і почати виконувати шкідливі дії по знищенню програм і даних.

Активізація вірусу може бути пов'язана з різними подіями:

- настанням певної дати або дня тижня
- запуском програми
- відкриттям документа ...



# Ознаки зараження:

- загальне уповільнення роботи комп'ютера та зменшення розміру вільної оперативної пам'яті;
- деякі програми перестають працювати або з'являються різні помилки в програмах;
- на екран виводяться сторонні символи і повідомлення, з'являються різні звукові та відео ефекти;
- розмір деяких здійснених файлів і час їх створення змінюються;
- деякі файли і диски виявляються зіпсованими;
- комп'ютер перестає завантажуватися з жорсткого диска

# Класифікація комп'ютерних вірусів





# ОЗНАКИ КЛАСИФІКАЦІЇ


```
graph TD; A[ОЗНАКИ КЛАСИФІКАЦІЇ] --- B[навколишнє середовище]; A --- C[особливості алгоритму роботи]; A --- D[операційна система]; A --- E[деструктивні можливості];
```

**навколишнє  
середовище**

**особливості  
алгоритму  
роботи**

**операційна  
система**

**деструктивні  
можливості**



# Середовище проживання

файлові

завантажувальні  
і

макро

мережеві

# Файлові віруси

Впроваджуються в програми і активізуються при їх запуску. Після запуску зараженої програмою можуть заражати інші файли до моменту вимикання комп'ютера або перезавантаження операційної системи.



# Файлові віруси

перезаписувані

файлові черви

паразитичні

компаньйони

віруси-ланки

Вражаючі код  
пограм



# За способом зараження файлові віруси поділяються на:

1. **Перезаписуючі віруси.** Записують своє тіло замість коду програми, не змінюючи назву виконуваного файлу, внаслідок чого програма не запускається.
2. **Віруси-компаньйони.** Створюють свою копію на місці заражаємо програми, але не знищують оригінальний файл, а перейменовують його або переміщують. При запуску програми спочатку виконується код вірусу, а потім управління передається оригінальній програмі.
3. **Файлові черви** створюють власні копії з привабливими для користувача назвами в надії, що він їх запустить.
4. **Віруси-ланки** не змінюють код програми, а змушують ОС виконати свій код, змінюючи адресу місця розташування на диску зараженої програми, на власну адресу.

# За способом зараження файлові віруси поділяються на:

5. **Паразитичні віруси** змінюють вміст файлу, додаючи в нього свій код. При цьому заражена програма зберігає повну або часткову працездатність. Код може впроваджуватися в початок, середину або кінець програми.
6. **Віруси, що вражають вихідний код програми.** Віруси даного типу вражають вихідний код програми або її компоненти (.OBJ, .LIB, .DCU). Після компіляції програми виявляються вбудованими в неї.

# Макровіруси

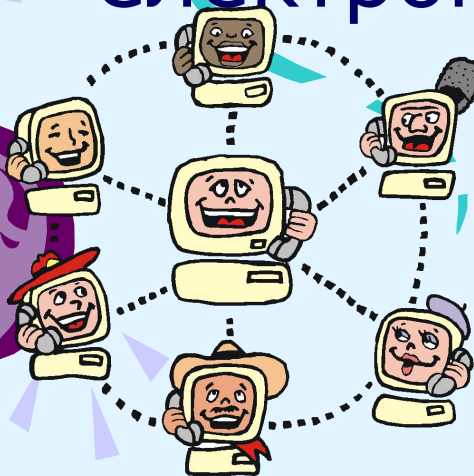
Заражають файли документів, наприклад текстових. Після завантаження зараженого документа в текстовий редактор макровірус постійно присутня в оперативній пам'яті комп'ютера і може заражати інші документи. Загроза зараження припиняється тільки після закриття текстового редактора.



# Мережні віруси

Можуть передавати по комп'ютерних мережах свій програмний код і запускати його на комп'ютерах, підключених до цієї мережі. Зараження мережевим вірусом може відбутися при роботі з електронною поштою

