Міністерство освіти і науки, молоді та спорту України
Національна академія наук України
Національний центр «Мала академія наук України»

МОГИЛЬНИЙ С. Б.

Налаштування популярних браузерів для безпечної роботи в Інтернеті

Збірник навчально-методичних матеріалів
для слухачів
Всеукраїнської заочної школи
інформаційно-телекомунікаційних технологій

Київ – 2012

Редакційна колегія:
Лісовий О. В., Могильний С. Б. (канд. тех. наук), Пещеріна Т. В.,
Кічайкіна С.І.

Рекомендовано науково-методичною радою Національного центру
«Мала академія наук України» (протокол № 1 від 20.01.12).

Могильний С.Б. Налаштування популярних браузерів для безпечної роботи в Інтернеті. Збірник навчально-методичних матеріалів для слухачів Всеукраїнської заочної школи інформаційно-телекомунікаційних технологій / [за ред. О.В. Лісового.] . – К. : ТОВ «Праймдрук», 2012. – 52 с.

© Міністерство освіти і науки,
молоді та спорту України, 2012
© Національний центр
«Мала академія наук України», 2012
© «Центр післядипломної освіти»
ПАТ «Укртелеком», 2012

Шановні старшокласники!

Освітній проект «Всеукраїнські заочні профільні школи Малої академії наук» було започатковано у 2007 році. Його реалізація передбачає співпрацю Малої академії наук з установами Національної академії наук України і провідними вищими навчальними закладами, створення на їх базах навчально-дослідницьких майданчиків.

Для задоволення Ваших наукових інтересів у дослідницькій діяльності в систему навчально-виховної роботи МАН у 2011 році впроваджено наступні профілі заочних шкіл з організацією сесійних зборів та консультацій:

- фізико-технічний (секції «Фізика та астрономія» і «Технічні науки»);
- математичний;
- хімічний;
- інформаційно–телекомунікаційних технологій.

Головними завданнями Всеукраїнської заочної школи інформаційно-телекомунікаційних технологій є:

- Оволодіння учнями системою знань, умінь і навичок з інформатики, достатніх для успішного засвоєння інших освітніх галузей знань;
- Формування наукового світогляду, уявлення про ідеї та методи вивчення науки – інформатики;
- Налаштування популярних браузерів для безпечної роботи в Інтернеті;
- Здійснення професійної орієнтації учнівської молоді.

Узагальнюючи досвід роботи Всеукраїнської заочної школи інформаційно-телекомунікаційних технологій, Могильним Борисом, завідувачем кафедрою Інформаційнихї технологій Центру післядипломної освіти ПАТ «Укртелеком», кандидатом технічних наук, підготовлено даний збірник, у якому представлені завдання, методичні рекомендації та розв’язки різних типів задач з інформатики, а також налаштування популярних браузерів для безпечної роботи в Інтернеті для слухачів Всеукраїнської заочної школи інформаційно-телекомунікаційних технологій 2011–2012 н.р.

За допомогою збірника Ви маєте можливість самостійно налаштувати популярні браузери для безпечної роботи в Інтернеті, перевірити свій рівень знань та долучитися до практичної і наукової діяльності.

Відчуття безпеки робить людину необережною
Олександр Дюма (батько)

Інтернет в Україні

У світі Інтернетом вже користуються близько 2,1 млрд. людей. Майже половина всіх інтернет-користувачів світу молодші 25 років. Число веб-сайтів в Інтернеті на кінець 2011 року складало більше 555 млн., причому близько 300 млн. з них з'явилися саме в минулому році

Можливість скористатися Інтернетом, як джерелом інформації, має 45% населення України. Частка регулярних користувачів менша - 36%.

Про це йдеться в результатах дослідження, проведеного компанією InMind [1].

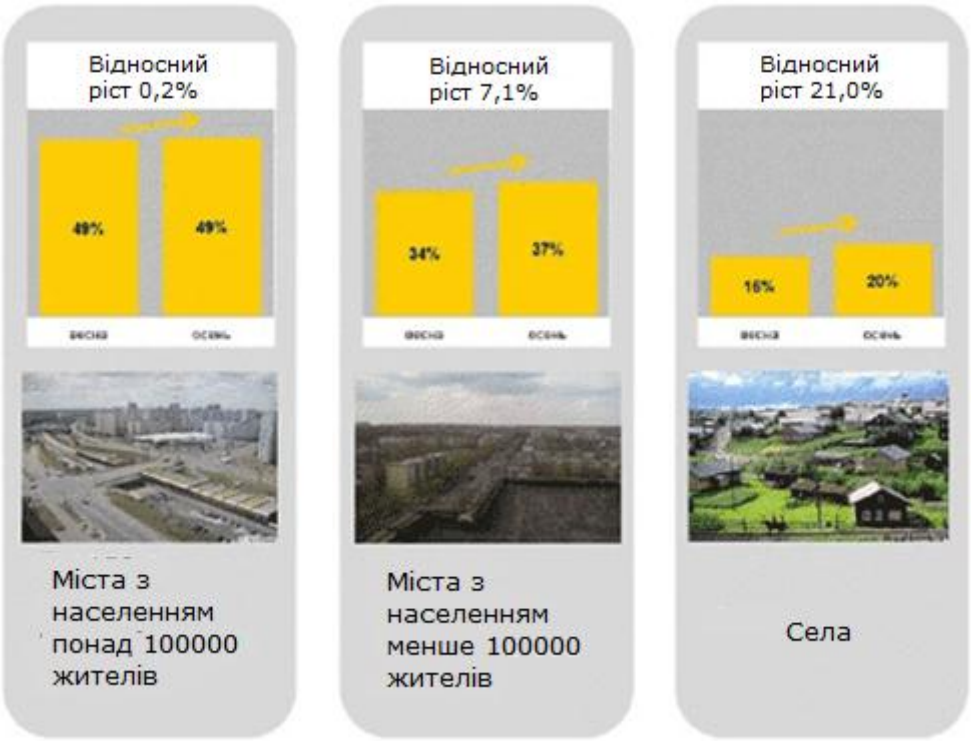
За результатами третього кварталу 2011 року вперше частка жінок (51%) перевищила частку чоловіків (49%). При цьому, в структурі всього населення частка жінок становить 55%.

Найбільш швидко в 2011 році проникнення зростало на заході і в центральній частині країни - 11,3% і 9%, відповідно. На сході та півдні динаміка була значно гіршою - 0,6% і 0,5%.

Динаміка росту проникнення Інтернету в регіонах України в 2011 році:

Згідно з новими даними InMind, у вересні кількість користувачів Інтернету в Україні склала 14,3 млн. При цьому зростання проникнення Інтернету в Україну сповільнюється і в наступному році становитиме лише 2-3%. За минулі півроку Інтернет ріс в основному за рахунок молодого населення малих міст і сіл.

Динаміка росту проникнення в різних типах населених пунктів України в 2011 році:

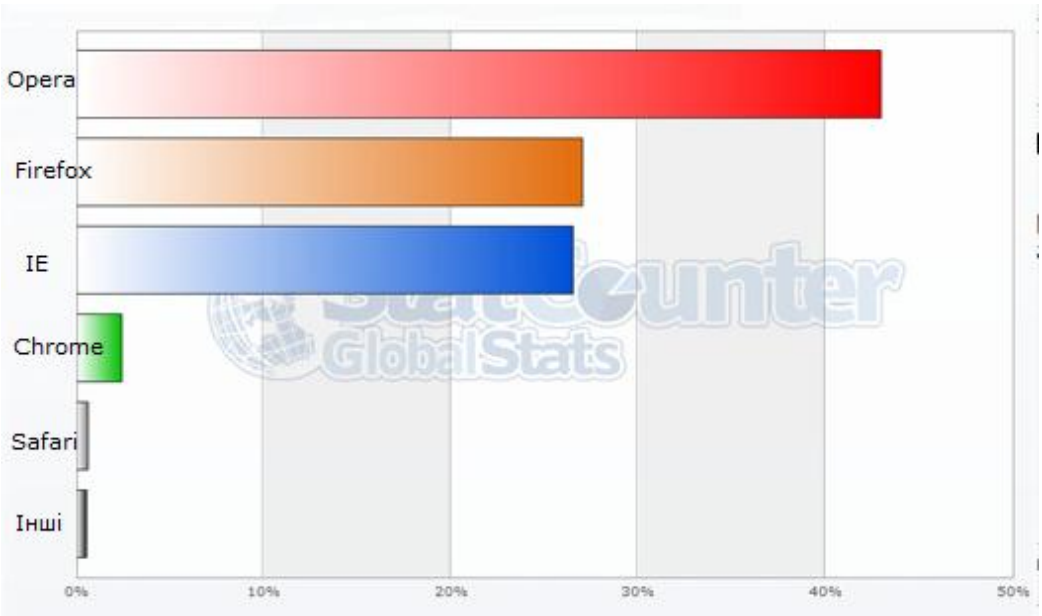


Якими браузерами користуються українці?

За даними одного з лідерів інтернет-статистики StatCounter розподіл популярності інтернет браузерів серед українських інтернет-користувачів має такий вигляд [2]:

Дещо здивувала така статистика для Opera, але при подальше вивченні матеріалів різних статистичних даних для браузерів, з'ясувалося, що в показнику для Opera додавалися показники за версіями Opera PC і показники Opera Mini. Різке зростання попиту на всілякі мобільні пристрої в Україні за останні 2 роки обумовило підвищення популярності Opera Mini.

А в 2009 році картина була зовсім іншою:



Що змінилось? Частка Opera знизилася, зате значно підвищилася частка Google Chrome, а тому можна припустити, що ті, хто спочатку поставив собі Opera, перейшли на більш зручну платформу Google - це те, що стосується мобільних пристроїв. Mozilla Firefox залишається приблизно на тому ж місці, прихильники браузера і його доповнень, не можуть мабуть відмовитися від тих зручностей, що пропонує браузер. Хоча бразер визиває все більше нарікань із-за того, що займає 1Гб пам'яті і навіть більше.

Що хотілося б зауважити про IE. Показники для IE змінилися не значно. І навряд чи будуть сильно змінюватися доти, поки IE буде наперед встановленим браузером в операційній системі Windows.

За даними агентства з онлайн досліджень Gemius, яке проводить постійний моніторинг, за 2009 рік приріст відвідувачів в Укрнет зріс в секторі жіночого контингенту з віком від 25 до 35 років – це, в основному, домогосподарки, які сидять вдома доглядаючи за дітьми. З цього випливає висновок про вміння користуватися Інтернетом відвідувача, який використовує тільки попередньо встановлений браузер.

За версіями браузерів, хотілося б відзначити, що якщо в 2009 році Opera тримала явно лідируюче становище, то в 2010 році ситуація кардинально змінилася на користь Firefox. В 2011 Opera намагалася вже на якісному рівні своєї 11-ої версії знову змогла змістити Firefox. Дуже порадувала ситуація з Chrome, який упевнено зростає в попиті користувачів і його 8 версія вже зайняла 3 місце, після Mozilla FF і Opera, обігнавши Internet Explorer. 4-е місце міцно за собою залишає Internet Explorer, поки у своїй 8-й версії, що в більшій мірі вказує на більше поширення Windows7, в якому встановлений IE8, ніж на свідомий вибір користувача.

Особливо важливо відзначити, що на IE6 вже припадає лише 2.32%, версія FF 3.5 складає 3,83%, а всі версії Opera до версії 10.5 включно не доходять до планки 6% разом, що дозволяє вже при HTML верстці веб-сторінок не орієнтуватися на ці браузери.

А як справи в інших? Проаналізувавши ряд проектів, можна з упевненістю сказати, що браузером дійсно по-різному користуються в Росії та Україні. Проекти, створені навіть в одній сфері: російські - частіше відвідуються за допомогою IE, Firefox, Opera, Chrome; в українських користувачів зовсім інші пріоритети - Opera, Firefox, Chrome, IE. Напевно, це хороший показник просунутості користувачів, що дозволяє розробникам створювати все більш цікаві технологічні проекти [2].

Порівняння безпеки популярних інтернет-браузерів

Розгляд проблем безпеки використання популярних сучасних браузерів для платформи Windows покликаний підняти питання безпеки використання

сучасних інтернет-технологій на тлі їх все більшої популяризації і все більш міцного входження в життя кожної сучасної людини.

Індустрія браузерів існує, в основному, за рахунок непрямих джерел доходу. Усі популярні браузери або можна встановити безкоштовно, або ж вони вбудовані в ту чи іншу операційну систему. Нагадаємо, що Internet Explorer вбудований в Microsoft Windows, починаючи з Windows 98, а Safari інтегрований в Mac OS. Відповідно, конкурувати виробникам інтернет-браузерів з використанням економічних важелів впливу неможливо.

Найчастіше користувачі віддають перевагу тому чи іншому браузеру через красивий інтерфейс, швидкість і зручність в роботі або наявність якихось розширень. Отже, у хід йдуть інші методи боротьби «за серце користувача» - з використанням таких, вельми претензійних, гасел як «найшвидший браузер», «найзручніший браузер», «самий функціональний браузер», «самий налаштовуваний браузер» та інші. Часто вибір використовуваного браузера для повсякденної роботи - це справа багаторічної звички або сліпа віра рекламі виробника браузера, або віра в ідеали в області розвитку вільного Інтернету, які ставлять перед собою виробники браузерів, чи авторитетну думку знайомих фахівців, або навіть бажання постійно пробувати щось нове.

При цьому часто забувається або спеціально замовчується про ступінь безпеки самого браузера. Адже безпосередньо через браузер ми переглядаємо вміст веб-сайтів. Через браузер ми заходимо на сайти інтернет-банків, оплачуємо товари і послуги, користуємося онлайн-сервісами або обмінюємося конфіденційною інформацією. Саме на браузер лягає первинна відповідальність за безпеку в Мережі. Так чому ж ми так мало про це замислюємося?

Розглянемо порівняння з точки зору безпеки чотири найпопулярніші браузери для платформи Microsoft Windows (в алфавітному порядку): Google Chrome 16.0, Microsoft Internet Explorer 9, Mozilla Firefox 9.0, Opera 11.11.

При цьому не віддаватимемо переваги жодному з них, так як кожен функціонал, достатній для всіх повсякденних інтернет-задач, з якими стикається більшість користувачів.

Нижче, для кожного браузера, наведемо ту інформацію, на якій акцентують свою увагу виробники браузерів з приводу безпеки їх продуктів для інтернет-серфінгу, бо подача такої інформації багато в чому виявляє пріоритети цих виробників в реалізації технологій безпеки в продуктах, які випускаються ними. При цьому буде запропонований огляд інформації, наведеної на офіційних сайтах відповідних браузерів, без поглиблення в технічні блоги розробників та іншу інформацію подібного роду, оскільки користувачі зазвичай керуються саме інформацією, розташованої на офіційних сайтах.

