

Курс “Комп’ютерна вірусологія”

Захист від комп’ютерних вірусів.

Ст. викладач

каф. Інформатики ФІ

Кирієнко Оксана Валентинівна

ok.kyrienko@gmail.com

Кібербезпека - це не гра, де можна розраховувати на щасливий випадок.

- Все шкідливе ПЗ можна розділити на відоме (70%), невідоме (29%) і складні загрози (1%).

Захист від комп'ютерних вірусів

Головні напрямки захисту:

запобігання надходженню вірусів;

запобігання вірусній атаці, якщо вірус все-таки поступив на комп'ютер;


запобігання руйнівним наслідкам, якщо атака все-таки сталася.

Основні методи захисту:

організаційний метод захисту;

апаратний метод захисту;

програмний метод захисту.



**Ціль шкідливого ПЗ –
«залишитись живим» –
як найдовше залишитися
невиявленим в зараженій системі**

Основні задачі

- приховати сліди присутності в системі від користувача
- ускладнити аналіз шкідливого ПЗ вірусними аналітиками
- атака на антивірусні рішення

Антивірус -

це програма, яка виявляє і
знешкоджує комп'ютерні
віруси.

NOD, Avast, Kaspersky, Dr.Web, McAfee,
Norton AntiVirus, Panda,...

*Користуйтесь антивірусними програмами,
або on-line сервісами перевірки.*



Не існує антивірусів, що гарантують стовідсотковий захист від вірусів. Оскільки на будь-який алгоритм антивірусу завжди можна запропонувати контр-алгоритм вірусу, невідомого для цього антивірусу (зворотне, на щастя, теж вірно: на будь-який алгоритм вірусу завжди можна створити антивірус). Більше того, неможливість існування абсолютного антивірусу була доведена математично на основі теорії скінченних автоматів (автор доведення - Фред Козн).

Основні завдання антивірусу:

- Сканування файлів і програм в режимі реального часу
- Сканування комп'ютера за потребою
- Сканування інтернет-трафіку
- Сканування електронної пошти
- Захист від атак ворожих веб-вузлів
- Відновлення пошкоджених файлів

Якість антивірусної програми

Визначається за такими параметрами:

- Надійність і зручність роботи
- Якість виявлення вірусів
- Кросплатформність антивірусу
- Можливість перевірки файлів з льоту
- Швидкодія

Класифікація антивірусів

За технологіями антивірусного захисту:

- **Класичні антивірусні продукти** (продукти, які застосовують тільки сигнатурний метод детектування)
- **Продукти проактивного антивірусного захисту** (продукти, які попереджують зараження системи, а не шукають вже відоме шкідливе ПЗ)
- **Комбіновані продукти** (продукти, які застосовують як класичні, сигнатурні методи захисту, так і проактивні)

Класифікація антивірусів

За технологіями виявлення вірусів:

- Технології сигнатурного аналізу. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі. Дозволяє виявляти відомі віруси зі стовідсотковою ймовірністю.
- Технології ймовірнісного аналізу:
 - Евристичний аналіз
 - Поведінковий аналіз
 - Аналіз контрольних сум
- Хмарні технології . Весь аналіз файлів відбувається на серверах вендорів - антивірус постійно питає у хмари оцінку кожного файлу, і якщо файл новий - передає його на перевірку.

Класифікація антивірусів

За технологіями виявлення вірусів:

Технології імовірнісного аналізу

- Евристичний аналіз – технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об'єктів. У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонам. Це допомагає визначати гібриди й нові версії раніше відомих вірусів. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не припускає лікування. Дана технологія не здатна на 100% визначити вірус перед нею чи ні, і як будь-який імовірнісний алгоритм грішить помилковими спрацьовуваннями.
- Поведінковий аналіз
- Аналіз контрольних сум

Класифікація антивірусів

За технологіями виявлення вірусів:

Технології імовірнісного аналізу

- **Поведінковий аналіз** - технологія, у якій рішення про характер об'єкта, що перевіряє, приймається на основі аналізу виконуваних їм операцій. Поведінковий аналіз досить вузько застосовується на практиці, тому що більшість дій, характерних для вірусів, можуть виконуватися й звичайними додатками. Найбільшу популярність одержали поведінкові аналізатори скриптів і макросів, оскільки відповідні віруси практично завжди виконують ряд однотипних дій. Можуть відслідковувати спроби прямого доступу до файлів, внесення змін у завантажувальний запис дискет, форматування жорстких дисків і т.д.

Поведінкові аналізатори не використовують для роботи додаткових об'єктів, подібних до вірусних баз й, як наслідок, нездатні розрізняти відомі й невідомі віруси - всі підозрілі програми апріорі вважаються невідомими вірусами.

Не припускають лікування.