або при «подорожах» по Всесвітній павутині



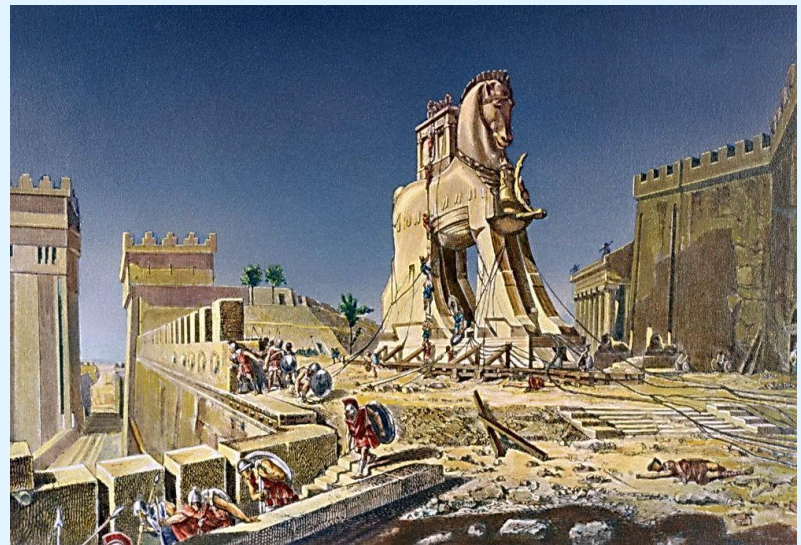


# Мережні віруси

мережові черви

Троянські програми

хакерські уліти



# Мережні віруси

Троянські програми. «Троянський кінь» вживається в значенні: таємний, підступний задум. Ці програми здійснюють різні несанкціоновані користувачем дії:

- ✓ збір інформації та її передача зловмисникам;
- ✓ руйнування інформації або зловмисна модифікація;
- ✓ порушення працездатності комп'ютера;
- ✓ використання ресурсів комп'ютера в непристойних цілях.

# Мережні віруси

Утиліти хакерів і інші шкідливі програми.

До даної категорії відносяться:

- ✓ утиліти автоматизації створення вірусів, хробаків і троянських програм;
- ✓ програмні бібліотеки, розроблені для створення шкідливого ПЗ;
- ✓ хакерські утиліти приховування коду заражених файлів від антивірусної перевірки;
- ✓ програми, що повідомляють користувача свідомо помилкову інформацію про свої дії в системі;
- ✓ інші програми, тим чи іншим способом навмисно завдають прямого або непрямого збитку даному або віддаленим комп'ютерам.



Не ждали?  
А я иду к вам!

# Особливості алгоритму роботи

резидентність

самошифрування  
поліформічність

стелс-алгоритми

Нестандартні  
прийоми

# Особливості алгоритму роботи

**Резидентний вірус** при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звертання операційної системи до об'єктів зараження і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до вимикання комп'ютера або перезавантаження операційної системи. Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Резидентними можна вважати макро-віруси, оскільки вони постійно присутні в пам'яті комп'ютера на увесь час роботи зараженого редактора.

Використання **стел-алгоритмів** дозволяє вірусам цілком або частково сховати себе в системі. Найбільш розповсюдженим стелс-алгоритмом є перехоплення запитів ОС на читання / запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або «підставляють» замість себе незаражені ділянки інформації.

# Особливості алгоритму роботи

## **Самошифрування і поліморфічність**

використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру детектування вірусу. Поліморфік-віруси - це досить труднообнаружимі віруси, що не мають сигнатур, тобто не містять жодного постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусу не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

Різні **нестандартні прийоми** часто використовуються у вірусах для того, щоб якнайглибше сховати себе в ядрі ОС, захистити від виявлення свою резидентну копію, утруднити лікування від вірусу і т.д.