Google Chrome

Сайт Google, присвячений огляду можливостей безпеки браузера Google Chrome, є досить лаконічним. У ньому йдеться про те, що в даному браузері існує захист від шахрайських і фішингових сайтів, зосереджена в технології «Безпечний перегляд».

Також виділяється функціональна можливість під назвою «пісочниця» (в англомовних матеріалах відповідне терміну sandboxing), за допомогою якого браузер може запобігти установці в системі шкідливих програм, а також має можливість відстежити вплив коду, що виконується в одній вкладок браузера, на вміст інших відкритих вкладок. У Chrome 12 з'явився фільтр шкідливих файлів на основі репутаційних технологій, який при подальшому розвитку може скласти конкуренцію технології Application Reputation від Microsoft.

З англомовних джерел можна дізнатися про забезпечення безпеки більш докладно. Зокрема, в Google Chrome існує технологія забезпечення безперервності HTTPS-з'єднання та захисту його від компрометації, захист від XSS-атак та інші корисні функції.

Microsoft Internet Explorer

Компанія Microsoft, говорячи про безпеку свого браузера, в першу чергу робить упор на фільтрацію ActiveX-вмісту. Загалом, проблема небезпечного ActiveX-вмісту актуальна саме для даного браузера, тому що без додаткових плагінів в конкуруючих браузерах взаємодія з активним вмістом, розташованим на інтернет-сторінках, проводиться за допомогою інших технологій.

Також акцент робиться на протидію XSS-атак, перегляд в приватному режимі InPrivate і функція захисту від стеження. Також реалізовано виділення домену другого рівня в адресному рядку браузера, жирним кольором, що дозволяє легко визначити, чи знаходиться користувач на цьому сайті, на який хотів зайти, або ж на шахрайському, адреса якого дуже схожа на адресу цього сайту.

Як унікальна функціональна особливість безпеки вказується широко рекламований фільтр SmartScreen, який в 9-ій версії Internet Explorer має можливість фільтрувати не тільки шкідливі сайти по URL, а й, власне, шкідливі файли за допомогою технології Application Reputation, яка заснована на репутаційних технологіях.

Слід зауважити, що актуальна версія Internet Explorer, значно поліпшена в плані підвищення стандартів інформаційної безпеки в порівнянні з попередніми версіями даного браузера, і його цілком можна рекомендувати до використання початківцям інтернет-користувачам для здійснення операцій інтернет-банкінгу

та інших потенційно- небезпечних операцій при чіткому дотриманні рекомендацій виробника.

Mozilla Firefox

Розробники браузера Firefox традиційно приділяють безпеці свого браузера пильну увагу. Тому інформація про функції безпеки цього браузера на його офіційній сторінці досить розлога.

Зокрема, якщо пробігтися по заголовкам врізок відповідного розділу інформації про браузер, можна дізнатися і про підтримку розширених EV-сертифікатів, і захист від XSS-атак, і про інтеграцію з батьківським контролем Windows 7, про функції «Приватний перегляд», інтеграцію з антивірусними продуктами, про фільтр шкідливих сайтів, захист від стеження за діями користувача в Інтернеті за допомогою спеціальних скриптів, що розміщуються на інтернет-сторінках, і підтримки HTTPS-з'єднань.

При розгляді даного браузера слід також звернути увагу на те, що розробники роблять ставку на широке використання функціональних доповнень (так званих розширень), які створюються сторонніми розробниками. За допомогою цих додатків можна значно підвищити безпеку використання даного браузера. Таким чином, браузер є ідеальним конструктором для користувачів, які володіють достатніми знаннями з інформаційної безпеки та точно знають, що хочуть отримати від браузера.

Opera

На закінчення розглянемо інформацію з безпеки, яку пропонують кінцевому користувачу розробники браузера Opera. Як і розробники Google Chrome, виробники Opera на офіційному сайті браузера в цьому питанні гранично лаконічні.

Зокрема, заявляється про існування фільтра від шкідливих інтернет-сайтів, режим приватного перегляду, підтримку розширених сертифікатів сайтів, і управлінні завантажуваними cookies.

Технології безпеки	Google Chrome 16.0	Microsoft Internet Explorer 9	Mozilla Firefox 9.0	Opera 11.11
Автоматичне оновлення браузера	Є	Є	Є	Є
Підтримка HTTPS-з'єднань і візуалізація безпечного з'єднання	Є	Є	Є	Є
Захист від компрометації HTTPS-з'єднань	Є	Частково	Немає	Немає
Підтримка EV-сертифікатів	Є	Є	Є	Є
Механізм захисту від XSS-атак	Є	Є	Є	Немає
Фільтр заражених сайтів по URL	Є	Є	Є	Є
Фільтр шкідливого програмного забезпечення	Є	Є	Частково	Немає
Режим приватного перегляду	Є (Режим інкогніто)	Є (Режим InPrivate)	Є (Приватний перегляд)	Є (Режим приватності)
Захист від стеження	Немає	Є	Є	Немає
Підтримка ASLR	Виконуваний файл і DLL-бібліотеки	Виконуваний файл і DLL-бібліотеки	Виконуваний файл і DLL-бібліотеки	Виконуваний файл і DLL-бібліотеки

Пробіжимося рядками поданої вище таблиці і розглянемо деякі нюанси.

Підтримка роботи з EV-сертифікатами, наявність режиму приватного перегляду, а також можливості з'єднань з веб-сайтами через захищений протокол HTTPS - все це реалізовано в усіх порівнюваних браузерах.

З захистом від компрометації HTTPS-з'єднання ситуація дещо гірша. З відомих технологій з даного приводу можна згадати тільки можливість стеження за безперервністю HTTPS-з'єднань у Google Chrome і закріплені сайти (pinned sites) в Internet Explorer 9 при використанні спільно з Windows 7.

Ця функція заснована на тому, що користувачі в більшості випадків набирають в адресному рядку сайту лише його домен (наприклад, domain.com), без вказівки протоколу, за яким необхідно з'єднуватися (http:// або https://). В цьому випадку браузер спочатку з'єднується з веб-сервером через протокол HTTP. Якщо сервер при цьому підтримує HTTPS-протокол, і на ньому налаштований автоматичний редирект на цей безпечний протокол, то тільки лише тоді відбувається редирект з HTTP-протоколу на HTTPS. На думку фахівців Microsoft, цього часу, який йде на редирект між HTTP-і HTTPS-протоколу може бути достатньо для проведення атаки. Використання закріплених сайтів зручно лише для невеликого набору найбільш важливих сайтів. Тому в таблиці дана технологія для IE9 відзначена як підтримувана частково.

Фільтр шкідливих сайтів за їх URL до цього часу також присутній у кожному поважаючому себе браузері, але такий стан речей виник відносно недавно. Не беремося судити про якість реалізації і ефективність даного функціоналу в браузерах, так як це вимагає проведення ряду порівняльних тестів.

З технологіями фільтрації небезпечних сайтів по URL взагалі все далеко не однозначно. Така функція є в усіх браузерах, але якість роботи такого функціоналу залежить безпосередньо від використовуваних баз і якості фідбек з користувачами, які беруть безпосередню участь у наповненні відповідних баз, розташованих в хмарах вендорів або їх партнерів. Наприклад, Firefox (детальніше: http://www.mozilla.com/en-US/firefox/releases/1.5.html # FAQ) для блокування шкідливих сайтів користується хмарами Google. Фактично, інформація про нові шкідливі сайти, які можна відправити за допомогою Firefox, відправляється в компанію Google, і браузер користується відповідними репутаційними технологіями. Решта браузерів використовують власні репутаційні технології, ефективність яких може істотно розрізнятися, і це тема для спеціальних досліджень.

Окремо варто сказати про захист від встановлення в системі шкідливих програм, по суті, про антивірусний функціонал на рівні браузера. Вона реалізована тільки в Internet Explorer 9. Фільтр SmartScreen, вбудований в цей браузер, оцінює репутацію для завантажуваних з Інтернету файлів. Детальніше про неї можна прочитати в огляді засобів безпеки Internet Explorer 9, який вийшов раніше. У Google Chrome реалізована пісочниця (sandboxing), яка в версії 12 отримала підтримку у вигляді нового компонента, що відповідає за перевірку завантаження на шкідливість за допомогою репутаційних технологій

і вже виглядає як повноцінна технологія фільтрації шкідливих програм, що завантажуються засобом браузера. Можливості Mozilla Firefox, на жаль, заслуговують лише половинчастого результату.

Слід зазначити, що репутаційні технології перевірки файлів, реалізовані в Google Chrome 12 на поточний момент виглядають сирими. Якщо провести невеличкий експеримент, задавши звичним рухом пошуковій системі запит «аватар скачати на великій швидкості» і через кілька кліків можна знайти свіжу модифікацію лже-архіву, що вимагає за «розпакування» відіслати гроші зловмисникам. IE9 вивів повідомлення про те, що файл «завантажується незвичайним чином». Chrome 12 теж кілька секунд перевіряв файл у своїй «хмарі», але повідомлення про те, що файл не підписаний і у нього немає видавця, вивела операційна система, а не браузер. Так що новому фільтру завантаження від Google повноцінна одиниця в підсумковій таблиці виставлена з надією на подальший розвиток даного функціоналу. Принаймні, Chrome виявився першим браузером після IE, де такий функціонал з'явився.

Що стосується автоматичного оновлення браузерів, то зазвичай під цим мається на увазі встановлення нових мінорних версій, що закривають виявлені вразливості і підвищують стабільність веб-клієнтів. Автоматичний перехід на нову мажорну версію браузерів зазвичай пов'язаний з явною вказівкою на подібне бажання від користувача. У зв'язку з цим інтернет-користувачам можна порадити погоджуватися на такі пропозиції, хоча це і може привести до того, що доведеться звикати до нового зовнішнього вигляду і функціоналу браузера, що полюбився. Також не завадить стежити за новинами (або підписатися на них), які публікуються на офіційному сайті виробника використовуваного браузера.

Невеликим сюрпризом виявилася підтримка технології ASLR (Address Space Layout Randomization, рандомізація розміщення адресного простору) всієї четвіркою популярних браузерів в реалізації для платформи Windows як для виконуваного файлу, так і для завантажуваних DLL-бібліотек. Це говорить, що розробники веб-браузерів для Windows «тримають руку на пульсі» і дотримуються рекомендацій Microsoft при створенні безпечних додатків.

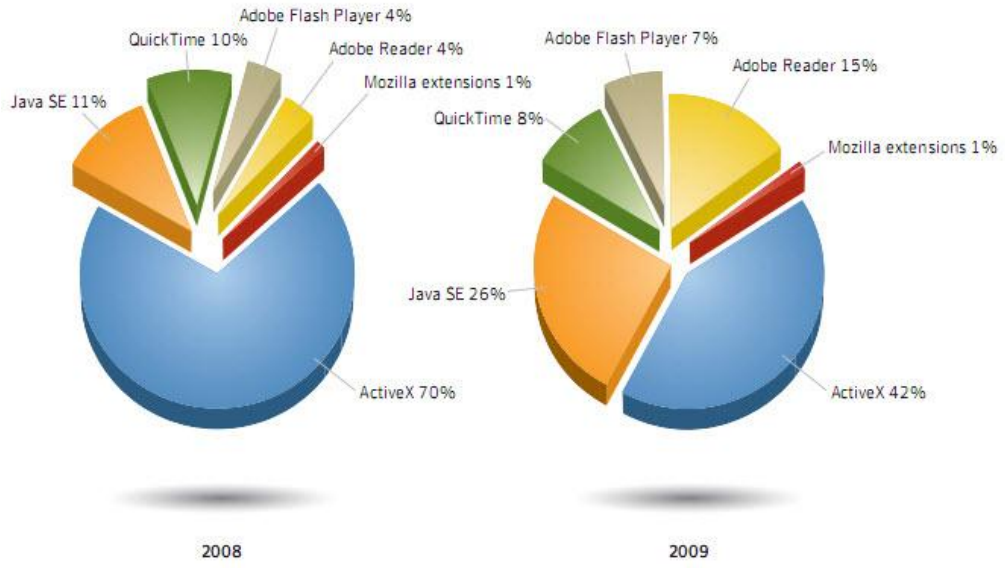
Що стосується нової модної функціональної можливості, що входить до підсистеми безпеки інтернет-браузера, під назвою «захист від стеження», то вона заявлена всього в двох описуваних продуктах - Internet Explorer і Mozilla Firefox. Подібні функції дозволяють припиняти передачу даних про відвідування користувачем сайтів в різні рекламні агентства та маркетингові відділи компаній, яка відбувається за допомогою спеціальних скриптів, впроваджуваних в рекламні оголошення і просто в код веб-сторінок. Про цю функції в IE9 докладно написано в огляді Internet Explorer 9, який вийшов раніше (http://anti-malware.ru/reviews/Internet_Explorer_9). У Mozilla Firefox 5 функція включається в розділі «Конфіденційність», налаштувань браузера,

відповідне встановлення називається «Повідомляти веб-сайтам, що я не хочу, щоб за мною стежили».

В цілому в таблиці виділяється Microsoft Internet Explorer, не сильно від них відстають Mozilla Firefox і Google Chrome, Opera замикає список. Однак тут варто повторитися, що ця таблиця не є результатом серйозного тестування, тому розставлені в результаті місця є суб'єктивними. Головна ж наша мета - привернути увагу користувачів не тільки до зручності і швидкості роботи браузерів, але також до захисту забезпечуваними ними інструментами безпеки при веб-серфінгу та захисту конфіденційної інформації. А її довіряють браузерам кожну секунду мільйони користувачів у всьому світі.

Версії браузерів змінюються надто швидко і вже завтра ми можемо отримати нову поживу для роздумів, як від зловмисників, так і від виробників браузерів, а «баланс сил» може змінитися в ту чи іншу сторону [3].

Фахівці Symantec в 2009 році задокументували 321 уразливість в надбудовах браузерів, і хоча це на третину менше, ніж роком раніше, легше від цього не стає. Лідирує в цьому сумному рейтингу технологія ActiveX, яка розроблена Microsoft, і навіть дворазове зниження кількості вразливостей, виявлених в надбудові ActiveX, не надто обнадіює.

