**Лекція 14. Комп’ютерні віруси, безпека і захист персонального комп’ютеру**

**Способи захисту ПК**

Підключаючись до Інтернету, дозволяючи іншим людям користуватися комп’ютером або відкриваючи загальний доступ до файлів, необхідно прийняти міри по захисту комп’ютеру, тому що існують комп’ютерні злочинці (хакери), які атакують ПК інших людей. Вони можуть атакувати напряму, проникаючи в комп’ютер через Інтернет і викрадаючи особисті дані, або посередньо, створюючи шкідливі програми для ПК.

Для захисту комп’ютеру від потенційних погроз існують різні способи:

* *брандмауер*, який захищає ПК, запобігаючи доступу до нього шкідливих програм і сторонніх користувачів. Брандмауер не протидіє вірусам вкладень електронної пошти і фішінгу;
* *Центр оновлення Windows*, який може регулярно перевіряти наявність оновлень для ПК і автоматично їх встановлювати;
* *захист від шпигунських і інших шкідливих програм.* Антишпигунське програмне забезпечення допоможе захистити комп’ютер від шпигунських програм і іншого небажаного програмного забезпечення;
* *захист від вірусів.* Антивірусні програми допомагають захистити комп’ютер від вірусів, хробаків і інших загроз безпеці.

**Класифікація шкідливих програм**

*Мережні хробаки*

*Мережний хробак* – це шкідливий програмний код, що розповсюджує свої копії по локальним і глобальним мережам з метою проникнення на комп’ютер, запуску на ньому своєї копії і подальшого розповсюдження. Для розповсюдження хробаки використовують електронну пошту, локальні мережі, мережі миттєвих повідомлень (чата), мережі обміну даними між мобільними пристроями. Більшість хробаків розповсюджуються в файлах (вкладення в лист, посилання на файл і т.д.), хоча існують і хробаки, які розповсюджуються в вигляді мережних пакетів.

*Класичні віруси*

Ці віруси можуть мати властивості інших типів шкідливих програм. Вони діляться на класи за середовищем мешкання, а ці класи, в свою чергу, діляться на підкласи за способом зараження. Так, за середовищем мешкання віруси можуть бути:

* файлові;
* завантажувальні;
* макровіруси;
* скриптові.

*Троянські програми*

*Троянська програма (троянець)* – це шкідливий код, що виконує несанкціоновані користувачем дії. В число таких дій входять викрадання, знищення або модифікація інформації, використання ресурсів комп’ютеру з злодійською метою і т.д.

*Інші шкідливі програми*

До них відносять різноманітні програми, які не створюють загроз безпосередньо комп’ютеру:

* мережні атаки (Dos, DDos) ;
* зломщики віддалених комп’ютерів (Exploit, Hacktool);
* засмічення Мережі (Flood);
* фатальні мережні атаки (Nuker);
* введення користувача в оману (Bad-Joke, Hoax);
* шифрувальники шкідливого ПЗ.

**Використання брандмауеру Windows**

На *Панелі керування* оберіть категорію **Брандмауер Windows** і в вікні (рис.14.1) клікніть на посилання **Включення і виключення брандмауеру Windows**. Потім в новому вікні (рис.14.2) для необхідної групи (локальної і/або глобальної мережі) оберіть перемикач **Включення брандмауеру Windows** і натисніть кнопку **ОК**.

Якщо брандмауеру *Windows* включено, то встановлення зв’язку більшості програм буде ним блокуватися. При необхідності розблокування програми її необхідно дописати в список включення. Для цього в вікні (див.рис.14.1) клікніть по посиланню **Дозволити взаємодію з додатком або компонентом брандмауеру Windows** і в вікні (рис.14.3) встановіть прапорці програм і служб, які повинні запускатися через брандмауер *Windows*.