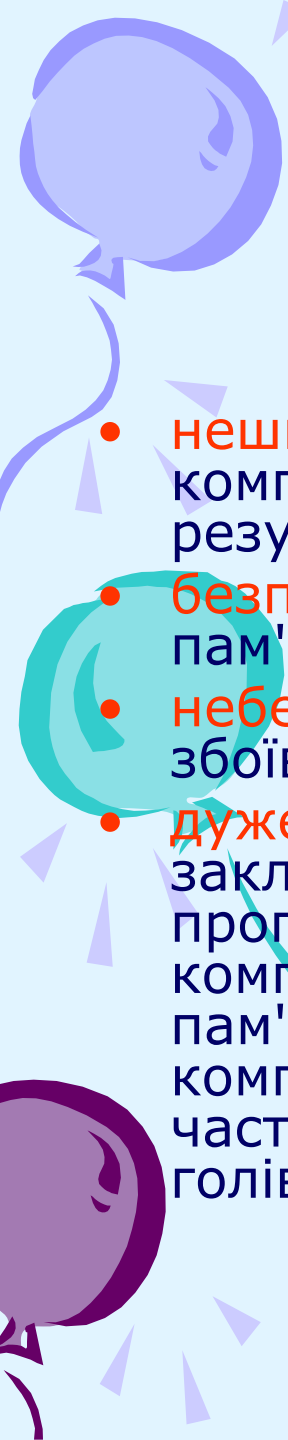
# Деструктивні можливості

не шкідливі

безпечні

небезпечні

дуже небезпечні



# За деструктивним особливостям віруси можна розділити на:

- **нешкідливі**, тобто ніяк не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширення);
- **безпечні**, вплив яких обмежується зменшенням вільної пам'яті на диску і графічними, звуковими й ін ефектами;
- **небезпечні віруси**, які можуть привести до серйозних збоїв у роботі комп'ютера;
- **дуже небезпечні**, в алгоритм роботи яких свідомо закладені процедури, що можуть привести до втрати програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті, і навіть, як говорить одна з неперевірених комп'ютерних легенд, сприяти швидкому зносу рухомих частин механізмів - вводити в резонанс і руйнувати голівки деяких типів вінчестерів



# Шляхи проникнення вірусів

- ❖ Глобальна мережа Internet
- ❖ Електронна пошта
- ❖ Локальна мережа
- ❖ Комп'ютери «Загального призначення»
- ❖ Піратське програмне забезпечення
- ❖ Ремонтні служби
- ❖ Знімні накопичувачі

# Шляхи проникнення вірусів

## Глобальна мережа Internet

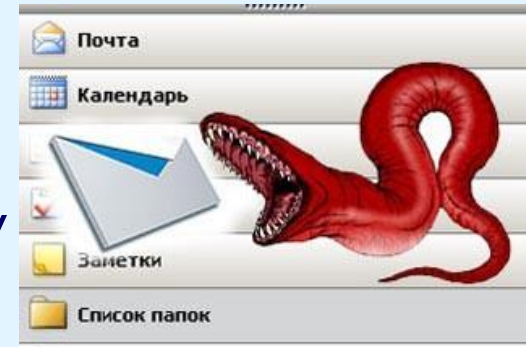
Основним джерелом вірусів на сьогоднішній день є глобальна мережа Internet. Можливе зараження через сторінки Інтернет через наявність на сторінках всесвітньої павутини різного «активного» вмісту: скриптів, ActiveX-компоненти, Java-аплетів. У цьому випадку використовуються уразливості програмного забезпечення, встановленого на комп'ютері користувача, або уразливості в ПЗ власника сайту, а нічого не підозрюючи користувачі зайшовши на такий сайт ризикують заразити свій комп'ютер.



# Шляхи проникнення вірусів

## Електронна пошта

Зараз один з основних каналів розповсюдження вірусів. Звичайно віруси в листах електронної пошти маскуються під безневинні вкладення: картинки, документи, музику, посилання на сайти. У деяких листах можуть міститися дійсно тільки посилання, тобто в самих листах може і не бути шкідливого коду, але якщо відкрити таку посилання, то можна потрапити на спеціально створений веб-сайт, що містить вірусний код. Багато поштові віруси, потрапивши на комп'ютер користувача, потім використовують адресну книгу з встановлених поштових клієнтів типу Outlook для розсилки самого себе далі.

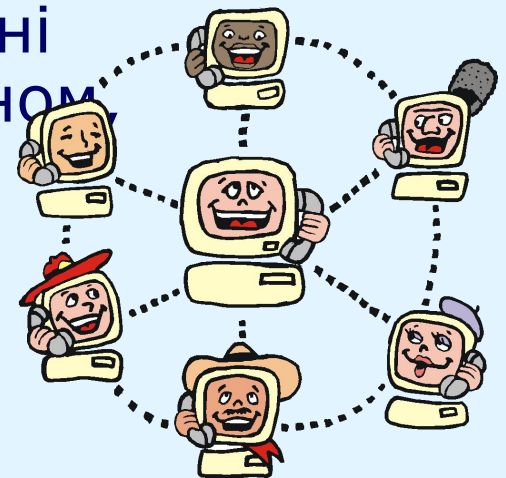


# Шляхи проникнення вірусів

## Локальна мережа

Третій шлях «швидкого зараження» - локальні мережі. Якщо не приймати необхідних заходів захисту, то заражена робоча станція при вході в мережу заражає один або кілька службових файлів на сервері

На наступний день користувачі при вході в мережу запускають заражені файли з сервера, і вірус, таким чином отримує доступ на комп'ютери користувачів.