Класифікація антивірусів

За технологіями виявлення вірусів:

Технології імовірнісного аналізу

- **Аналіз контрольних сум** - це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін - одночасність, масовість, ідентичні зміни довжин файлів - можна робити висновок про зараження системи.

Аналізатори контрольних сум ("ревізори") не використовують у роботі додаткові об'єкти й видають вердикт про наявність вірусу в системі винятково методом експертної оцінки. Більша популярність аналізу контрольних сум пов'язана зі спогадами про однозадачні операційні системи, коли кількість вірусів бути відносно невеликим, файлів було небагато й мінялися вони рідко. Сьогодні ревізори втратили свої позиції й використовуються в антивірусах досить рідко. Частіше подібні технології застосовуються в сканерах при доступі - при першій перевірці з файлу знімається контрольна сума й міститься в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, порівнюється, і у випадку відсутності змін файл вважається незараженим.

Класифікація антивірусів

За функціоналом продуктів:

- **Антивірусні продукти** (продукти, що забезпечують тільки антивірусний захист)
- **Комбіновані продукти** (продукти, що забезпечують не тільки захист від шкідливих програм, але і фільтрацію спаму, шифрування та резервне копіювання даних та інші функції)

Класифікація антивірусів

За цільовими платформами:

- ▶ для ОС сімейства Windows
- ▶ для ОС сімейства *NIX (ОС BSD, Linux та ін.)
- ▶ для ОС сімейства MacOS
- ▶ для мобільних платформ (iOS, Android, Windows Mobile, Symbian, BlackBerry, Windows Phone, ...)

Класифікація антивірусів

для корпоративних користувачів по об'єктах захисту:

- для захисту робочих станцій
- для захисту файлових і термінальних серверів
- для захисту поштових та Інтернет-шлюзів
- для захисту серверів віртуалізації

Види антивірусів (інша класифікація)

детектори

фільтри

лікарі

вакцини

ревізори

Види антивірусів (інша класифікація)

- **Детектори (сканери).** Розраховані на виявлення конкретних вірусів. Принцип роботи антивірусних сканерів заснований на порівнянні *сигнатур* або *масок* вірусів.
- **Лікарі (фаги).** Знаходять заражені вірусами файли і “лікують” їх, тобто видаляють з файлу тіло програми-вірусу, повертаючи файли в початковий стан.

Види антивірусів (інша класифікація)

- ➔ **Програми-ревізори** Запам'ятовують початковий стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан з початковим. Виявлені зміни виводяться на екран монітора.

Види антивірусів (інша класифікація)

- **Фільтри** - невеликі резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерними для вірусів.

Такими діями можуть бути: спроби корекції файлів з розширеннями COM, EXE зміна атрибутів файлу прямий запис на диск за абсолютною адресою запис в завантажувальні сектори диска завантаження резидентної програми При спробі якої-небудь програми провести вказані дії «сторож» посилає користувачеві повідомлення і пропонує заборонити або вирішити відповідну дію.

Види антивірусів (інша класифікація)