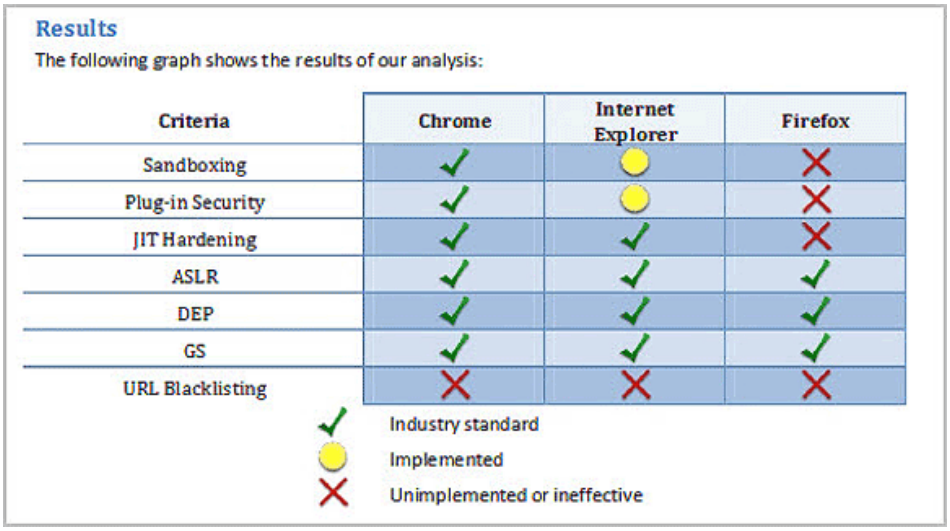


Вразливості в надбудовах браузерів за 2008 - 2009 роки (дані Symantec)

З ActiveX все сумно настільки, що три уразливості були виявлені в програмі iDefense COMRaider, яка використовується фахівцями для ... виявлення вразливостей ActiveX! Тому рекомендується, по можливості, утримуватися від встановлення надбудов, що використовують цю технологію. Що ж до інших завсідників списку проблемних додатків, то їх треба не просто знати, а і оновлювати на першу вимогу. Це Adobe Reader і Flash Player, платформа Java і Apple QuickTime [4].

В останніх дослідженнях фірми Accuvant кінця 2011 року Firefox відстає від браузерів Google Chrome і Internet Explorer в декількох ключових областях.

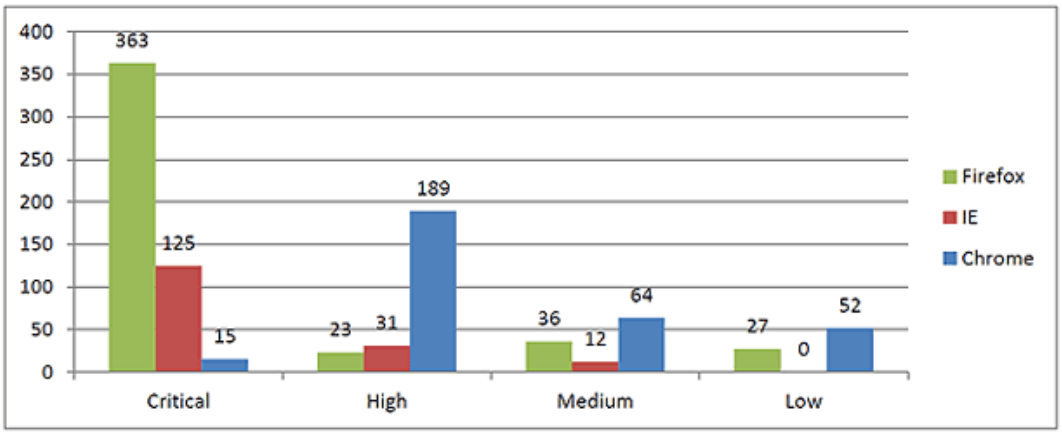
Доповідь фірми Accuvant, яка займається інформаційною безпекою, приводить до висновку, що Firefox Mozilla не вистачає, коли мова заходить про сучасні гарантії безпеки.
Доповідь була профінансована Google, але Accuvant є поважною фірмою з IT-безпеки, а доповідь видається справедливою і точною.
Ось декілька результатів дослідження [5]:



Було знайдено, що Firefox не вистачає безпеки в трьох ключових областях:

- Sandboxing (пісочниця)- технологія, яка обмежує, наскільки багато експлойтів отримують доступ на цільовій машині.
- Just-In-Time (JIT) hardening – технологія, яка запобігає компіляції шкідливого коду JavaScript з веб-сайту на цільовому комп'ютері.
- Plug-in security - обмежує, наскільки доступні плагіни, а також запобігає завантаженню шкідливих додатків.

Firefox також очолив список, коли справа дійшла до критичних вразливостей



Висновки доповіді не роблять комфортним їх читання для шанувальників Firefox:

- Обидва інші браузери Google Chrome і Microsoft Internet Explorer реалізували сучасні анти-експлуатаційні технології, а Mozilla Firefox відстає без JIT-оновлення. Хоча і Google Chrome і Microsoft Internet Explorer реалізували однаковий набір анти-експлуатаційних технологій, плагіни безпеки Google Chrome і архітектура пісочниці реалізуються на більш ретельній і всеохоплюючій основі.

Тому в докладі робиться висновок, що Google Chrome є браузером, який найбільш захищений від нападу.

Нижче розглянемо, як на практиці реалізувати задекларовану безпеку кожного з чотирьох популярних браузерів.

НАЛАШТУВАННЯ БЕЗПЕКИ INTERNET EXPLORER 9

У багатьох сучасних досвідчених користувачів комп'ютерів, за довгі роки виробилося негативне ставлення до цього браузеру, який з досить давніх часів вбудований в операційну систему Microsoft Windows, та і зараз є частиною Windows - це видно навіть у повній офіційній назві браузера - Windows Internet Explorer 9.

Власне, це негативне ставлення мало цілком об'єктивні передумови. По-перше, присутній певний елемент нав'язування використання цього браузера, який за замовчуванням встановлюється в систему, і лише в країнах Євросоюзу користувачі можуть на етапі встановлення Windows вибрати браузер, який буде встановлений. По-друге, частка Internet Explorer (або скорочено IE) на ринку браузерів, за даними на початок 2011 року, перевищувала 40%, а значить, він є привабливим для шкідливих атак, орієнтованих саме на цей інтернет-браузер.

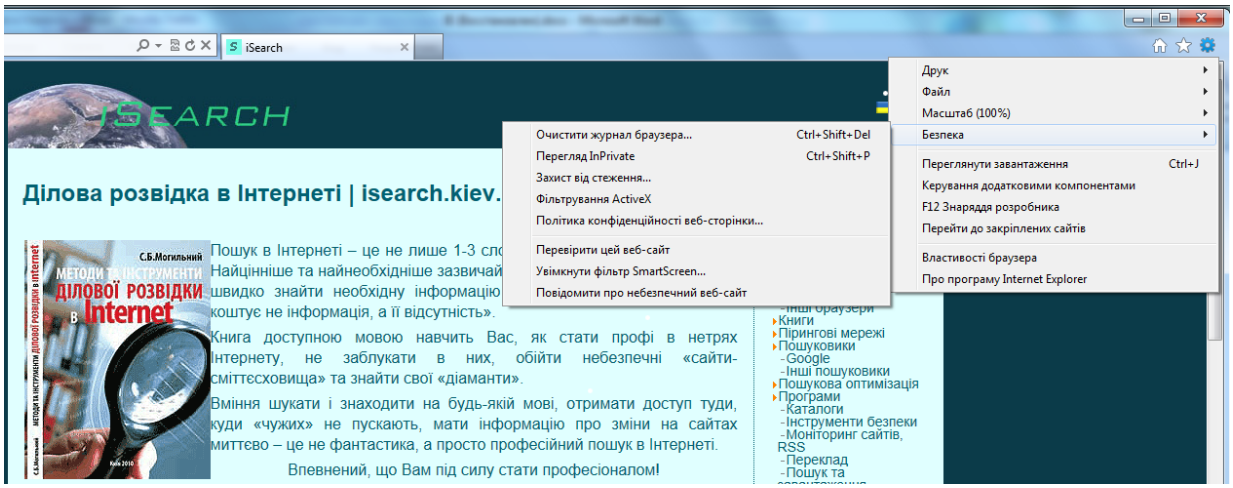
До розробки IE9 з самого початку були пред'явлені високі вимоги. Нова версія браузера розроблялася у повній відповідності з політикою Microsoft SDL (Security Developmment Lifecycle, процес створення безпечного ПЗ), що, з досвіду розробки інших продуктів з використанням даної політики, істотно знижує кількість потенційних вразливостей.

Отже, перелічимо коротко, які ж нові механізми безпеки пропонує нам Internet Explorer 9:

• Фільтрація завантажуваних додатків (SmartScreen Application Reputation);
• Фільтрація ActiveX;
• Закріплені сайти (pinned sites);
• Захист від стеження;
• Поліпшений захист пам'яті;
• Зміни в системі оповіщення;
• Приватний інтернет-серфінг (режим InPrivate);
• Фільтр запуску міжсайтових сценаріїв

До речі, якщо врахувати той факт, що IE9 можна встановити тільки на Windows Vista/7 і Windows Server 2008/2008 R2, то внаслідок необхідності переходу з Windows XP та раніших версій Windows на сучасні їх аналоги більша кількість користувачів виявляться більш захищеними при роботі в Інтернеті. Адже в нових версіях Windows реалізовані нові механізми забезпечення безпеки, які будуть додаватися до можливостей IE версії 9.

Більшість засобів безпеки вмикаються і доступні через кнопку «Знаряддя» (крайня праворуч) на верхній панелі браузера:

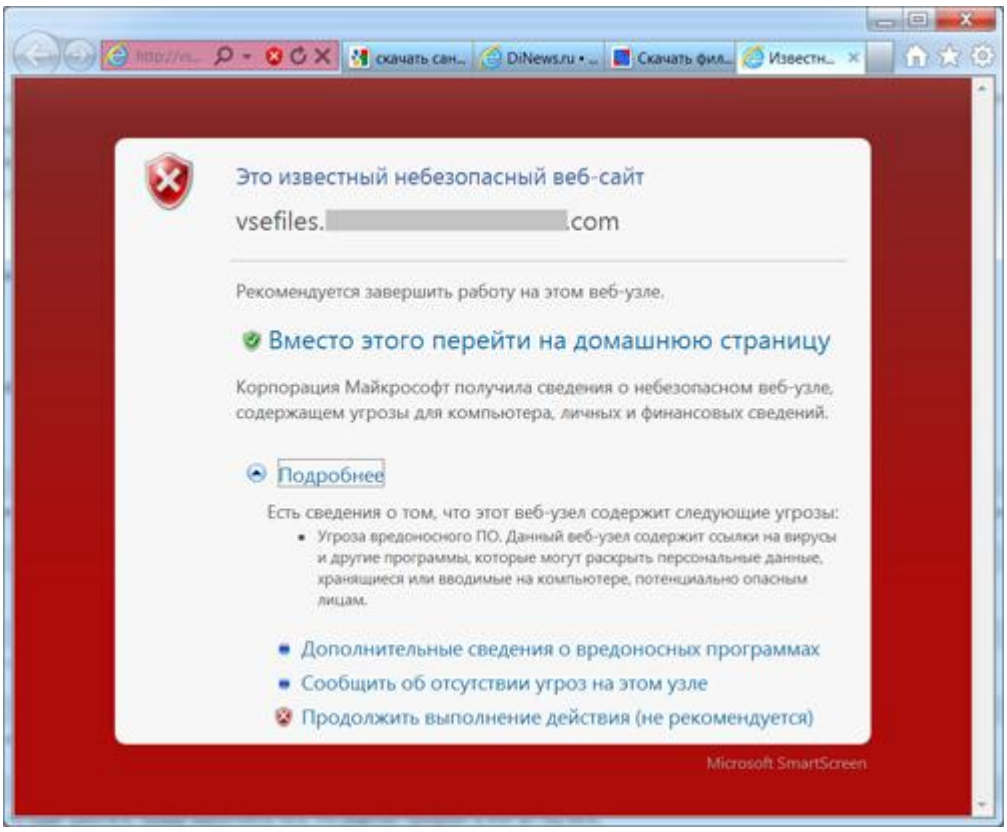


Розглянемо всі перераховані вище нововведення більш докладно, в тому числі, і як ними скористуватися:

Фільтрація завантажуваних додатків

Якщо фільтрацією небажаних і шкідливих сайтів вже складно здивувати середнього користувача інтернет-браузера, і в багатьох популярних браузерах така функція існує і більш-менш ефективно працює, то фільтрація завантажуваних додатків, реалізована в IE9, - це нове явище з дуже великим потенціалом. І старі, і нові можливості фільтрації сайтів та завантаження реалізовані в IE в рамках компоненту SmartScreen.

SmartScreen блокує шкідливий сайт:



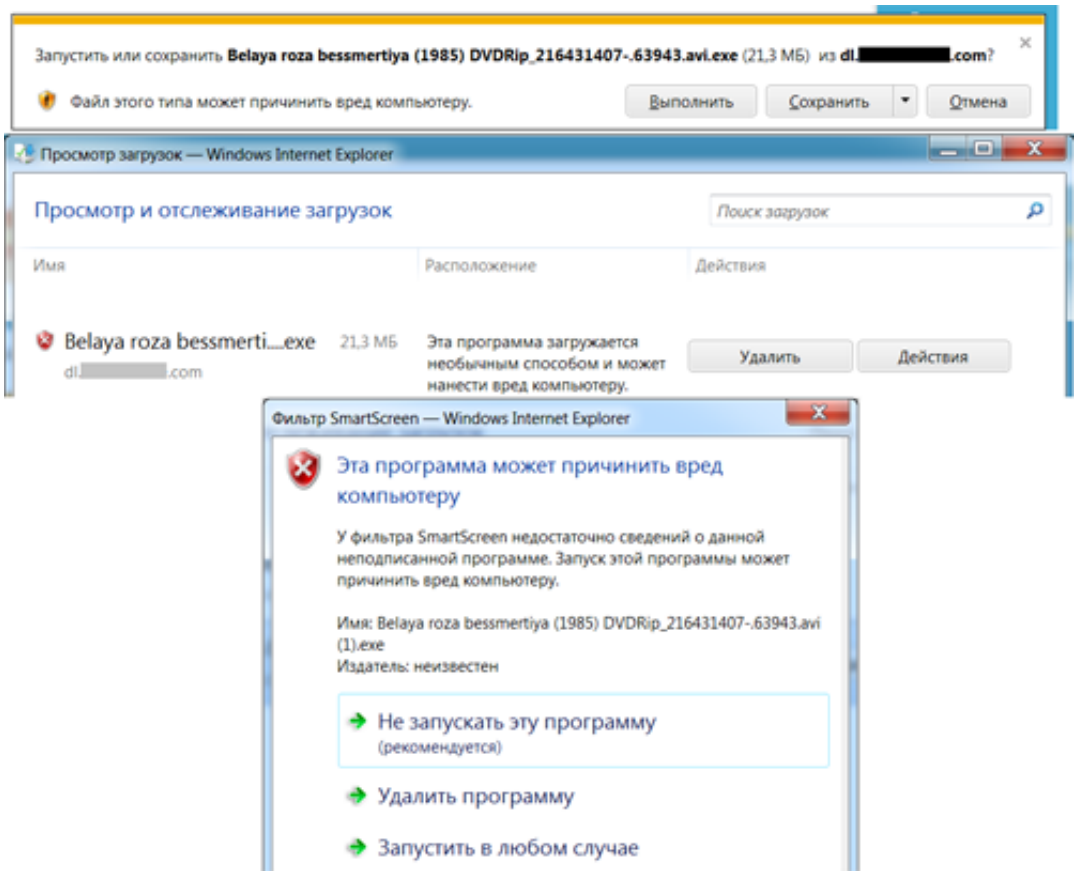
Для визначення репутації завантажуваної користувачем програми використовується безліч алгоритмів, які враховують такі критерії як результат перевірки антивірусом, кількість завантажень, історія завантажень, а також репутація адреси сайту, з якого відбувається завантаження. В якості вхідних параметрів для цих алгоритмів використовується хеш завантаження і цифровий сертифікат, який був використаний для підпису файлу (якщо він підписаний).