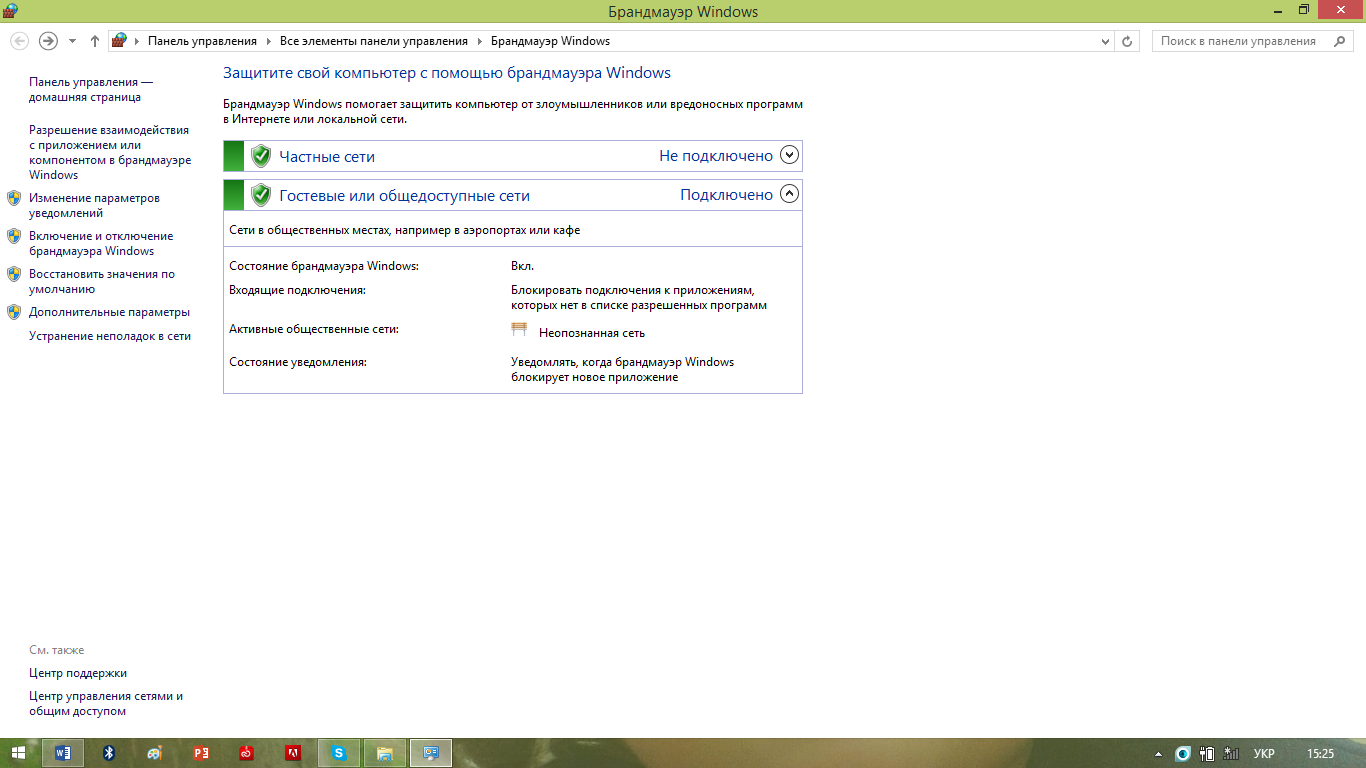


Рис.14.1. Вікно для роботи з брандмауером *Windows*

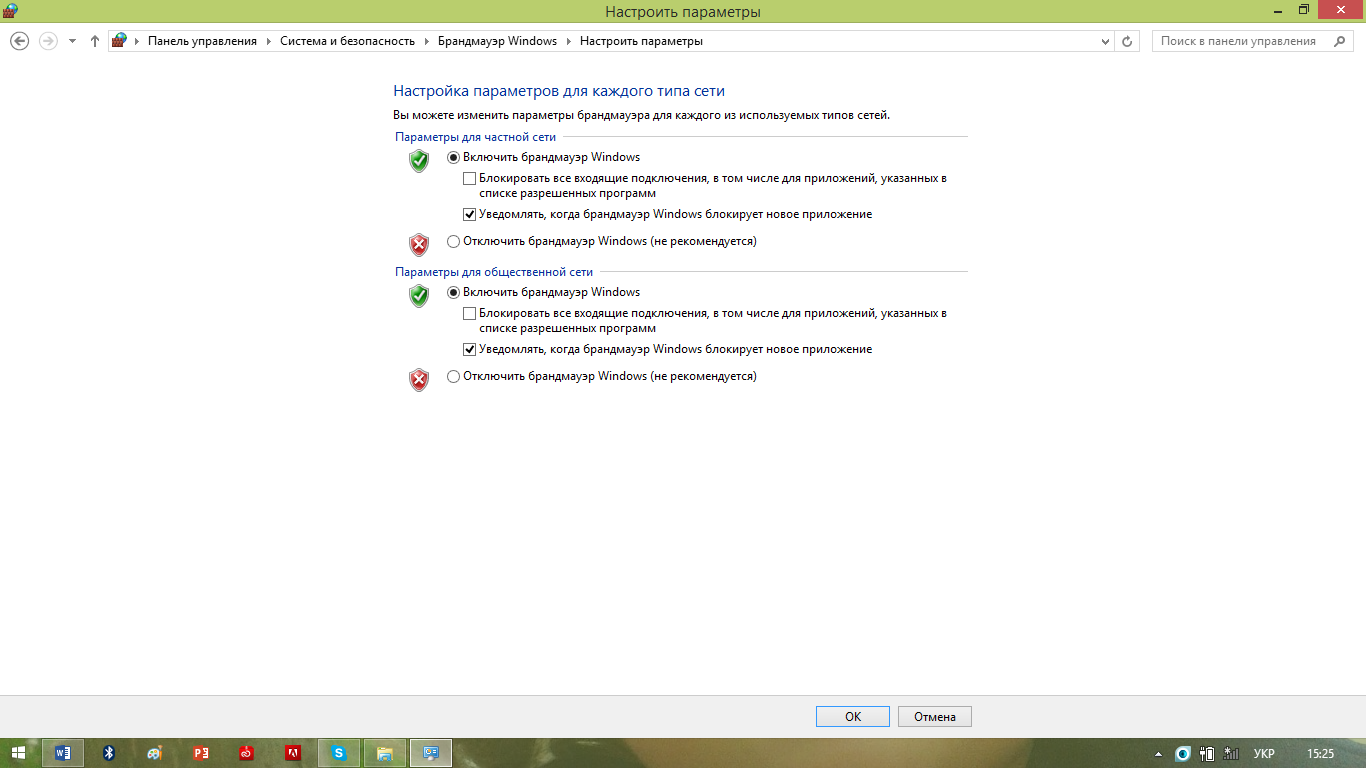


Рис.14.2. Загальні параметри брандмауеру

Щоб в список дозволів додати програму, клікніть по кнопці **Дозволити інший додаток**, в вікні оберіть програму і натисніть кнопку **Додати**.