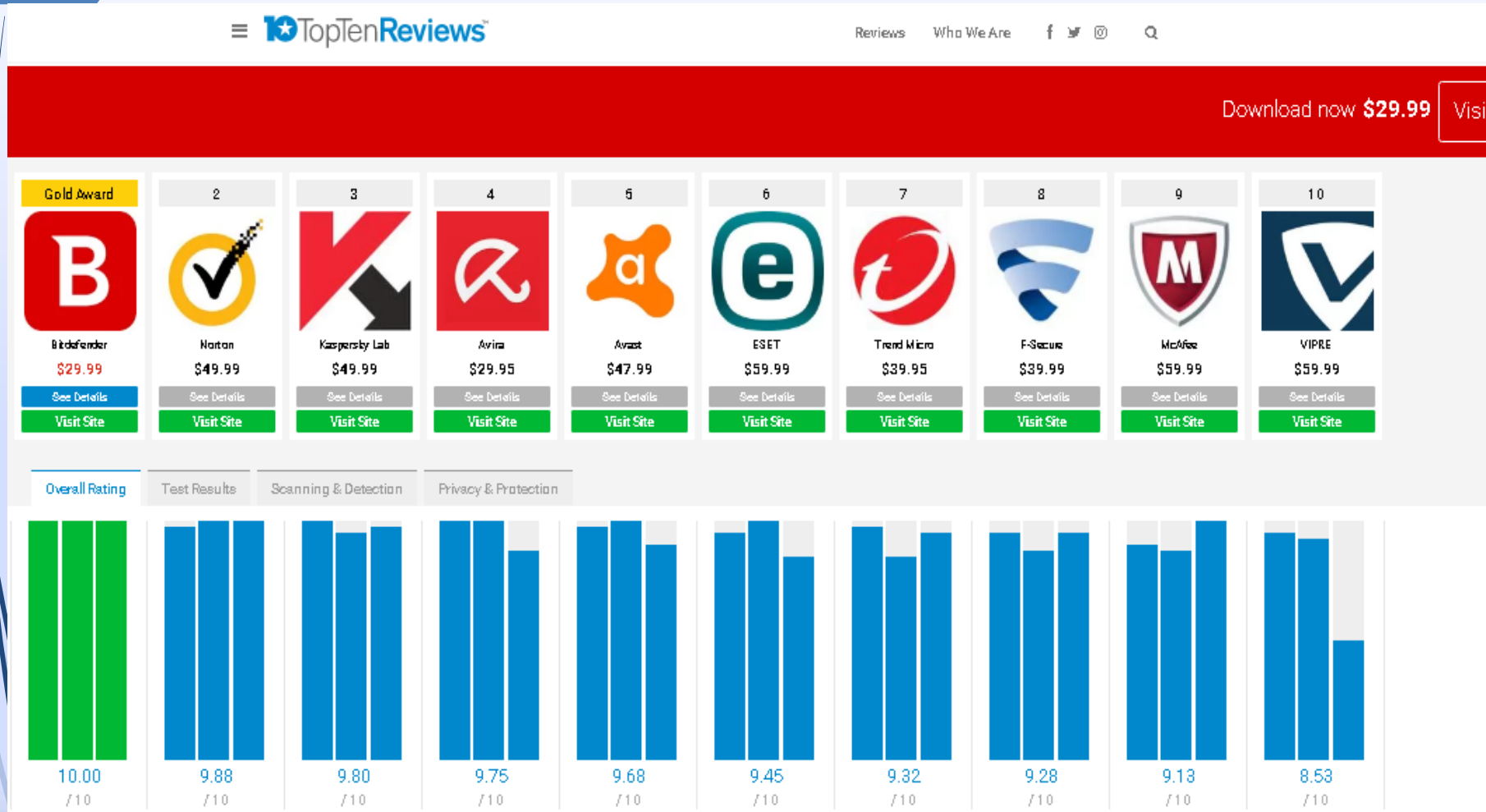
- ➔ **Вакцини (імунізатори)** - резидентні програми, що запобігають зараженню файлів - модифікує програму або диск так, щоб це не відбивалося на їх роботі, а вірус сприйматиме їх зараженими і тому не упровадиться.

Вакцини застосовують, якщо відсутні програми-доктори, що «лікують» цей вірус. Вакцинація можлива тільки від відомих вірусів. Вакцина




























2016-04 Windows 8.1	 Kaspersky Internet Security Vendor: Kaspersky Lab	Passed 			55.65	Stable
	 ESET NOD32 Antivirus Vendor: ESET	Passed 	 RAP 84.6%	84.56	32.20	Stable
	 Avast Free Antivirus Vendor: AVAST Software	Passed 	 RAP 81.6%	81.58	605.91	Solid
2016-02 SUSE Linux Enterprise Server	 ESET Security Vendor: ESET	Passed 	 RAP 88.0%	88.00	5.39	Solid
	 Avast for Linux Vendor: AVAST Software	Passed 	 RAP 85.2%	85.16	1.63	Solid
2015-12 Windows 10 Pro	 Avast Free Antivirus 2015 Vendor: AVAST Software	Passed 	 RAP 82.8%	82.84	27.18	Stable
	 ESET Nod32 Antivirus Vendor: ESET	Passed 	 RAP 84.0%	84.00	-11.95	Solid
	 Kaspersky Internet Security Vendor: Kaspersky Lab	Passed 			41.23	Solid

Порівняти надійність антивірусів Ви можете на сайті
<https://www.virusbulletin.com/testing/results/compare/vb100-antimalware>

















Який антивірус кращий?