Якщо з тих чи інших критеріїв, якими керується SmartScreen, завантаження буде визнане небезпечним, користувачеві будуть виводитися відповідні повідомлення - в спливаючих повідомленнях внизу вікна браузера, в менеджері завантажень і при спробі запустити підозрілий додаток з менеджера завантажень.

Нижче, як приклад, приведена спроба завантаження і запуску підробленого архіву, який просить відправити гроші зловмисникам для завершення розпаковування файлу - сьогодні нарватися на подібні сайти труднощів не становить. На скріншотах показані повідомлення, які виникають у цьому випадку.

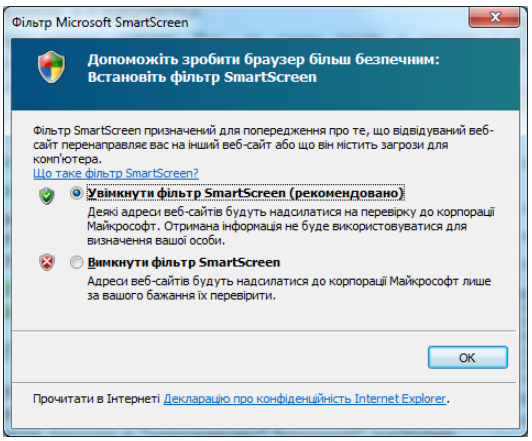
Можливо, не всі відразу звернуть увагу, але реакція в даному випадку йде також і на подвійне розширення файлу - *.avi.exe - браузер повідомляє, що файл цього типу може заподіяти шкоду комп'ютеру. Тобто, мова йде дійсно про цілий набір правил, за результатами відповідності яким видається та чи інша резолюція.

Повідомлення при завантаженні підозрілої програми:



У цих повідомленнях можна побачити формулювання: «Ця програма завантажується незвичайним способом і може завдати шкоди комп'ютеру». Хоча може здатися, що в даному випадку мова йде саме про незвичайний спосіб завантаження файлу з сайту, але насправді все трохи інакше. Фільтр SmartScreen перевіряє файл за списком програм, які завантажують багато користувачів IE, а також за списком відомих небезпечних програм. І з аналізу присутності файла в обох списках виводиться подібне повідомлення.

За умовчуванням фільтр SmartScreen і його рекомендується цвімкнути:



Можна довго сперечатися про вдалий чи невдалий перекладу термінів російською мовою, але при цьому дана функція може підняти рівень безпеки інтернет-серфінгу на новий рівень. Дійсно, наприклад, деякі виробники антивірусних програм вже сьогодні пропонують користувачам включати фільтр запуску непідписаних додатків, який часто інтегрується також з репутаційними технологіями. IE9 пропонує вже на етапі завантаження програми перевіряти його на наявність підпису, і в разі відсутності такого (при відсутності програми в списках довірених) виводить користувачеві відповідне повідомлення. Подібні функції, які з'являються в браузерах, при ефективному їх використанні, можуть дозволити в найближчому майбутньому для багатьох користувачів зробити достатнім використання безкоштовних антивірусних продуктів. Це припущення підкреслює і статистика, яку пропонує Microsoft.

Зокрема, згідно цій статистиці ризик для середнього користувача завантажити файл, який виявиться шкідливим, знаходиться в межах від 25 до 40 відсотків. При цьому дослідження показали, що близько 90% («хороших») додатків в даний час визначаються IE9, як мають достатню репутацію, по хешу файлу і цифровому підпису. 7% файлів, що завантажуються за допомогою Internet Explorer, в майбутньому визначаються як шкідливі. Частина цих атак зупиняються за допомогою фільтра адрес сайтів SmartScreen. При цьому зрозуміло, що будь-яка технологія, яка базується на списках блокування, не може дати 100%-ної ефективності. І в цьому сенсі фільтр завантажуваних додатків, заснований на репутаційних технологіях, може істотно підвищити ефективність фільтра SmartScreen для тих програм, які ще не визначаються як відомі шкідливі програми.

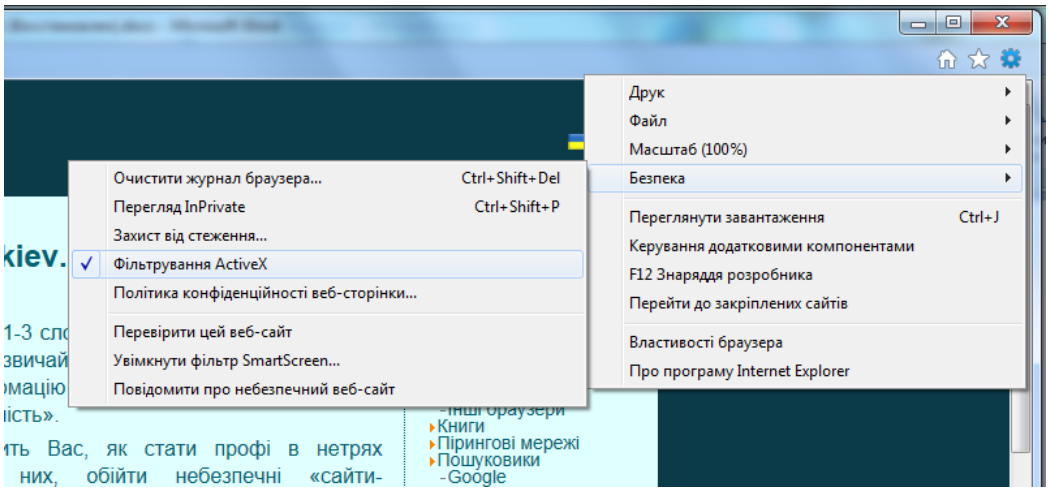
В іншому джерелі фахівці Microsoft пропонують іншу цікаву статистику:

- 90% користувачів бета-версії і реліз-кандидата IE9 ніколи не бачили попередження про те, що завантажується підозріла програма, тому що завантажували програми, які визначалися як довірені;
- від 20 до 40% завантажених файлів, які визначаються IE9 як підозрілі, зрештою признаються шкідливими. Це ті шкідливі програми, які обходять усі існуючі рішення і могли бути запущені користувачами у своїх системах, якби не були попереджені;
- 95% до цього невизначених шкідливих файлів були видалені користувачами після того, як SmartScreen показав попередження.

Загалом-то, ця статистика виглядає цілком правдоподібною, і є всі підстави припускати, що користувачі Internet Explorer гідно оцінять новий фільтр додатків.

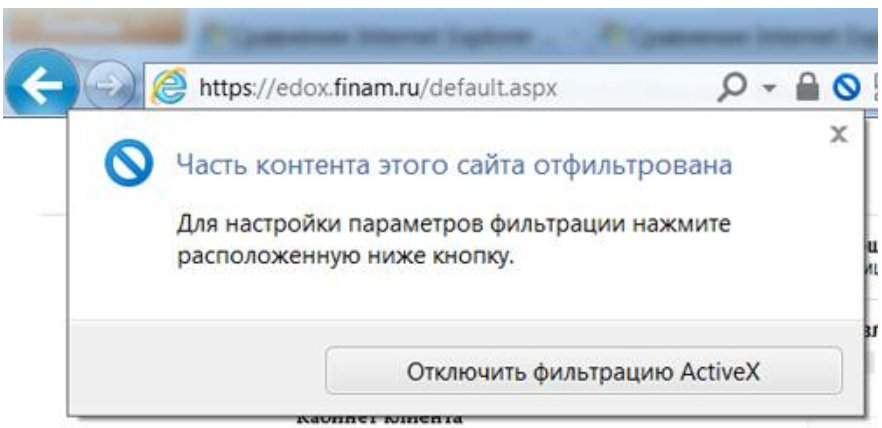
Фільтрація ActiveX

Internet Explorer 9 в своєму складі містить фільтр ActiveX-об'єктів, розміщених на сторінках сайтів. Зокрема, за допомогою ActiveX-об'єктів на сторінки впроваджуються flash-та інші відеоролики, інші складні за будовою об'єкти. Оскільки досить часто в додатках, які використовують ActiveX для впровадження власних об'єктів на сторінках веб-сайтів, виявляються уразливості, розробники IE9 вирішили перекрити цей канал, популярний серед зловмисників, за допомогою фільтра ActiveX. За замовчуванням він відключений, але якщо його включити, то жоден ActiveX-об'єкт на веб-сторінках працювати не буде, поки користувач в явному вигляді його не дозволить:



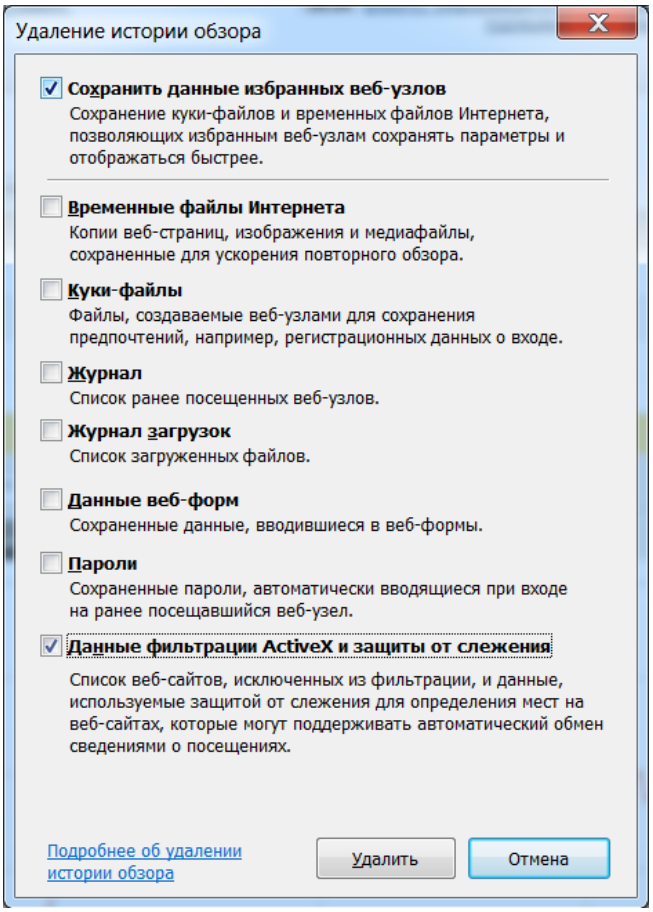
Дозволити використання ActiveX-об'єктів на конкретній сторінці можна, натиснувши на синє перекреслений коло, яке присутнє в повідомленні, що з'явилося, про те, що частина контенту сайту відфільтрована, натиснувши на кнопку «Відключити фільтрацію ActiveX». При цьому браузер запам'ятає, що для цього сайту використання ActiveX дозволене. Аналогічним чином можна і виключити файл зі списку довірених для обговорюваного фільтра.

Internet Explorer 9 відфільтрував ActiveX:



Видалити список сайтів, для яких включена фільтрація, можна, вибравши в налаштуваннях браузера пункт Безпека - Очистити журнал браузера і вибравши прапорець «Дані фільтрації ActiveX і захисту від стеження».

Видалення списку сайтів, довірених для відображення ActiveX:



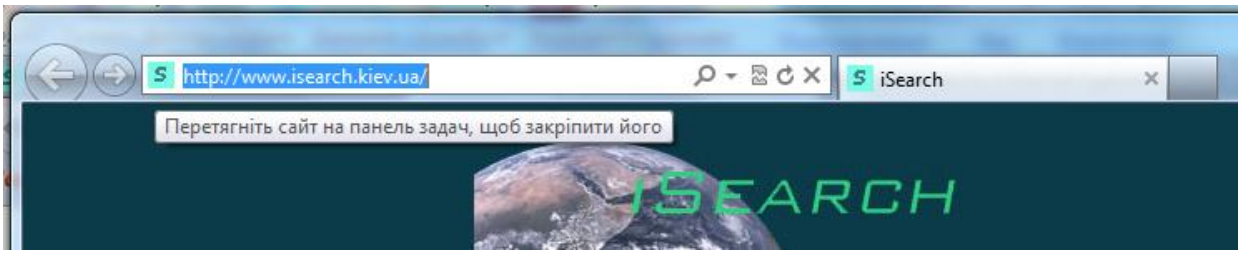
Наскільки можна бачити, фільтр ActiveX знаходиться в зародковому стані, на початку свого розвитку. Зокрема, для кожного сайту можемо або заборонити відображення всіх ActiveX-об'єктів, або дозволити - IE9 пропонує нам налаштувати параметри фільтрації для відображуваного сайту, але на ділі можемо лише включити для нього фільтр або вимкнути. Вибірково дозволити або заборонити певний тип ActiveX-об'єктів користувач не зможе, так само як і немає повноцінного редактора списку довірених сайтів. Якщо ми захочемо видалити який-небудь сайт зі списку довірених для даного фільтра, то ми повинні або зайти на нього і тим же способом, як і включали до списку, видалити сайт зі списку довірених, або ж повністю очистити список довірених сайтів. В останньому випадку ми повинні будемо також видалити і дані, які використовуються захистом від стеження, про яку мова піде нижче.

При цьому фільтр ActiveX, як здається, передчасно, розробниками IE9 називається більш загальним рішенням, ніж такі плагіни як Flashblock (для Mozilla Firefox) або ClickToFlash (для Safari).