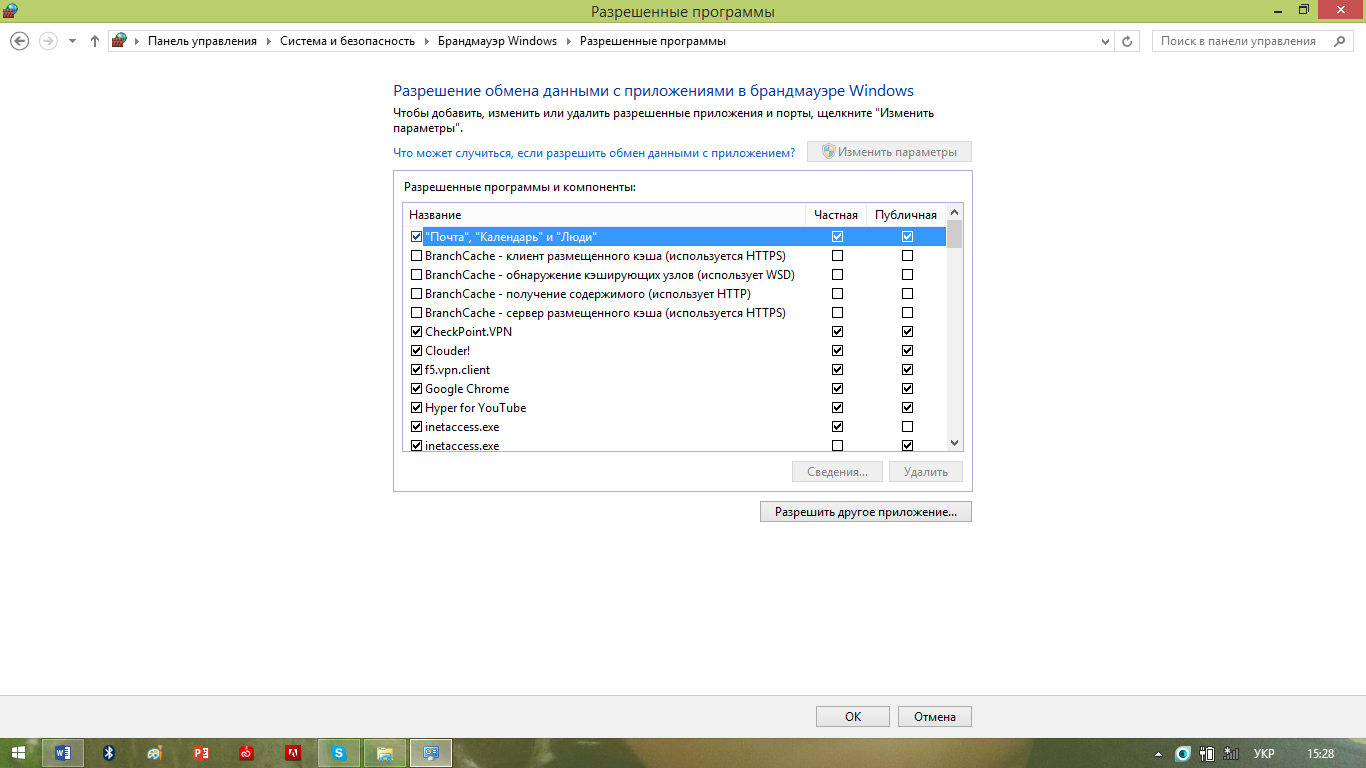


Рис.14.3. Дозвіл запуску програми через брандмауер *Windows*

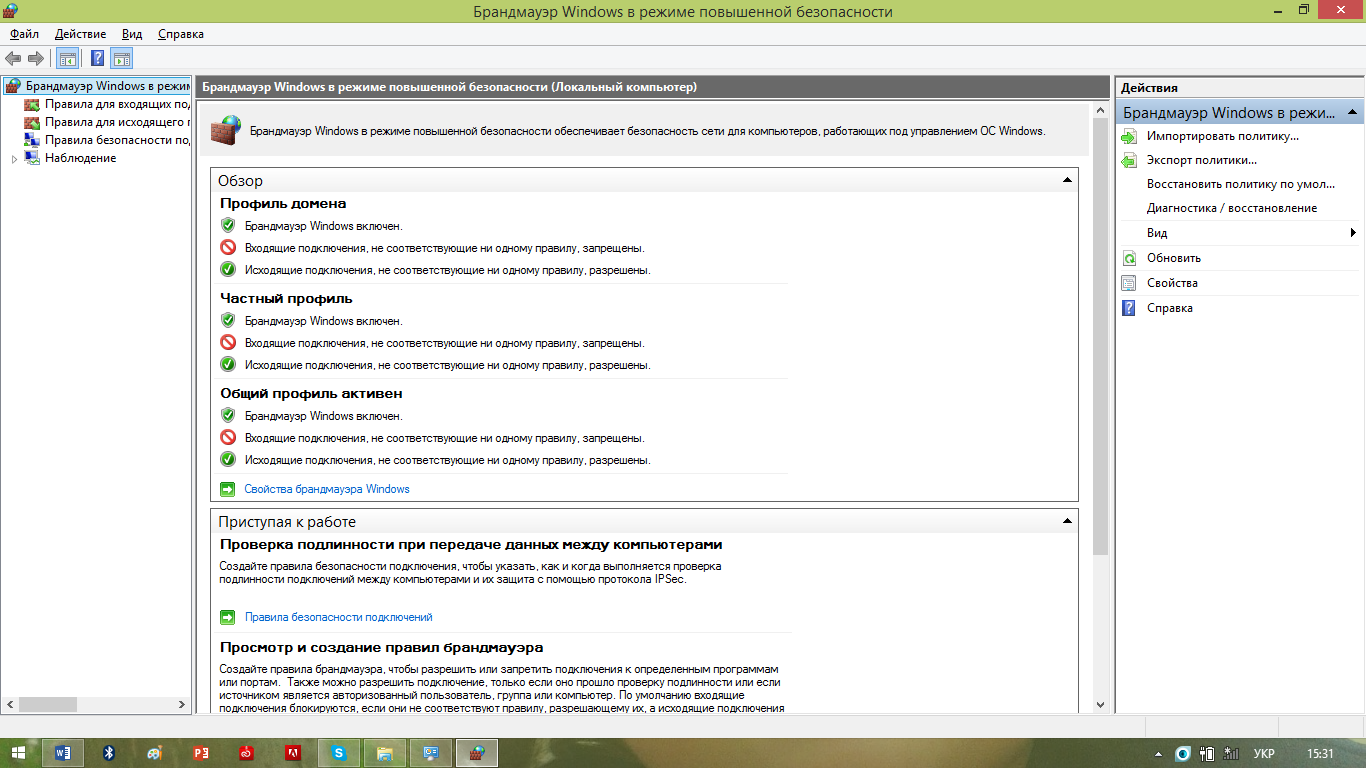


Рис.14.4. Налаштування параметрів підвищеної безпеки

Якщо в списку дозволів вибрати програму (див.рис.14.3) і клікнути по кнопці **Видалити**, то вона буде видалена із списку.

Щоб відключити брандмауер[[1]](#footnote-1) *Windows*, оберіть перемикач **Відключити брандмауер Windows (не рекомендується)** (див.рис.14.2) і натисніть кнопку **ОК**.

Щоб встановити параметри брандмауера *Windows* за замовчуванням, в вікні (див.рис.14.1) клікніть на посилання **Відновити замовчування** і в наступному вікні натисніть кнопку **Відновити значення за замовчуванням**.

Налаштування додаткових параметрів брандмауера *Windows* відбувається в вікні підвищеної безпеки (рис.14.4), яке відкривається кліканням по посиланню **Додаткові параметри** (див.рис.14.1).

**Захист ПК від вірусів**

Проста програма *USB Disk Security* (<http://www.zbshareware.com>) забезпечує захист комп’ютера від погроз, що надходять від переносних накопичувачів інформації, наприклад флешок. Вона не потребує оновлення антивірусних баз.

Після її встановлення на ПК в області повідомлень з’являється значок. При встановлені флешки в USB-порт програма перевірки запускається автоматично. В випадку виявлення вірусів їх можна видалити за допомогою кнопки **Видалити** або **Видалити все**.

Якщо на панелі інструментів обрати кнопку **Інструменти**, то в вікні (рис.14.6) можна відновити змінений шкідливими програмами системний реєстр *Windows*, почистити системний диск від непотрібних файлів і шкідливих програм в папці тимчасових файлів, а також відредагувати список програм, які повинні запускатися при завантаженні ОС.

**Антивірусні програми**

В 2014 році було відзначено так званий ювілей: 30 років з моменту створення першої антивірусної програми. За цей час світ змінився до невпізнанності, з’явились троянці для різних операційних систем і мобільних платформ, а розробка антивірусного програмного забезпечення перетворилась в цілу індустрію. Але ідеї, вперше реалізовані Енді Хопкінсом в далекому 1984 році, не втратили своєї актуальності і сьогодні.