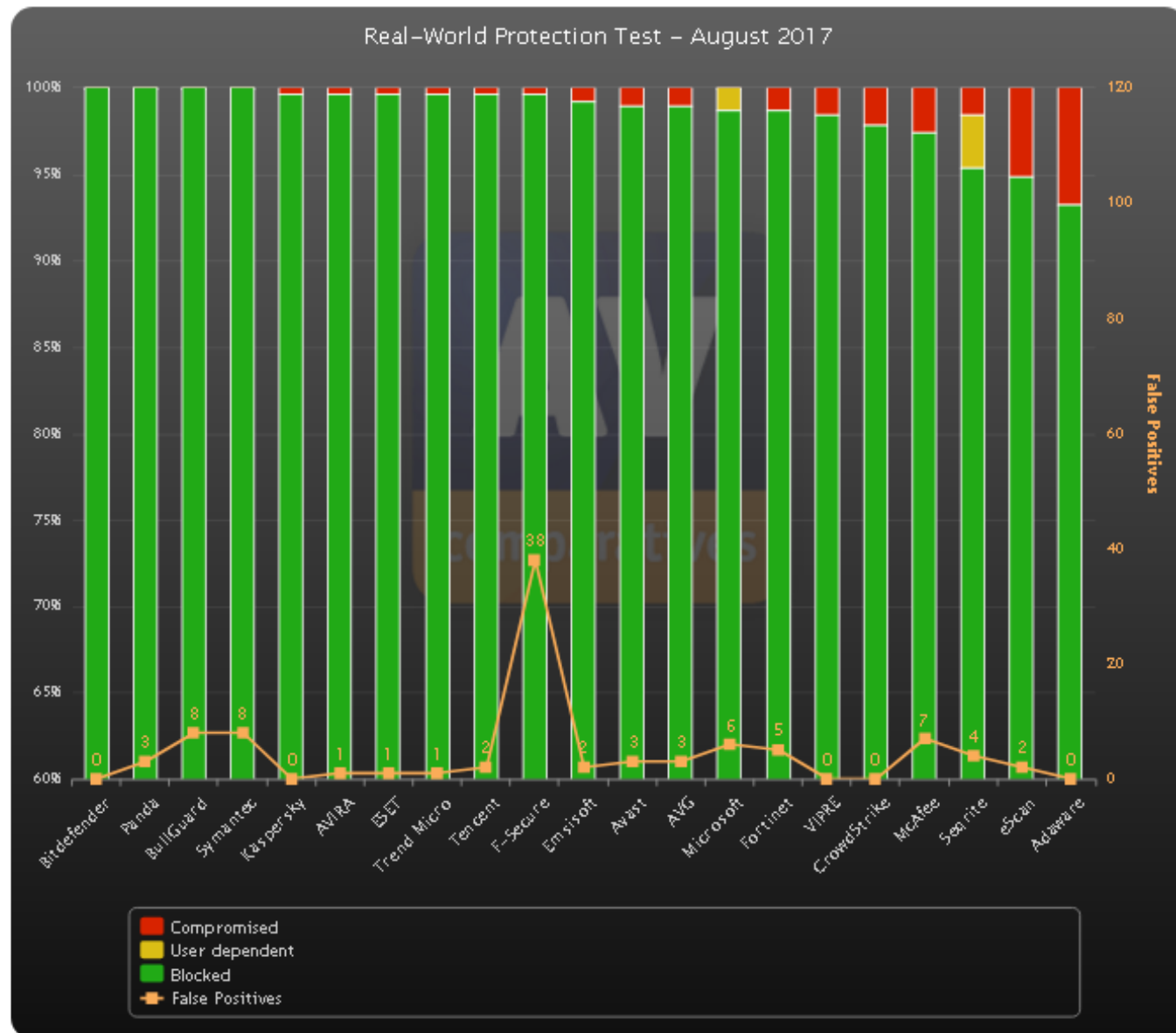
Порівняти надійність антивірусів Ви можете на сайті
<http://www.toptenreviews.com/software/security/best-antivirus-software/>

									
	Avast Free Antivirus	360 Total Security	Panda Antivirus Pro	AVG Anti-Virus Free	ESET NOD32 Smart Security	Avira Free Antivirus	Bitdefender Antivirus Free Edition	Comodo Antivirus	Dr.Web Antivirus
									
Общий рейтинг									
	9	8.3	7.7	7.7	7.7	7	6.3	5.3	5

Общие сведения:

Лицензия	бесплатная	бесплатна	пробная	бесплатна	пробная	бесплатна	бесплатная	бесплатна	пробная
Стоимость			от \$31.99		\$6/мес.				от €13/год
Русский язык									
Поддержка									

Порівняти рейтинги безкоштовних антивірусів Ви можете на сайті <http://softcatalog.info/ru/obzor/rejting-antivirusov>




Порівняти рейтинги антивірусів Ви можете на сайті
<http://chart.av-comparatives.org/chart1.php>

Заходи протидії загрозам:

- Політика безпеки і просвітницька робота
- Мережна безпека
- Системне адміністрування
- Спеціалізовані рішення по забезпеченню безпеки

Додаткові заходи:

- Протидія експлойтів для ОС
- Система попередження вторгнень
- Динамічний аналіз електронної пошти і веб-контенту



Жоден із застосовуваних підходів та методів захисту не дає гарантії 100% виявлення невідомих вірусів та шкідливих програм. Очевидно, що й спільне використання всіх технологій не дає такої гарантії.

Порівняти антивірусне ПЗ Ви можете також на сайтах:

- <https://www.av-test.org/en/compare-manufacturer-results/>
- <https://www.av-comparatives.org/>