# Шляхи проникнення вірусів

## Персональні комп'ютери «загального користування»

Небезпеку становлять також комп'ютери, встановлені в навчальних закладах. Якщо один з учнів приніс на своїх носіях вірус і заразив небудь навчальний комп'ютер, то чергову «заразу» отримають і носії всіх інших учнів, які працюють на цьому комп'ютері.

Те ж відноситься і до домашніх комп'ютерів, якщо на них працює більше однієї людини.

## Піратське програмне забезпечення

Нелегальні копії програмного забезпечення, як це було завжди, є однією з основних «зон ризику». Часто піратські копії на дисках містять файли, заражені найрізноманітнішими типами вірусів.

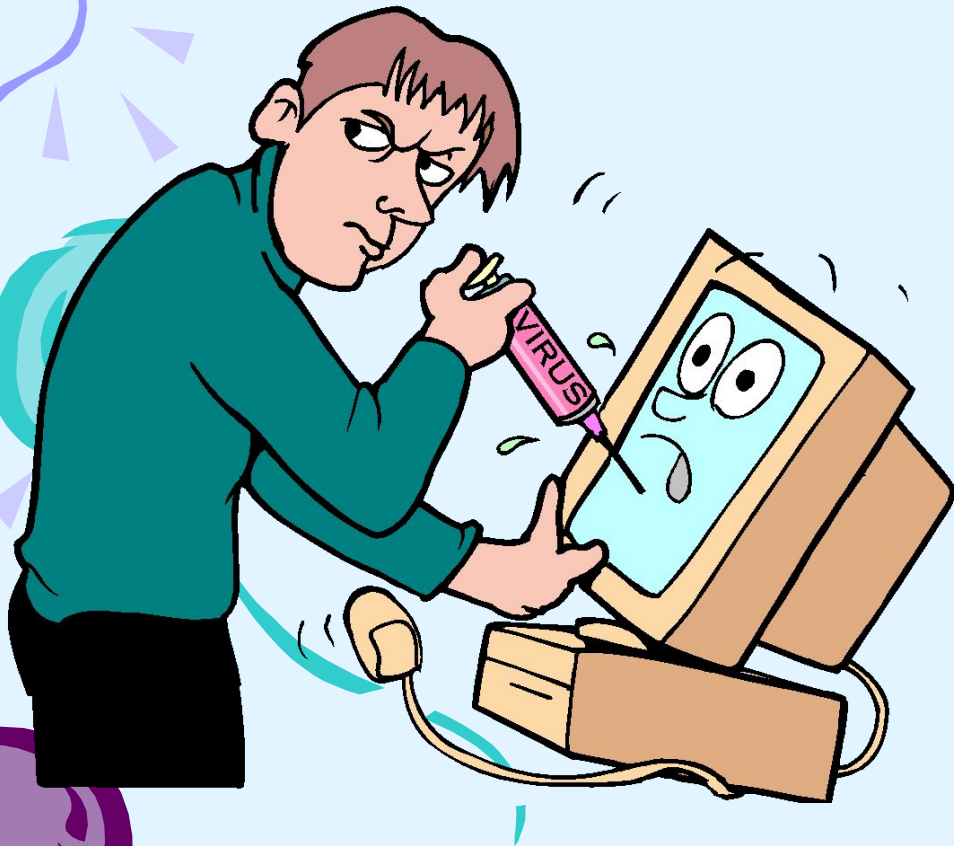


# Методи захисту

- ❖ Захист локальних мереж
- ❖ Використання дистрибутивного ПО
- ❖ Резервне копіювання інформації
- ❖ Використання антивірусних програм
- ❖ Не запускати непро-вірені файли



# Антивірусні програми



# Шляхи проникнення вірусів

## Ремонтні служби

Досить рідко, але досі цілком реально зараження комп'ютера вірусом при його ремонті або профілактичному огляді.

Ремонтники - теж люди, і деяким з них властиво байдуже ставлення до елементарних правил комп'ютерної безпеки.