Цілком ймовірно, що даний фільтр буде розвиватися в наступних версіях браузера.

Закріплені сайти

Для користувачів Windows 7 розробники IE9 приготували ще один сюрприз під назвою «закріплені сайти» (pinned sites), який повинен зробити інтернет-життя користувачів значно безпечнішим. Щоб створити і використовувати закріплений сайт, користувачеві Windows 7 досить відкрити його у браузері, потім перетягнути вкладку, яка відповідає сайту, на Панель завдань.



При цьому на значку кнопки, що з'явиться в Панелі завдань, буде відображено логотип відповідного сайту, а не логотип Internet Explorer.

Які ж переваги дає користувачеві IE9 використання закріплених сайтів? Розробники виділяють цілих п'ять:

1. Коли сайт винесений на Панель завдань у вигляді окремої кнопки, користувач може запускати його безпосередньо з цієї кнопки. Таким чином, можна уникнути переходу на такі сайти за посиланнями з фішингових листів, метою яких є відправити користувача на підроблений сайт, схожий лише зовні на той сайт, на який звик заходити користувач. Також запуск з окремою кнопки виключає ймовірність зробити помилку при наборі адреси сайту в адресному рядку браузера і також потрапити на шкідливий сайт - зловмисники часто реєструють домени, які з написання відповідають друкарським помилкам, які найчастіше зустрічаються при наборі адрес відомих сайтів.

2. Закріплені сайти відкриваються в окремій сесії браузера. Це означає, що ймовірність атаки знижується за рахунок того, що куки, активні в основному вікні браузера, недоступні в сесії, яка створена для закріпленого сайту.

3. Закріплені сайти відкриваються без будь-яких тулбаров і доповнень, а також без BHO (Browser Helper Object, DLL-бібліотеки, що створюються для розширення функціональності браузера). Чим менше запущеного коду, - кажуть розробники IE9, - тим менша ймовірність, що користувач стане метою атаки.

4. Закріплені сайти дозволяють уникнути зайвих редиректів між незахищеним протоколом HTTP і захищеним протоколом HTTPS. Зокрема, коли користувач

набирає адресу сайту вручну, то спочатку сайт відкривається через протокол HTTP, і лише потім відбувається редирект на протокол HTTPS. Ця особливість може збільшити ймовірність атаки. При запуску ж закріпленого сайту з'єднання може відразу проводитися через протокол HTTPS.

5. Використання закріплених сайтів також знижує ймовірність атаки «людина посередині» (man-in-the-middle). Якщо будуть виявлені які-небудь проблеми з сертифікатом, наприклад, він буде підмінений, то з'єднання відразу перерветься з висновком відповідного повідомлення.

Якщо закріплений сайт підписаний сертифікатом класу Extended Validation Certificate (до видачі сайтам таких сертифікатів пред'являються підвищені вимоги), то адресний рядок IE9 буде виділений зеленим кольором.

Виділення зеленим кольором адресного рядка на прикладі сайту «Ощадбанк ОнЛ@йн»:

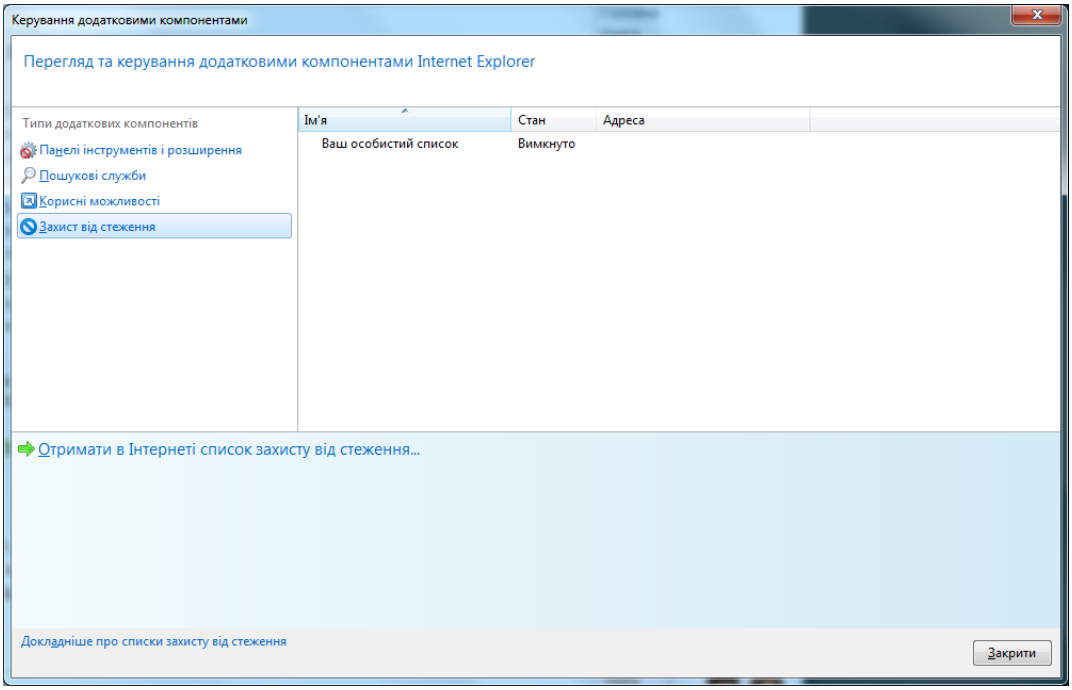
Розробники Internet Explorer настійно рекомендують користувачам 9-ої версії не нехтувати можливостями закріплених сайтів та використовувати цей функціонал для відвідування найбільш важливих для них сайтів, і, судячи з усього, це не позбавлено сенсу.

Захист від стеження (Tracking Protection)

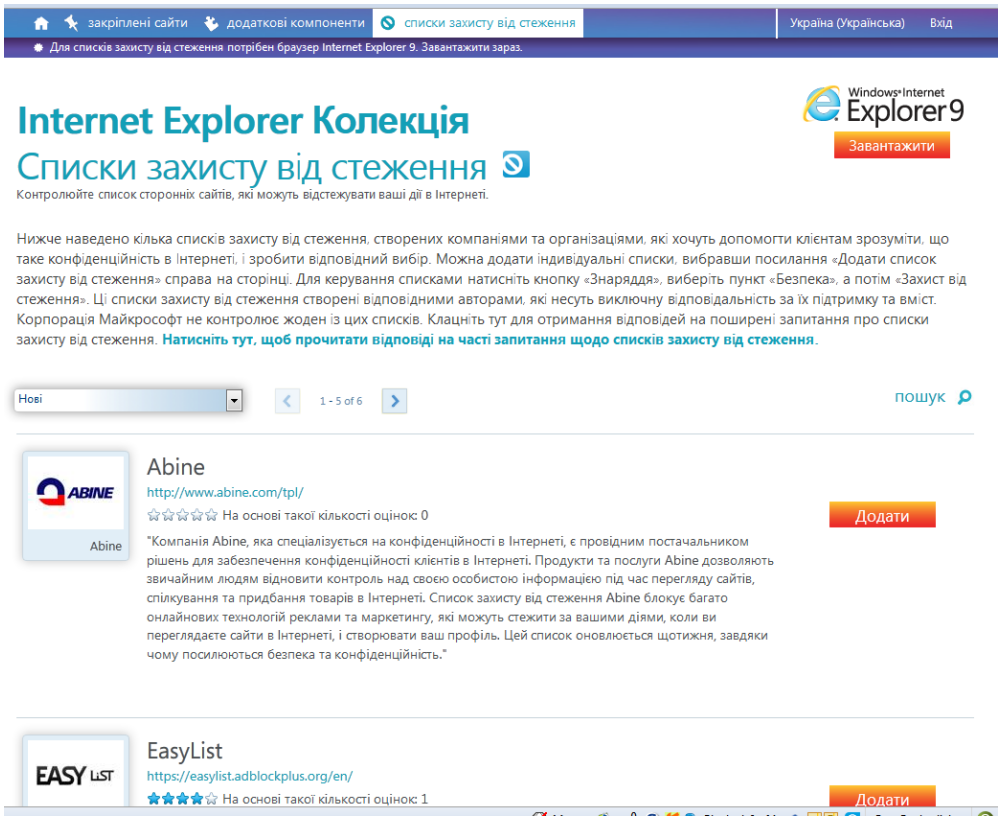
Все частіше в ЗМІ публікуються матеріали про те, що рекламодавці, які публікують свою рекламу на сайтах, або ж автори популярних програм для соцмереж в прихованому режимі збирають інформацію про відвідувачів сайтів. На підставі поведінки користувача на тому чи іншому сайті, частоти відвідування цих сайтів та іншої непрямої інформації можна складати профілі середньостатистичного користувача того чи іншого сайту, користувача того чи іншого додатка в соцмережах. Далі, ця інформація може використовуватися відділами маркетингу деяких компаній, яким продається дана інформація, для своєї успішної діяльності. І це в кращому випадку. У най найгіршому варіанті такі відомості можуть використовуватися для відточування методів соціальної інженерії і при розробці різних шкідливих схем.

Цілком зрозуміло небажання багатьох інтернет-користувачів надавати подібну інформацію третім особам, і розробники Internet Explorer приділяють цій проблемі достатньо серйозну увагу. В IE9 запропонований досить гнучкий

підхід, що дозволяє користувачеві як самостійно створювати список серверів, на які не будуть відправлятися дані про відвідування, так і використовувати ті списки серверів, які пропонують деякі довірені постачальники. При цьому компанія Microsoft не створює і не підтримує такі списки, пропонуючи складати їх незалежним ентузіастам.



Сторінка, на якій можна вибрати списки серверів, що здійснюють спостереження за діями користувачів, від різних виробників:

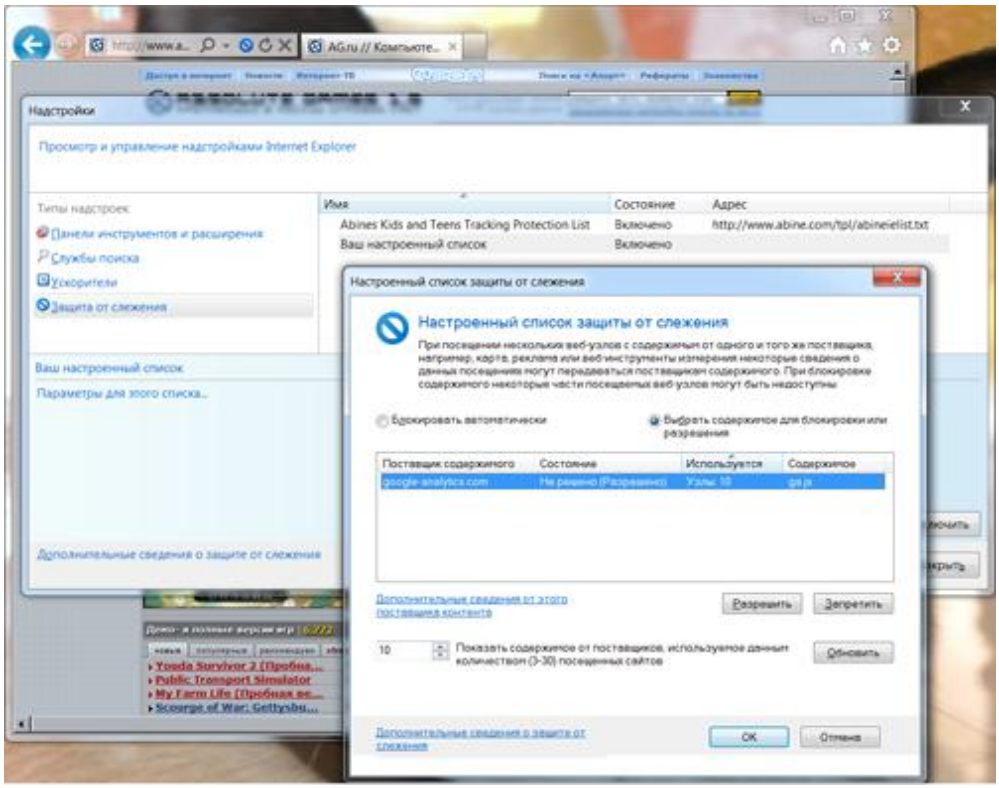


Як мінус існуючої реалізації системи Tracking Protection відзначається невелика кількість серверів, присутніх у пропонованих ентузіастами списках, і не часте їх оновлення. Правда, це може компенсуватися можливістю користувача створювати власний список серверів, які збирають дані про користувачів, і блокувати передачу даних цими каналами.

Розглянемо цю можливість на прикладі ігрового сайту ag.ru. Власний список захисту від стеження можна подивитися, вибравши в налаштуваннях IE9 пункт Безпека - Захист від стеження. При цьому можна помітити, що система захисту від стеження була віднесена до надбудов Internet Explorer.

Якщо в даному вікні вибрати рядок «Ваш налаштований список» і клацнути на посиланні «Параметри для цього списку ...», то буде виведено вікно «Настроєний список захисту від стеження», де буде видно, що на активному сайті ag.ru «розвернувся» складальник інформації під назвою Google Analytics. Відповідно, ми можемо почати дії для того, щоб дані серверу Google Analytics надалі не відправлялися.

Ручне додавання сервера в список захисту від стеження:



Варто зауважити, що цей фільтр працює набагато гнучкіше, ніж фільтр ActiveX, дозволяючи переглядати популярні сайти, на яких рідко обходиться без таких систем збору інформації від користувачів. Тобто, користувач може продовжувати відвідувати ці сайти, але не боятися за те, що за ним пильно спостерігають.