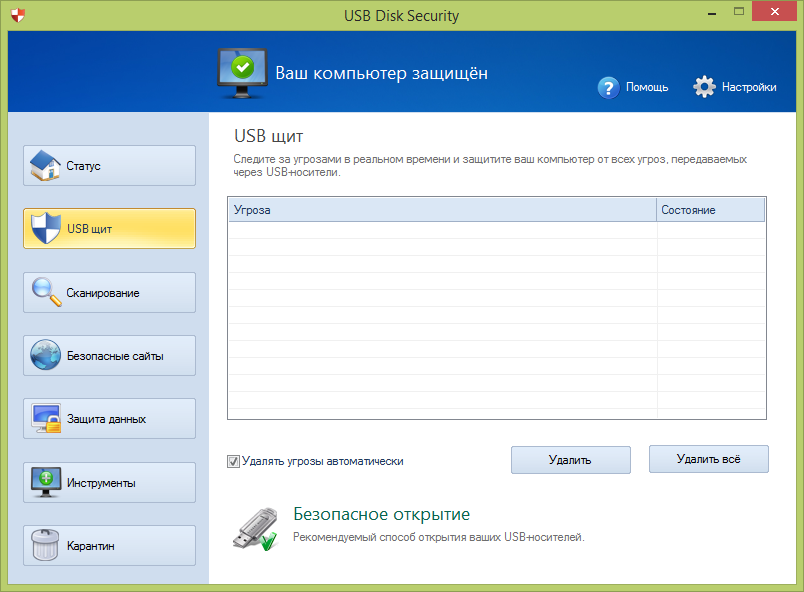


Рис.14.5. Вікно програми *USB Disk Security*

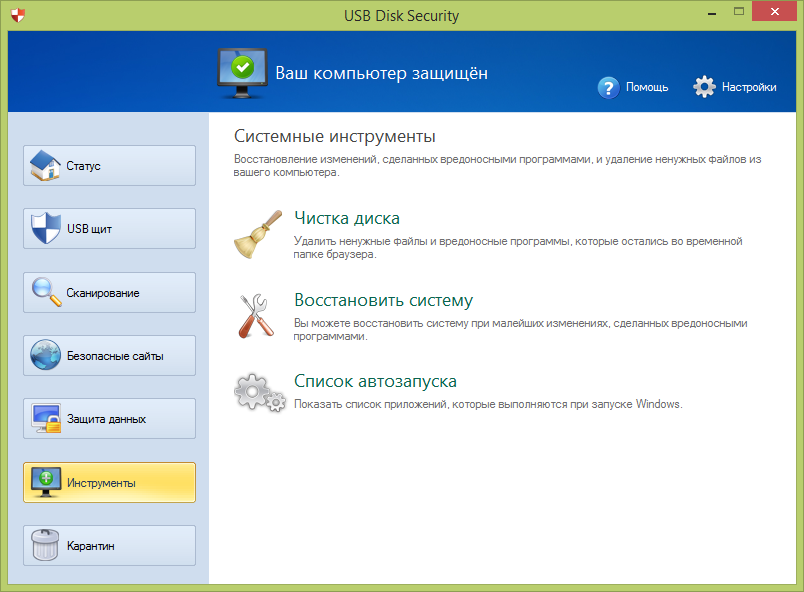


Рис.14.6. Робота з даними

**Кращий антивірус 2015 року**

Річний рейтинг кращих антивірусів. 2015 рік в цьому плані цікавий: лідери змінилися і, що слід відмітити — в ТОПі з’явився безкоштовний антивірус (який з’явився на слуху лише лудь більше року назад), не уступаючи, а в деяких речах і обходячи платних лідерів[[2]](#footnote-2).

**Кращі з кращих**

Якщо за три попередні роки в більшості незалежних тестів антивірусів лідером був Bitdefender Internet Security (про що компанія радісно повідомляла на своєму офіційному сайті), то по результатам грудня минулого року і початку цього він віддав першість продукту лабораторії Касперського — Kaspersky Internet Security.

На третьому місці з’явився безкоштовний антивірус, що влетів в рейтинг за доволі короткий час.

## Kaspersky Internet Security 2015

Почнемо з результатів останніх тестів від провідних незалежних антивірусних лабораторій:

* AV-Test (лютий 2015) — Захист 6/6, Продуктивність 6/6, Зручність використання 6/6.
* AV-Comparatives — три зірки (Advanced +) у всіх пройдених тестах (визначення, видалення, активний захист і ін.).
* Dennis Technology Labs — 100% у всіх тестах (визначення, відсутність хибних спрацювань).
* Virus Bulletin — пройдено, без хибних спрацювань (RAP 75-90%).

По сумі тестів отримуємо перше місце для антивірусного продукті Касперського.

Сам антивірус (рис.14.7), а точніше пакет Kaspersky Internet Security— зручний і ефективний продукт для захисту комп’ютеру від самих різних загроз, видалення вірусів з широкими додатковими можливостями, такими як захист платежів, батьківський контроль, аварійний диск Kaspersky Rescue Disk (що є одним із самих ефективних інструментів такого роду) і не тільки.

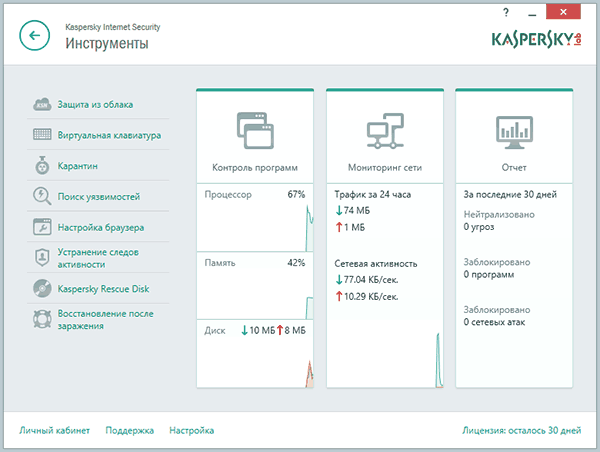


Рис.14.7. Антивірус Касперського

Один із самих частих аргументів проти антивірусу Касперського — його негативну дію на продуктивність комп’ютера. Але, тести говорять про інше: продукт добре себе показує і на збіднених ресурсами віртуальних машинах.

Офіційний сайт в Росії: <http://www.kaspersky.ru/> (є безкоштовна пробна версія на 30 днів).

## Bitdefender Internet Security 2015

Антивірусне програмне забезпечення Bitdefender (рис.14.8) весь час було лідером у всіх тестах і рейтингах. Але на початку цього року — все-таки друге місце. Результати тестів:

* AV-Test (лютий 2015) — Захист 6/6, Продуктивність 6/6, Зручність використання 6/6.
* AV-Comparatives — три зірки (Advanced +) у всіх пройдених тестах.
* Dennis Technology Labs — 92% захист, 98% точне спрацювання, загальний рейтинг — 90%.
* Virus Bulletin — пройдено (RAP 90-96%).