## Знімні накопичувачі

В даний час велика кількість вірусів розповсюджується через знімні накопичувачі, включаючи цифрові фотоапарати, цифрові відеокамери, цифрові плеєри (MP3-плеєри), стільникові телефони





# Критерії вибору антивірусних програм

- ❖ Надійність і зручність в роботі
- ❖ Якість виявлення вірусів
- ❖ Існування версій під всі популярні платформи
- ❖ швидкість роботи
- ❖ Наявність додаткових функцій і можливостей



# ПРОЦЕС ЗАРАЖЕННЯ ВІРУСОМ ТА ЛІКУВАННЯ ФАЙЛУ

Комп'ютерни  
й вірус

Не заражена  
програма

Заражений  
файл

Комп'ютерни  
й вірус

Антивірусна  
програма

Вилікуваний  
файл



# Антивірусні програми

СКАНЕРИ  
(фаги, поліфаги)

CRC-СКАНЕРИ  
(ревізори)

Блокувальники

Імунізатори

Універсальні

Спеціалізовані

Резидентні

Нерезидентні

# Програми-лікарі



Принцип роботи  
антивірусних  
сканерів  
заснований на  
перевірці файлів,  
секторів і  
системної пам'яті  
та пошуку в них  
вірусів

# Програми-детектори



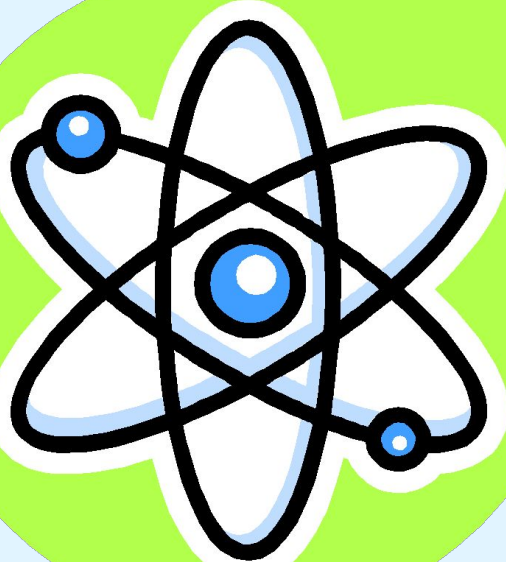
Принцип роботи  
антивірусних  
сканерів  
заснований на  
перевірці файлів,  
секторів і  
системної пам'яті  
та пошуку в них  
вірусів

# Програми-ревізори



Принцип їх роботи полягає в підрахунку контрольних сум для присутніх на диску файлів / системних секторів. Ці суми потім зберігаються в базі даних антивірусу, як, втім, і деяка інша інформація: довжини файлів, дати їх останньої модифікації і т.д. При подальшому запуску CRC-сканери звіряють дані, що містяться в базі даних, з реально підрахованими значеннями. Якщо інформація про файл, записана в базі даних, не збігається з реальними значеннями, то CRC-сканери сигналізують про те, що файл був змінений або заражений вірусом.

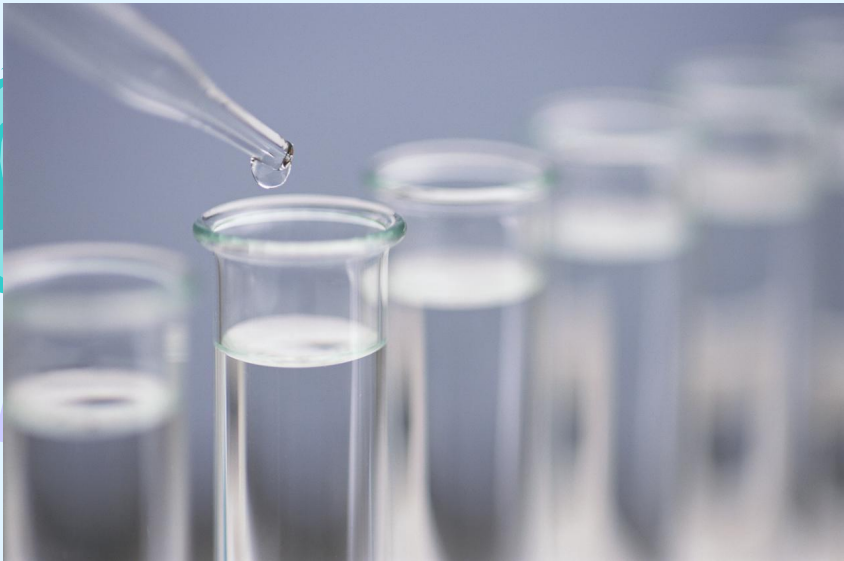
# Програми-фільтри



Антивірусні блокувальники - це резидентні програми, що перехоплюють «вірусонебезпечні» ситуації і що повідомляють про це користувачеві. До «вірусонебезпечним» відносяться виклики на відкриття для запису у виконуваних файлах, запис в boot-секторі дисків або вінчестера, спроби програм залишитися резидентно і т.д., тобто виклики, які характерні для вірусів в моменти з розмноження.