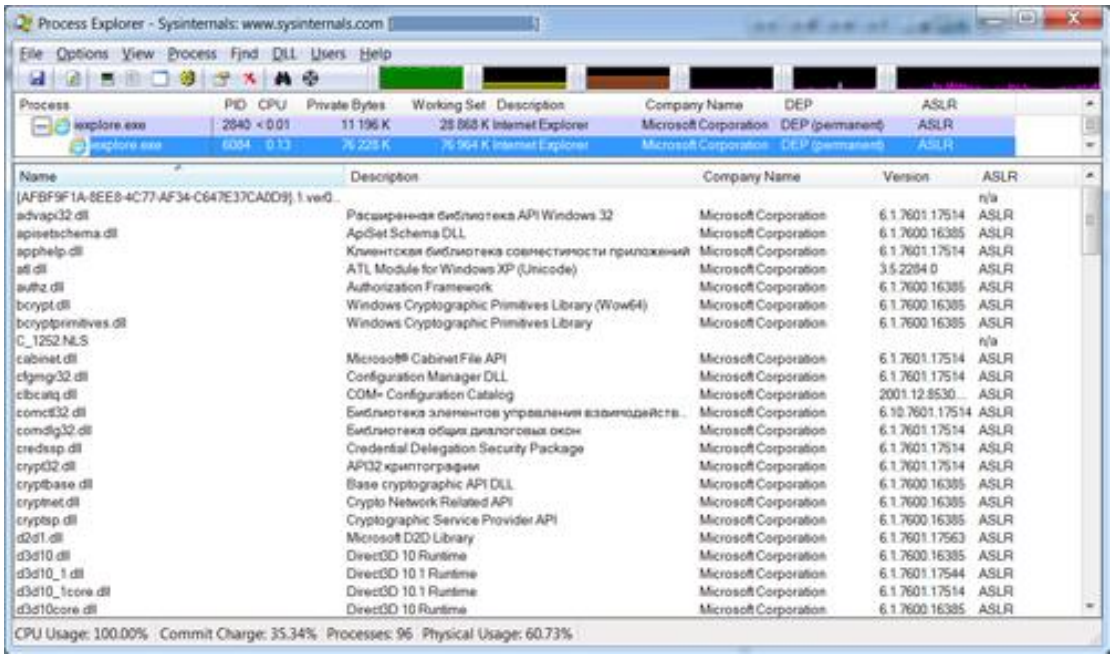
Поліпшений захист пам'яті

На випадок, якщо користувач все таки клюнув на вудку зловмисників і став жертвою одного з методів соціальної інженерії, розробники Microsoft передбачили в IE9 кілька механізмом захисту "останнього рубежу".

В IE9 використовується технологія DEP (Data Execution Protection, запобігання виконання даних), що не дозволяє додаткам виконувати код з області пам'яті, яка призначена тільки для даних і дозволяє запобігти деякі типи атак, що реалізуються за допомогою переповнення буфера (buffer overflow).

Так само, як і раніше, використовується технологія ASLR, яка дозволяє випадковим чином змінювати розташування в адресному просторі процесу важливих структур. Але, на відміну від IE8, в IE9 технологія ASLR використовується для кожної завантаженої DLL-бібліотеки окремо, що можна спостерігати за допомогою утиліти Process Explorer. Втім, в тому ж Process Explorer можна побачити, що й інші браузери, наприклад, Mozilla Firefox, використовують технологію ASLR аналогічним чином.

Використання технології ASLR для кожної завантаженої DLL в IE9:



Єдиною перепоною для ефективного захисту браузерів від атак за допомогою технології ASLR може служити той факт, що виробники надбудов і доповнень для браузерів не поспішають користуватися цією технологією в своїх продуктах, і атаки можуть теоретично відбуватися через відповідні аддони.

Також можна відзначити той факт, що IE9 був зібраний за допомогою нового компілятора Microsoft Visual C++ 2010 при використанні технології

Enhanced GS, яка дозволяє припиняти випадки можливого переповнення буферів в автоматичному режимі. При використанні Enhanced GS, за запевненням Microsoft, при незначному впливі на продуктивність браузера значно підвищується рівень його захищеності.

Зміни в системі сповіщень

Будь-який новий функціонал, який стосується забезпечення безпеки, часто пов'язаний з організацією зворотного зв'язку з користувачем. Якщо повідомлень про роботу тієї чи іншої програми буде занадто багато, користувачам це перестане подобатися, тому що зайва кількість повідомлень відволікає від роботи і змушує задуматися про ефективність захисного ПЗ, яке використовується. Тому дуже важливо при розробці захисного ПЗ (а інтернет-браузер є на сьогоднішній день одним з найбільш важливих контурів захисту системи від проникнення шкідливого коду та інших дій зловмисників) не забувати про ергономічність взаємодії з користувачем.

Як запевняють розробники Internet Explorer, в версії 9 вони досягли балансу в системі оповіщення користувачів між такими крайнощами як «шумність» і «тиша». Для цього всі повідомлення Internet Explorer були спочатку поділені на 3 категорії:

- ***блокуючі повідомлення*** - повідомлення на які користувач повинен зреагувати негайно для того, щоб продовжити роботу з браузером;

- ***повідомлення-пропозиції*** - повідомлення, які пропонують користувачеві зробити які-небудь дії, але при цьому такі повідомлення не перешкоджають подальшому інтернет-серфінгу; до таких повідомлень, наприклад, відносяться пропозиції зберегти пароль для веб-сайту;

- ***повідомлення-підтвердження*** - повідомлення, які інформують користувача про щось, наприклад, це повідомлення про те, що історія відвідувань була успішно вилучена.

Після аналізу всіх повідомлень, які видає Internet Explorer, розробники видалили 23 повідомлення з групи блокуючих повідомлень. Деякі з таких повідомлень було видалено зовсім, а деякі перенесені в інші групи. Наприклад, питання про те, чи потрібно зберегти пароль для сайту, не блокує в IE9 можливість подальшого перегляду сайту без відповіді на це питання.

Всі подібні рішення повинні сприяти більш зручному використанню захисних механізмів Internet Explorer, які раніше своїми повідомленнями викликали у користувачів роздратування.

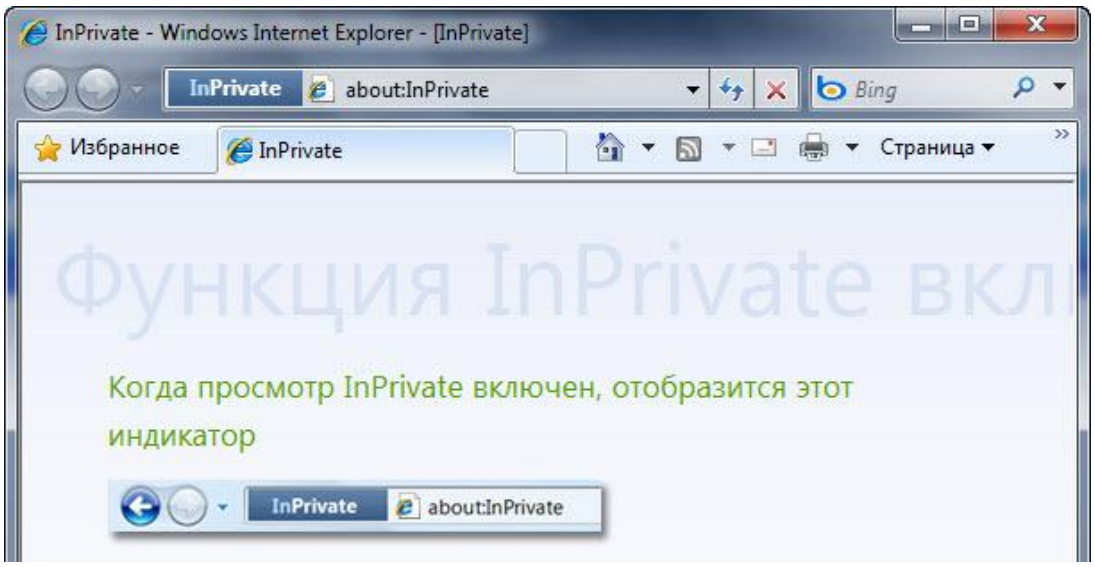
Приватний інтернет-серфінг

З попередньої, восьмий, версії браузера в IE існує популярний останнім часом режим приватного інтернет-серфінгу InPrivate. Якщо браузер працює в цьому режимі, то інформація про відвідані веб-сторінках не зберігається в журналі IE, також не зберігаються тимчасові файли, дані веб-форм, паролі до сайтів та куки. При цьому для режиму InPrivate запускається окрема сесія браузера, ізольована від інших сесій.

Перейти в режим InPrivate можна кількома способами:

- на панелі браузера натиснути кнопку «Безпека» і клацнути в меню «Перегляд InPrivate»;
- відкрити нову вкладку і клацнути «Переглянути в режимі InPrivate»;
- в Windows 7 клацнути правою кнопкою миші на значку IE в панелі завдань і вибрати режим зі списку переходів;
- натиснути комбінацію клавіш Ctrl +Shift+P.

Нарешті, можна ввести `about:inprivate` в адресному рядку, як показано



Дивно, але при такій різноманітності способів запуску режиму InPrivate, їм нехтують не лише домашні користувачі, а й фахівці.

На додаток, можна нагадати, що в Adobe Flash, починаючи з версії 10.1, вбудована підтримка приватних режимів відразу для декількох браузерів, в т.ч. підтримка режиму InPrivate в Internet Explorer. Зокрема, при використанні актуальних версій плагіна Adobe Flash в режимі InPrivate не зберігаються так

звані «флеш-куки» - такі об'єкти видаляються при виході з приватного режиму перегляду сайтів.

Фільтр запуску міжсайтових сценаріїв

XSS-атаки є широко використовуваним інструментом для зловмисників. XSS-вразливості, які виявляються і експлуатуються зловмисниками на безлічі сайтів, дозволяють контролювати обмін інформацією між користувачем і веб-сайтом, або веб-додатком, якому користувачі довіряють. Міжсайтові сценарії дозволяють організувати такі атаки як:

• крадіжка куків, включаючи крадіжку куків сесій (дозволяють зламувати аккаунти користувача);

• відстежувати рядки, які жертва вводить з клавіатури на веб-сайті або у веб-додатку;

• здійснювати дії на сайтах від імені користувача-жертви. Наприклад, успішна атака на Gmail дозволила б зловмисникам читати пошту користувача та пересилати її, а також додавати нові події в календар.

Фільтр запуску міжсайтових сценаріїв в Internet Explorer на льоту аналізує код сторінок, які завантажуються, визначає підозрілі скрипти, які можуть використовуватися для XSS-атак, і припиняє виконання таких скриптів. При цьому користувачеві не видається жодних питань - IE9 просто блокує запуск скриптів і виводить повідомлення про те, що код сторінки було змінено для того, щоб попередити скоєння атаки з використанням міжсайтових сценаріїв. У разі, якщо через даний фільтр який-небудь сайт відображається некоректно, розробники браузера рекомендують звертатися до веб-майстра сайту.

В цілому IE9 пропонує користувачеві досить потужні технології забезпечення безпеки роботи в Інтернеті, хоча можна відзначити і певні мінуси [6]:

Плюси:

• фільтр завантажуваних додатків SmartScreen Application Reputation;
• фільтр ActiveX;
• захист від стеження;
• функція «Закріплені сайти»;
• наявність приватного режиму інтернет-серфінгу (Private Mode);
• наявність фільтра запуску міжсайтових сценаріїв;
• позитивні зміни у системі сповіщень.

Мінуси:

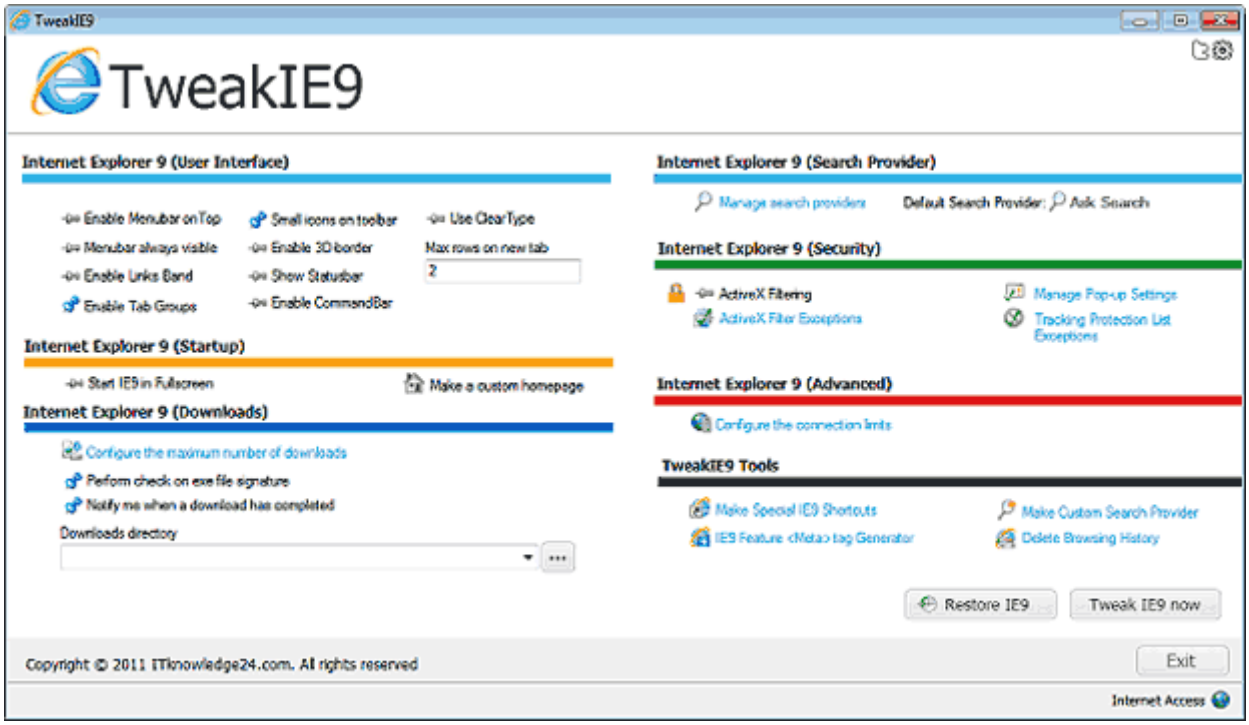
• недостатня гнучкість фільтра ActiveX;
• відсутність власних засобів обмеження показу реклами та обмеження запуску скриптів.

Інструменти налаштування Internet Explorer 9

Коли Ви намагаєтеся налаштувати веб-браузер Internet Explorer 9 від Microsoft, то Ви обмежені варіантами конфігурації в, так званих, Internet Options браузера.

Ці варіанти насправді не сильно змінилися з моменту випуску Internet Explorer 6. Користувачам, які хотіли б налаштовувати і модифіковані інші елементи браузера, доводиться покладатися на твіки реєстру, групових політик і сторонніх утиліт.