Також в Bitdefender Internet Security є додаткові інструменти батьківського контролю і захисту платежів, функції пісочниці, чищення і прискорення завантаження, технології анти-злодій для мобільних пристроїв, paranoid mode для параноїків і інше профілі роботи.

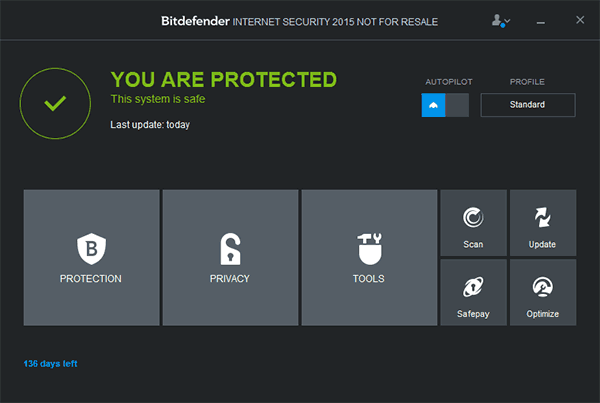


Рис.14.8. Антивірус Bitdefender Internet Security

Із мінусів для нашого користувача може бути відсутність російського інтерфейсу, в зв’язку з чим деякі функції (особливо з фірменою назвою) можуть бути не зрозумілими. В іншому — гарний зразок антивірусу, що забезпечує надійний захист, невибагливий до ресурсів комп’ютера і досить зручний.

## Qihoo 360 Internet Security (або 360 Total Security)

Безкоштовний антивірус від китайського розроблювача Qihoo 360 (раніше Qihoo 360 Internet Security, зараз під назвою 360 Total Security) (рис.14.8) буквально за рік обійшов багато платних аналогів і заслужено залишився в лідерах по всіма важливими для захисту комп’ютера і системи параметрами.

Результати тестів:

• AV-Test (лютий 2015) — Захист 6/6, Продуктивність 6/6, Зручність використання 6/6.

• AV-Comparatives — три зірки (Advanced +) у всіх пройдених тестах, дві зірки (Advanced) в тесті продуктивності.

• Dennis Technology Labs — тест даного продукту відсутній.

• Virus Bulletin — пройдено (RAP 87-96%).

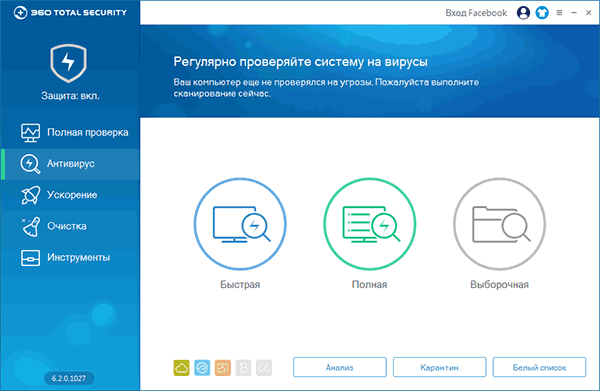
.

Рис.14.9. Антивірус 360 Total Security

Антивірус 360 Total Security[[3]](#footnote-3) має один із самих зручних і зрозумілих інтерфейсів (на російській мові), безліч дійсно корисних інструментів для чищення комп’ютера, розширене налаштування захисту, безпечний запуск програм, які згодяться як початківцю, так і досвідченому користувачеві, використовує одразу декілька технологій захисту (наприклад, задіє движок Bitdefender), забезпечуючи майже гарантоване знаходження і видалення вірусів і інших погроз з комп’ютера.

Офіційний сайт 360 Total Security на російській мові:  <http://www.360totalsecurity.com/ru/>

## Ще 5 відмінних антивірусів

Якщо попередні три антивірусу знаходяться в ТОПі по всім параметрам, то ще 5 антивірусних продуктів, які вказані нижче, по результатам тестів практично не уступають їм за якістю знаходження і видалення погроз, але знаходяться ледь позаду в плані продуктивності і зручності використання (хоча останній параметр досить суб’єктивний).

### Avira Internet Security Suite

Багатьом користувачам знайомий безкоштовний антивірус Avira (добрий і досить таки швидкий) (рис.14.10).

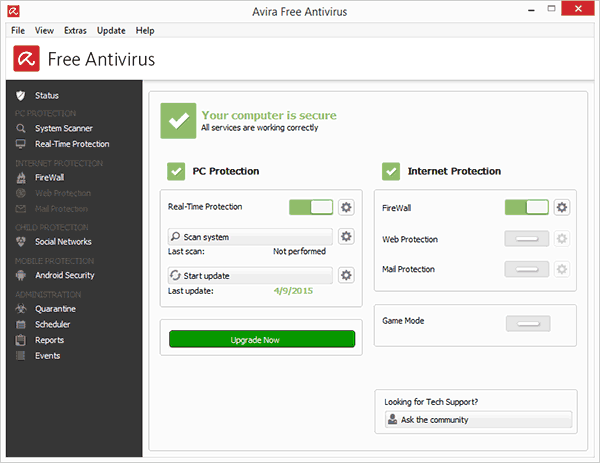


Рис.14.10. Антивірус Avira

Платне рішення для забезпечення безпеки, захист комп’ютера і даних від тієї ж компанії — Avira Internet Security Suite 2015 в цьому році також знаходиться вверху рейтингів антивірусів.