# Програми-вакцини

Імунізатори діляться на два типи:  
імунізатори, що повідомляють про зараження, і імунізатори, блокуючі зараження яким-небудь типом вірусу.





ADinf32 v3.02/Pro ( Настройки по умолчанию )



# Advanced DiskinfoScope™



- Рабочий стол
- Мой компьютер
  - Дискета 3,5" A:
  - Диск C: 20 янв 2005 г.
  - Диск D: 20 янв 2005 г.

Режимы

Без CRC

Не обнов.

<http://www.adinf.com>

Диски: 0  
Готово 0 из 0

Настройки

Старт

Выход

Нажмите "Старт" для начала работы или F1 для помощи

# ESET Smart Security 4

Business Edition



Состояние защиты



Сканирование ПК



Обновление



Настройка



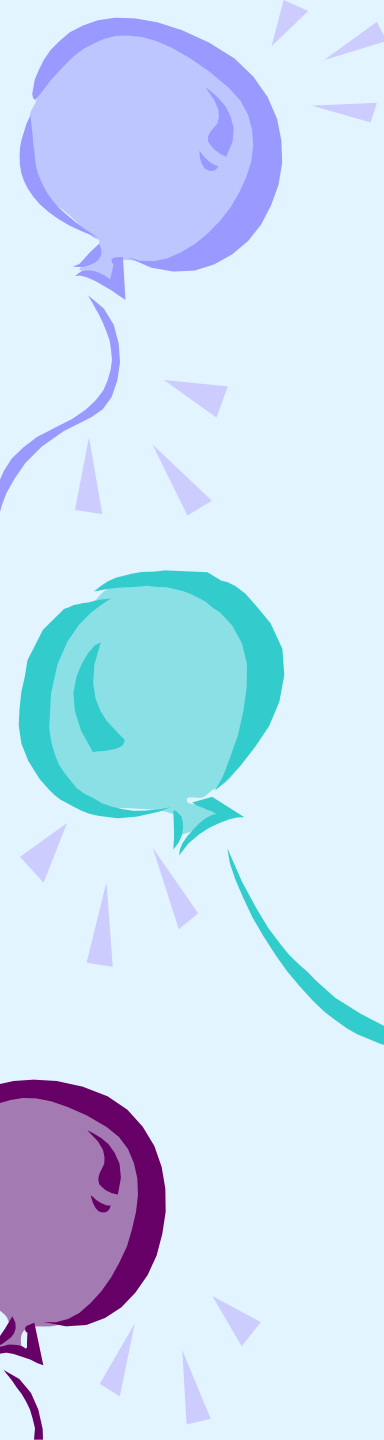
Справка и поддержка



Максимальная степень защиты

- ✓ Защита от вирусов и шпионских программ
- ✓ Персональный фаервол
- ✓ Модуль защиты от спама

Количество обнаруженных атак: 0  
Версия вирусной базы данных сигнатур: 4798 (20100122)



# Можливості програми Антивірус Касперського

- захист від вірусів, троянських програм і черв'яків;
- захист від шпигунських, рекламних та інших потенційно небезпечних програм;
- перевірка файлів, пошти і інтернет-трафіку в реальному часі;
- проактивний захист від нових і невідомих погроз;
- антивірусна перевірка даних на будь-яких типах знімних носіїв;
- перевірка і лікування файлів, що архівуються;
- контроль виконання небезпечних макрокоманд в документах Microsoft Office;
- засоби створення диска аварійного відновлення

Kaspersky  
**Anti-Virus**



Настройка



Справка

**Защита**

Активация защиты

**АНТИ-СПАМ**

**Плигк вирусов**

- Сервис**
- Обновление
  - Файлы данных
  - Аварийный диск
  - Поддержка

**Сервис**

Информация о программе

Версия:	6.0.3.837
Срочное обновление:	b.c.d.e
Дата выпуска сигнатур:	17.12.2008 12:59:56
Количество сигнатур:	1468877

Информация о системе

<u>Операционная система:</u>	<u>Microsoft Windows XP Professional Service Pack 3 (build 2600)</u>
------------------------------	--

Информация о лицензии

Владелец:	ОУсредняя ОШ 3 "Образовательный центр"	
	Мартынова Ольга Владимировна	
	Россия	
	пр-т Гагарина	
Номер:	0B2C-0003F4-03CA22F7	
Тип:	Коммерческая на 89 компьютеров	
Дата окончания:	03.01.2011 2:59:59	