Нещодавно випущена нова версія одного з таких інструментів сторонніх виробників [7]. Tweak IE9 було розроблено спеціально для браузера Internet Explorer 9. Портативна програма перевіряє, чи встановлений Internet Explorer 9 в системі. Якщо так, то відображається стартова кнопка для запуску програми:



Програма відображає всі доступні параметри налаштування в головному інтерфейсі. Твіки розділені на кольорові секції. Зміни доступні, наприклад, для інтерфейсу користувача Internet Explorer, завантаження файлів і безпеки.
Ось список можливих параметрів конфігурації:

Інтерфейс користувача:

- Включити зверху рядок меню

- Рядок меню завжди видно
- Включити смужку посилань
- Включити групи вкладок
- Маленькі іконки на панелі інструментів
- Включити 3D-окантування
- Показувати рядок стану
- Включити панель команд
- Використання технології ClearType
- Максимум рядків на новій вкладці

Запуск:

- Стартувати IE9 на повний екран
- Зробити налаштовуваною домашню сторінку

Завантаження:

- Налаштувати максимальну кількість завантажень
- Виконати перевірку підпису EXE файла
- Повідомляти, коли завантаження завершена
- Змінити каталог завантаження

Постачальник пошуку:

- Управління постачальниками пошуку
- Постачальник пошуку за замовчуванням

Безпека:

- Фільтрація ActiveX
- Фільтри винятків ActiveX
- Управління налаштуванням спливаючих вікон
- Відстеження винятків списку захисту

Додаткові:

- Налагодження обмеження на підключення

Спеціальні інструменти:

- Додавання спеціальних ярликів IE9
- Функція мета-тег генератора IE9
- Зробити налаштовуваного постачальника пошуку
- Видалити історію відвіданих сторінок
- Відновлення IE9

Більшість варіантів конфігурації вмикається і вимикається одним натисканням на значок поруч з кожним налаштуванням. Після того, як Ви зробите всі зміни, треба натиснути на кнопку Tweak IE9, щоб застосувати зміни в веб-браузері. Якщо Ви хочете скасувати зміни, натисніть кнопку Restore IE9.

TweakIE9 сумісний з 32- і 64-розрядними версіями операційних систем

НАЛАШТУВАННЯ БЕЗПЕКИ GOOGLE CHROME

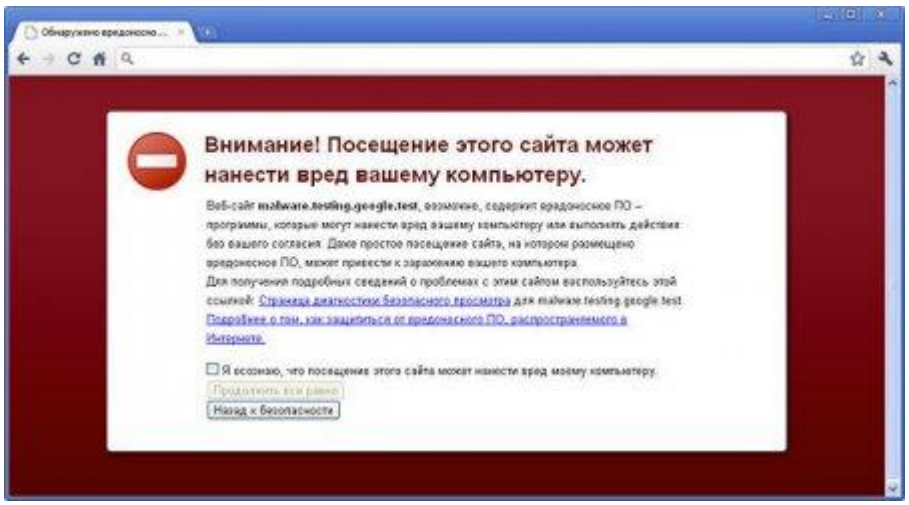
Google Chrome містить функції, які допомагають захистити користувачів та комп'ютер від шахрайських веб-сайтів при роботі в Інтернеті. Для забезпечення захисту від фішингу та атак шкідливого програмного забезпечення Google Chrome використовує такі технології, як безпечний перегляд, тестування та автоматичне оновлення.

Безпечний перегляд

При спробі відкрити сайт, який, за нашими відомостями, може містити шкідливе програмне забезпечення або створювати загрозу фішингу, Chrome видає попередження.

Фішингова атака полягає в тому, що шахраї, видаючи себе за іншу особу, намагаються отримати особисту інформацію та інші важливі відомості про користувача, зазвичай використовуючи підроблені веб-сайти. Шкідливе програмне забезпечення - це програми, які встановлюються на комп'ютер без відома користувача і призначені для нанесення шкоди комп'ютера або крадіжки інформації.

Завдяки технології безпечного перегляду, реалізованої в Chrome, при спробі переходу на веб-сайт, який потенційно може створювати загрозу фішингової атаки або містити шкідливе програмне забезпечення, Ви побачите попередження, як показано в прикладі нижче:



Тестування

Тестування дозволяє запобігти встановленню шкідливого програмного забезпечення на комп'ютер, а також використання операцій на одній вкладці для впливу на операції на іншій вкладці. Тестове середовище створює додатковий шар для захисту браузера від шкідливих веб-сайтів, які намагаються встановити програми на комп'ютер, контролювати дії, що

виконуються користувачем при роботі в Інтернет, або вкрасти інформацію з жорсткого диска комп'ютера.

Автоматичне оновлення

Для того, щоб гарантувати захист за допомогою останніх доступних оновлень безпеки, Chrome періодично здійснює перевірку наявності оновлення. Завдяки цій функції оновлення та виправлення для Chrome встановлюються автоматично без яких-небудь дій з боку користувача.

Показники безпеки веб-сайту

При підключенні до веб-сайту Google Chrome показує інформацію про з'єднання і видає попередження, якщо повністю безпечне з'єднання з сайтом встановити не вдалося.

Перевірка використання сайтом безпечного з'єднання (SSL)

При введенні конфіденційної інформації на сторінці переконайтеся, що ліворуч від URL сайту в адресному рядку відображається значок замка, який означає, що сайт використовує SSL. SSL є протоколом зашифрованою передачі даних між вашим комп'ютером і веб-сайтом, який переглядається. Сайти можуть використовувати SSL для запобігання доступу третіх осіб до переданої каналами інформації.

- Сайт не використовує SSL.

Більшості сайтів не потрібно використовувати SSL, тому що через них не передається конфіденційна інформація. Намагайтеся не вводити конфіденційну інформацію, наприклад імена користувачів і паролі, на таких сторінках .

https:// ***- Google Chrome встановив безпечне з'єднання з веб-сайтом.***

Переконайтеся, що відображається цей значок і перевірте URL, якщо потрібно ввести реєстраційні дані для входу на сайт або ввести конфіденційну інформацію на сторінці.

Якщо сайт використовує сертифікат Extended Validation SSL (EV-SSL), поруч із позначкою відображається назва організації зеленим шрифтом. Переконайтеся, що в браузері встановлена перевірка оглядів сертифікації сервера для ідентифікації сайтів за допомогою EV-SSL сертифікатів.

https:// ***- Сайт використовує SSL, але Google Chrome виявив вразливий зміст на цій сторінці.***

Проявіть обережність, якщо потрібне введення конфіденційної інформації на цій сторінці. Таким вразливим змістом може хтось скористатися для коректного зміни цієї сторінки.

- Сайт використовує SSL, але Google Chrome виявив вразливий зміст високого ризику на сторінці або проблеми з сертифікатом сайта.

Не вводьте конфіденційну інформацію на цій сторінці. Недійсний сертифікат або інша серйозна проблема, що стосується https, може означати, що хтось намагається проникнути в Ваше з'єднання з сайтом.

Перегляд додаткової інформації про веб-сайт

Натисніть значок або замка, щоб переглянути додаткову інформацію про ідентифікаційні дані, з'єднання, Вашу історію відвідування веб-сайту.

Ідентифікаційні дані веб-сайту

Сайти, що використовують SSL, надають браузерам сертифікати безпеки для підтвердження їх ідентифікаційних даних. Один веб-сайт може видавати себе за іншого, але тільки справжній веб-сайт має дійсний сертифікат безпеки для URL. Недійсні сертифікати можуть свідчити про спробу неавторизованого доступу третіх осіб у Ваше підключення до веб-сайту.

- Сертифікат веб-сайту є дійсним і перевірений довіреним стороннім центром сертифікації.

- Веб-сайт не надав браузеру сертифікат. Це нормально для звичайних http-сайтів (з позначкою в адресному рядку), оскільки сертифікати звичайно надаються тільки сайтами, які використовують SSL.

- Google Chrome виявив проблеми з сертифікатом сайту. Слід виявити обережність, тому що веб-сайт може видавати себе за інший сайт з метою отримання Вашої персональної або іншої конфіденційної інформації.

З'єднання з сайтом

Браузер Google Chrome відображає, чи з'єднання є повністю зашифрованим. Якщо з'єднання не є безпечним, треті особи можуть переглядати або підробляти інформацію на веб-сайті.

- Браузер Google Chrome встановив безпечне з'єднання з веб-сайтом, що переглядається.

- З'єднання з сайтом не зашифроване. Це нормально для звичайних http-сайтів (з позначкою в адресному рядку).

- З'єднання з сайтом зашифроване, але Google Chrome виявив змішаний зміст на сторінці. Проявіть обережність, якщо потрібне введення інформації на цій сторінці. Таким змішаним змістом може хто-небудь скористатися для коректної зміни сторінки. Це означає, що на сторінці є сторонні картинки, відео або вбудована реклама.

Якщо для підключення до Інтернету використовується загальнодоступна бездротова мережа, змішаний зміст може бути особливо небезпечним, оскільки такий тип з'єднання більш схильний втручанню з боку в порівнянні з дротяними мережами.

Розширені налаштування безпеки

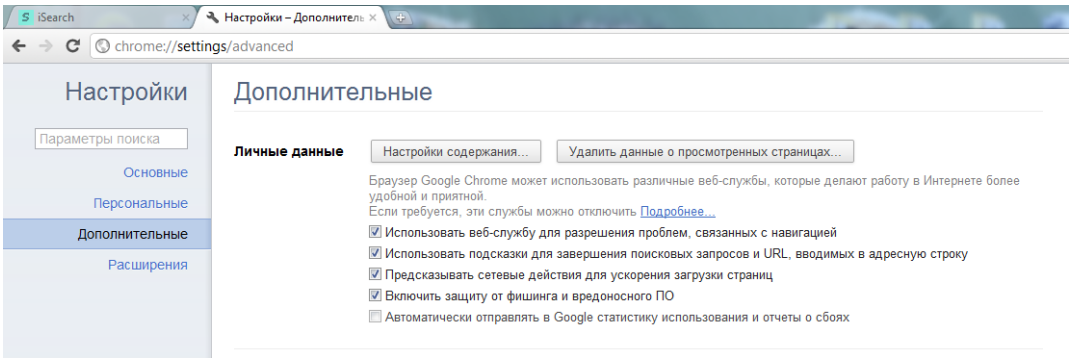
У Google Chrome передбачені спеціальні засоби для захисту Вашої безпеки під час перегляду веб-сторінок. Щоб змінити ці налаштування, виконайте наступні дії.

1. Натисніть на значок  гайкового ключа на панелі інструментів браузера.

2. Виберіть Параметри (Настройки на Mac і Linux, Установки на Chrome OS).

3. Перейдіть на вкладку Додаткові.

4. Нижче буде наведений список установок, які можна змінювати.



Захист від фішингу і зловмисного ПЗ

Цей параметр в розділі "Персональні дані" включений за умовчанням. Коли він включений, Google Chrome показує попередження, якщо сайт, що відкривається, підозрюється в фішингу або поширенні зловмисних програм. При включеному захисті від фішингу та зловмисних програм відображаються такі повідомлення.

Повідомлення	Значення
Увага! Виявлена проблема.	Це повідомлення відображається для сайтів, які Google Chrome визначає як такі, що містять потенційно шкідливе ПЗ.
Увага! Можливо, цей сайт створений з метою фішингу.	Це повідомлення з'являється, коли Google Chrome виявляє, що відвідуваний вами сайт підозрюється в фішингу.

Відключення захисту від фішингу та шкідливих програм

1. Натисніть на значок  гайкового ключа на панелі інструментів браузера.
2. Виберіть Параметри (Настройки на Mac і Linux, Установки на Chrome OS).
3. Перейдіть на вкладку Додаткові і знайдіть розділ "Конфіденційність".
4. Зніміть прапорець "Увімкнути захист від фішингу та зловредних програм".

Налаштування і сертифікати SSL

Керування налаштуваннями та сертифікатами SSL здійснюється в розділі "Безпека".

Налаштування веб-змісту

В діалоговому вікні "Налаштування вмісту" можна налаштувати параметри для файлів cookie, зображень, JavaScript, модулів, спливаючих вікон, відомостей про місцезнаходження і оповіщень.

Щоб змінити ці налаштування, виконайте такі дії:

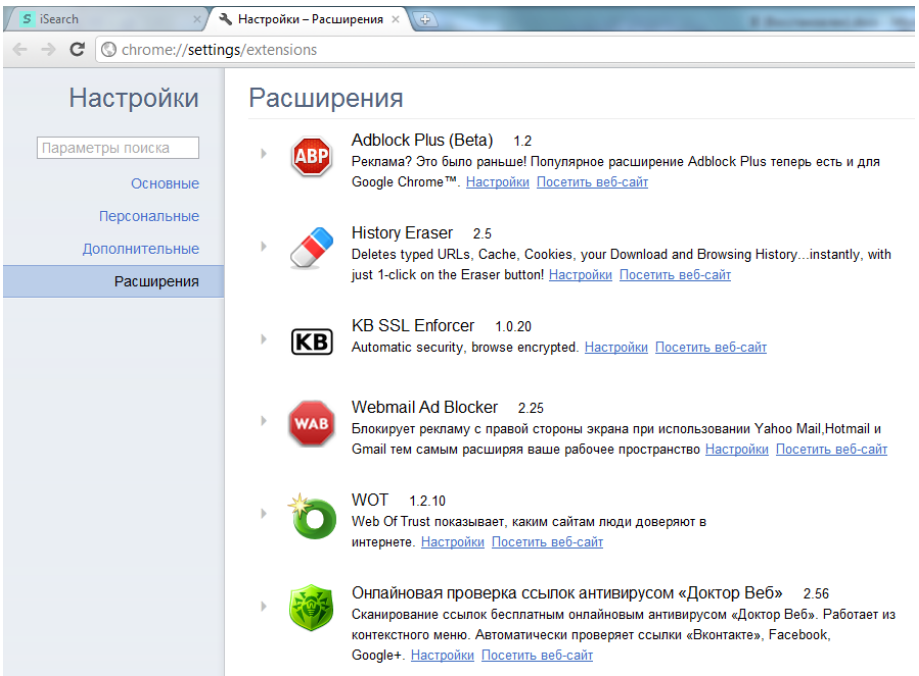
1. Натисніть на значок  гайкового ключа на панелі інструментів браузера.
2. Виберіть Параметри (Настройки на Mac і Linux, Установки на Chrome OS).
3. Перейдіть на вкладку Додаткові.
4. В розділі "Персональні дані" виберіть **Налаштування змісту**.
    - ***Файли cookie*** – це файли, створювані відвідуваними Вами веб-сайтами для зберігання інформації користувача, наприклад, установки веб-сайту або даних про профіль. За умовчанням вони включені. Важливо мати уявлення про налаштування файлів cookie, оскільки з їх допомогою веб-сайти можуть відстежувати дії своїх відвідувачів.
    - ***Картинки*** за умовчанням відображаються. Щоб відключити картинки, виберіть "Не показувати зображення".
    - ***JavaScript*** широко використовується у веб-дизайні для розширення функціональності сайтів. Якщо підтримка JavaScript відключена, деякі сайти можуть не працювати належним чином.
    - ***Модулі*** використовуються на веб-сайтах для відображення певного змісту, який браузери не можуть обробляти самостійно, наприклад файлів Flash або Windows Media. За умовчанням вони включені

- ***Спливаючі вікна*** за умовчуванням блокуються, щоб не захаращувати екран
- ***Запити про розташування***: за умовчуванням Google Chrome попереджає користувача, якщо сайт запитує інформацію про місцезнаходження.
- ***Оповіщення.*** Деякі сайти, такі як Календар Google, можуть відображати оповіщення на робочому столі Вашого комп'ютера. Google Chrome за умовчанням оповіщає Вас, якщо сайту потрібен дозвіл на автоматичний показ сповіщень.