### ESET Smart Security

Ще один популярний в Росії антивірусний продукт — ESET Smart Security (рис.14.11) вже другий рік показує себе одним із кращих в антивірусних тестах, лише незначно поступаючись першій трійці по не самим критичним параметрам (а в деяких тестах, навпаки, перевершуючи їх).

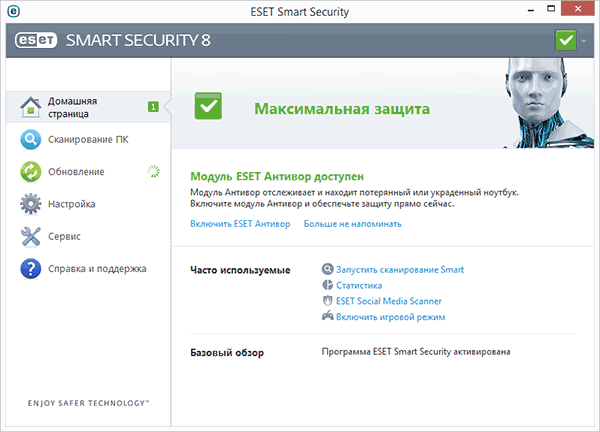


Рис.14.11. Антивірус ESET Smart Security

### Avast Internet Security 2015

Багато хто використовує безкоштовний антивірус Avast і, якщо ви один із таких користувачів і задумуєтесь про перехід на платний варіант Avast Internet Security 2015 (рис.14.12) — можна розраховувати, що захист вас не підведе, якщо судити по тим же тестам. При цьому, і безкоштовний варіант (Avast Free Antivirus) теж не набагато гірший.

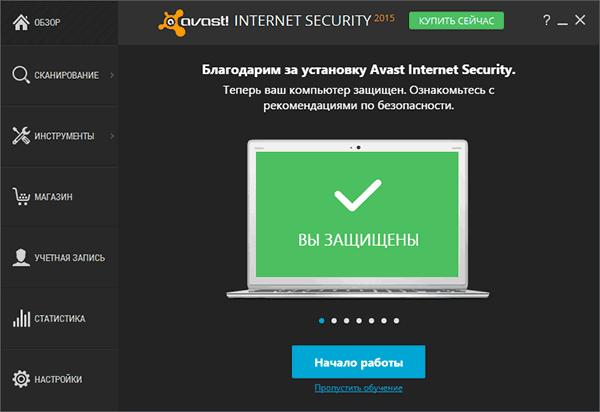


Рис.14.12. Антивірус Avast Internet Security

Результати Avast ледь більш неоднозначні, ніж у інших розглянутих продуктів (наприклад, в тестах AV-Comparatives підсумки добрі, але не кращі).

### Trend Micro і F-Secure Internet Security

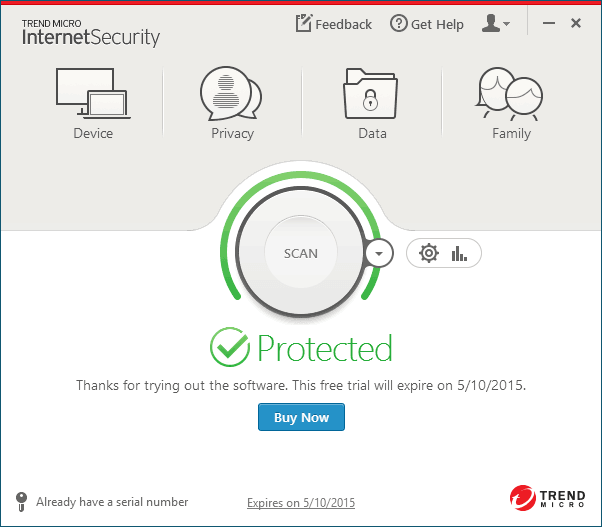


Рис.14.13. Антивірус Trend Micro

І останні два антивіруса — один от Trend Micro (рис.14.13), інший — F-Secure (рис.14.14). Обидва фігурували в рейтингах кращих антивірусів в останні роки і досить таки непопулярні в Росії. Хоча в тому, що стосується своїх прямих обов’язків, ці антивіруси справляються на відмінно.

AV-Comparatives (рис.14.15) виконує найбільш широкий набір тестів, частина із яких проводиться за підтримки влади Австрії. Майже всі тести направлені на виявлення ефективності антивірусів проти самих різних векторів атак, спроможності ПЗ знаходити самі останні загрози і видаляти їх. Максимальний результат в тестах — 3 зірки або Advanced +.

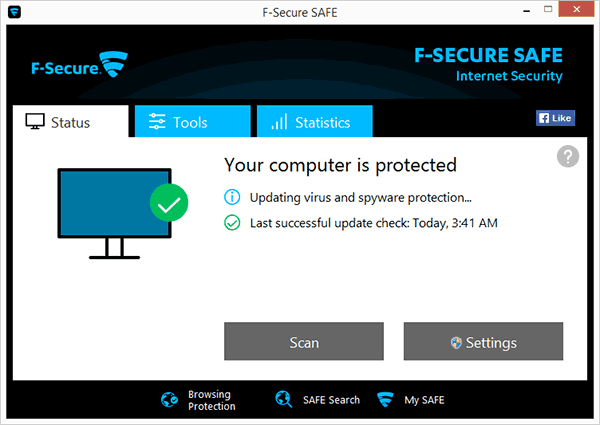


Рис.14.14. Антивірус F-Secure

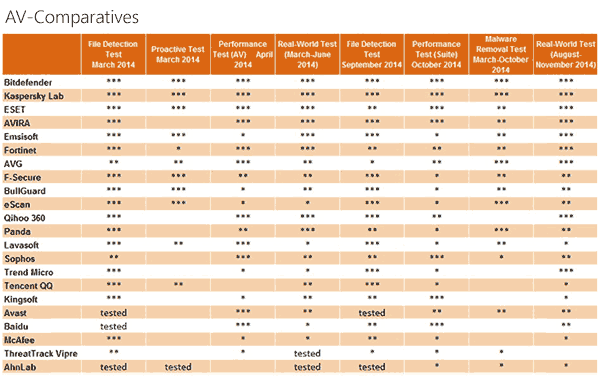


Рис.14.15. Рейтинг за AV-Comparatives

AV-Test (рис.14.16) регулярно проводить випробування антивірусів за трьома характеристиками: захист, продуктивність і зручність використання. Максимальний результат за кожною із характеристик — 6.

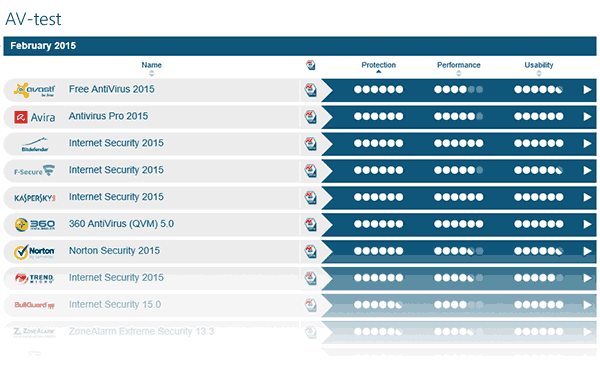


Рис.14.16. Рейтинг за AV-Test

Лабораторія Dennis Technology Labs (рис.14.17) спеціалізується на тестах, наближених до реальних умов використання, проводячи випробування на існуючих джерелах зараження вірусами і шкідливим кодом в контрольних умовах.

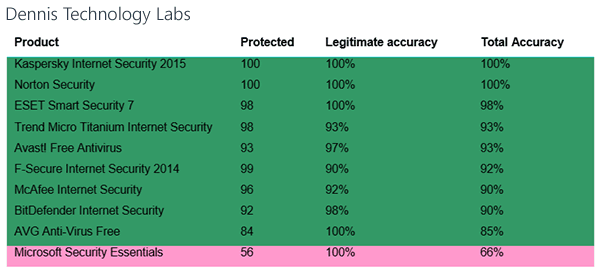


Рис.14.17. Рейтинг за Dennis Technology Labs

Virus Bulletin (рис.14.18) проводить щомісячні тести антивірусів, для проходження яких антивірус повинен виявити всі без виключення зразки вірусів без жодного хибного спрацювання. Також для кожного із продуктів розраховується відсотковий параметр RAP, який являє собою відображення ефективності активного захисту і видалення загроз на протязі декількох тестів (у жодного із антивірусів не дорівнює 100%).

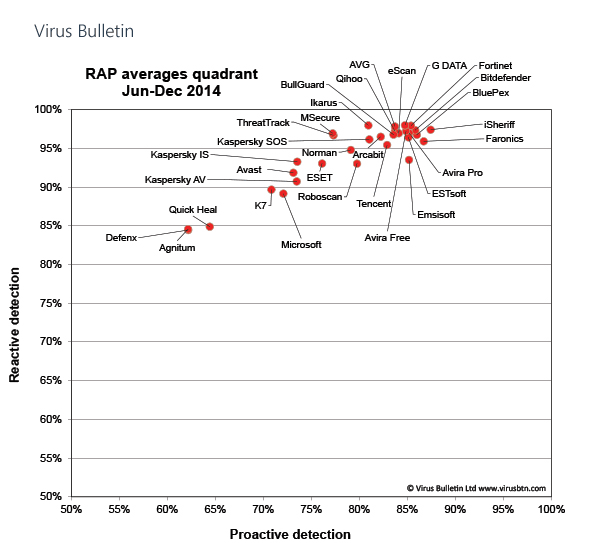


Рис.14.18. Рейтинг за Virus Bulletin

Стовідсотковий захист і знаходження на перших місцях списків антивірусів, зовсім не гарантують повну відсутність шкідливих програм на комп’ютері: існують варіанти небажаного ПЗ (наприклад, що викликають показ небажаної реклами в браузері), яке майже не визначається антивірусом, а дії користувачів можуть бути прямо направлені на те, щоб на комп’ютері з’явились віруси (наприклад, коли встановлюється неліцензійне ПЗ і спеціально для того, щоб воно встановилось, відключається антивірус).

1. Не рекомендується відключати брандмауер *Windows* до тих пір, поки не буде запущено інший брандмауер. [↑](#footnote-ref-1)
2. Аналізуються антивіруси для домашнього використання для ПК і ноутбуків з ОС Windows 7, 8 и 8.1. Можна стверджувати, що для Windows 10 результати будуть схожі. [↑](#footnote-ref-2)
3. У розробника на даний час більше одного офіційного сайту, а також дві назви — Qihoo 360 і Qihu 360,. [↑](#footnote-ref-3)