Натисніть ***Винятки*** ... в будь-якому з розділів, щоб вказати, що робити з відповідним змістом на певних сайтах. Потрібно додати сайт в список виключень? Можна ввести ім'я хоста і IP-адресу, а також можна задати маску домена (наприклад, введіть [*.]google.com, щоб вказати сайти google.com і www.google.com, але не сайт othergoogle.com).

Також бажано розширити базові функції забезпечення безпеки Chrome наступними доповненнями:

• AdBlock Plus - блокування реклами;
• Flash Block - блокування флеш-контенту (для розблокування медіа-контенту - відео ВКонтакті та іншого необхідно просто кликнути на відео ролику);
• KB SSL Enforser - розширення забезпечує автоматичне шифрування трафіку;
• WOT - індикатор довіри сайту;
• History Eraser – очищення історії відвідування сайтів (URL, кеш, куки, завантаження тощо)

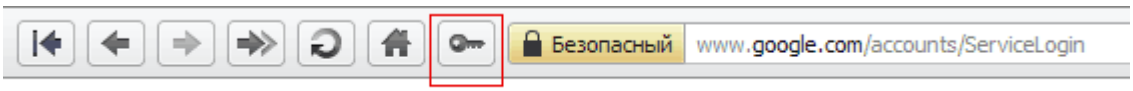


НАЛАШТУВАННЯ БЕЗПЕКИ OPERA

Ви можете змінювати налаштування безпеки браузера Opera на свій розсуд. Далі перейдіть Налаштування> Загальні налаштування> Розширені> Безпека [9]

Нові версії браузера Opera (так само як і Mozilla Firefox) дозволяють зберігати паролі авторизації на сайтах. При авторизації на якомусь сайті вперше Opera запитає, чи зберігати пароль. У разі позитивної відповіді, логін і пароль будуть збережені в браузері і Вам не потрібно його запам'ятовувати і вводити щорашу по пам'яті.

Коли Вам потрібно буде авторизуватись на сайті, замість введення логіна і пароля Вам достатньо натиснути на кнопку «Ключ»:



- логін і пароль будуть введені.

Але збереження паролів у браузері не безпечно. Підвищити безпеку зберігання паролів в Opera Ви можете, задавши в налаштуваннях браузера додатковий пароль безпеки (його ще називають майстер-паролем) на базу паролів.

Встановлення майстер-пароля

Клієнтські сертифікати, які іноді називають особистими сертифікатами, видають банки або інші захищені веб-сайти для того, щоб Вас ідентифікувати. Так, як клієнтські сертифікати, призначені для Вашої ідентифікації, зберігаються на локальному комп'ютері, рекомендується захистити їх за допомогою майстер-пароля.

При першому встановленні клієнтського сертифіката Opera автоматично запропонує встановити майстер-пароль. Обраний пароль повинен триматися в секреті і бути достатньо складним, щоб його не можна було підібрати. При спробі використовувати клієнтський сертифікат Opera автоматично запросить у Вас майстер-пароль для використання сертифіката.

Якщо виникне необхідність у зміні головного пароля або ж Ви просто захочете захистити збережені в Opera паролі, Ви можете знову відкрити меню Налаштування> Загальні налаштування> Розширені> Безпека і натиснути на кнопку «Встановити пароль». Майстер-пароль може використовуватися не лише для захисту Ваших клієнтських сертифікатів, але і для захисту збережених Вами паролів авторизації на сайтах.

Запит на введення пароля

Після встановлення майстер-пароля, можна налаштувати часовий інтервал його перевірки. За умовчанням встановлено значення «Щоразу при

необхідності», тобто Opera буде питати майстер-пароль кожного разу, коли виникне необхідність використовувати клієнтський сертифікат або збережений пароль (за умови, що включений параметр «Використовувати для захисту збережених паролів»).

Використання майстер-пароля для захисту збережених паролів

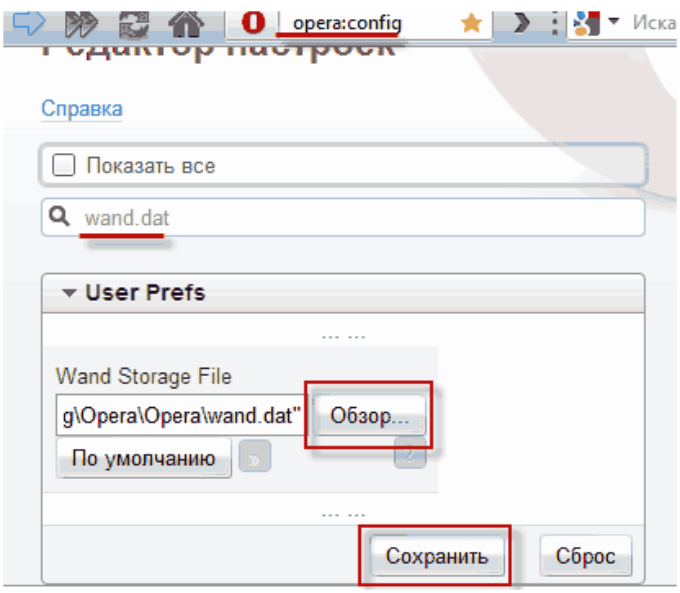
Якщо включити параметр «Використовувати для захисту збережених паролів», Opera буде питати майстер-пароль кожного разу, коли буде необхідно використовувати збережений пароль, або з інтервалом, встановленим в параметрі «Запитувати пароль».

Паролі зберігаються в Opera в зашифрованому вигляді, що досить безпечно. Але у випадку обвалу системи Ви можете втратити всі паролі, які були збережені браузером. Тому можете або налаштувати зберігання файлу з паролями на іншому жорсткому диску (відмінному від диска C), або вручну здійснювати його резервування. Файл з паролями в Opera називається wand.dat і зазвичай знаходиться цим шляхом:

```
c:\Users\Ім'я користувача\AppData\Roaming\Opera\Opera\
```

Там же Ви зможете знайти і файл bookmarks.adr, в якому зберігаються всі зроблені Вами в Opera закладки. Якщо Ви, наприклад, скопіюєте ці файли, а після відновлення операційної системи знову їх скопіюєте за приведеним вище шляхом (з заміною наявних вже там wand.dat і bookmarks.adr), то всі Ваші закладки та паролі будуть успішно відновлені.

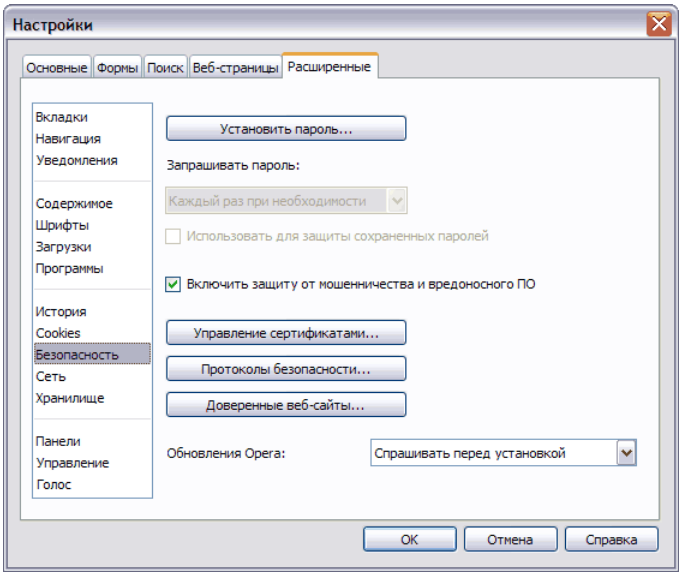
Ну, а якщо Ви захочете налаштувати зберігання файлу паролів з Opera на іншому диску Вашого комп'ютера, то введіть в адресному рядку браузера «opera:config» і натисніть Enter на клавіатурі. На сторінці, що відкриється, введіть в рядку пошуку wand.dat і Ви побачите поле, де можна буде поміняти місце зберігання файла паролів:



При необхідності паролі з Opera також можна легко експортувати за допомогою програми Opera Password Recovery.

Включення захисту від шахрайства

Захист від шахрайства попереджає Вас про підозрілі веб-сторінки, відправляючи запит до бази даних відомих «фішингових» і «шкідливих» сайтів. За замовчуванням «Захист від шахрайства» включений. При бажанні його можна включити/виключити, встановивши/знявши прапорець «Увімкнути захист від шахрайства та зловредного ПЗ»:



Управління сертифікатами

Для перегляду встановлених сертифікатів натисніть кнопку «Управління сертифікатами» та виберіть серед запропонованих опцій:

Особисті

При здійсненні операцій на захищених веб-сторінках клієнтські сертифікати використовуються для ідентифікації Вас.

Центри сертифікації

Центри сертифікації призначені для перевірки сертифікатів веб-сайтів.

Проміжні центри сертифікації

Проміжні центри сертифікації призначені для перевірки сертифікатів веб-сайтів.

Схвалені

Список схвалених Вами сертифікатів, у яких є проблеми з безпекою.

Відхилені

Відхилені Вами сертифікати, у яких є проблеми з безпекою.

Протоколи безпеки

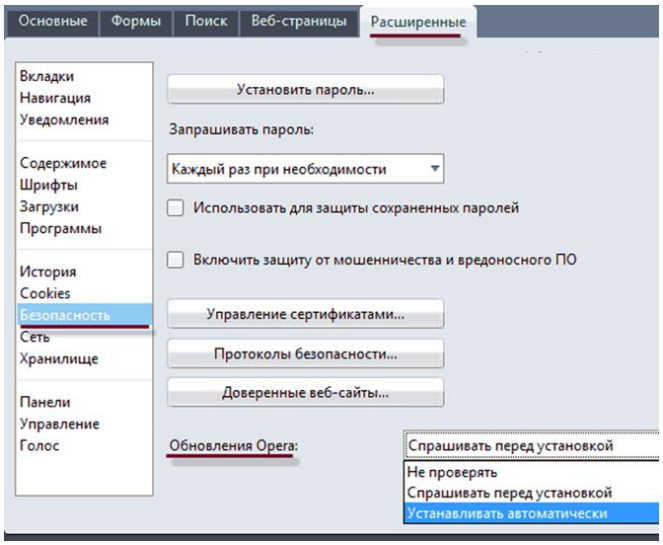
Протоколи безпеки призначені для організації безпечного обміну даними з сайтами, де необхідно обмінюватися конфіденційною інформацією, наприклад, даними про кредитні картки.

Коли Ви підключаєтеся до сайту через безпечне з'єднання, то в полі адреси праворуч з'являється жовтий індикатор використання безпечного протоколу, або ж відображається зелений індикатор при використанні технології розширеної перевірки (Extended Validation). Поруч із позначкою замка відображається ім'я домену, якому видано сертифікат, в той час як для сайтів, що використовують технологію розширеної перевірки, відображається назва організації, якій видано цей сертифікат. Для виводу більш докладної інформації натисніть на індикатор.

Рекомендується зазначити всі види протоколу SSL.

Автооновлення

Opera має вбудований механізм автоматичного оновлення:



Для параметра «Оновлення Opera» можна встановити наступні значення:

Не перевіряти
Opera не буде вас повідомляти про вихід нових оновлень

Запитувати перед установкою
При виході нових оновлень Opera показуватиме вікно з пропозицією завантажити оновлення

Встановлювати автоматично (дане значення встановлено за умовчанням)
При виході нових оновлень Opera автоматично буде їх завантажувати і встановлювати

Очищення куків і кеша в Opera

Управління cookies дозволяє Вам переглядати та редагувати cookies, які зберігає Opera: Головне меню - Інструменти - Налаштування - Розширені-Cookies – Управління

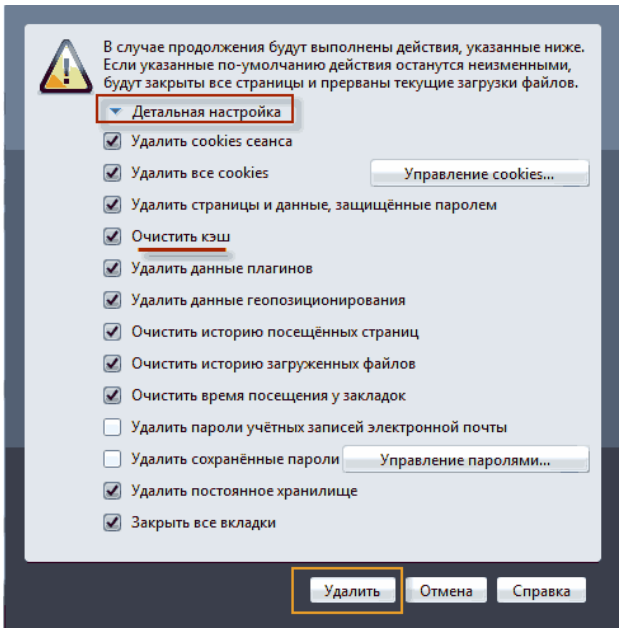
Натиснувши кнопку «Управління cookies ...», Ви побачите набір папок, назви яких відповідають доменам. Використовуйте поле «Знайти» для пошуку доменного імені, потім відкрийте відповідну папку для отримання детальної інформації про всі cookies, пов'язані з цим доменом.

Деякі сайти вимагають прийняття cookies, щоб можна було використовувати їхніми службами. Якщо Ви хочете, щоб ці сайти працювали, але не хочете зберігати cookies в перервах між відвідинами, оберіть "Видаляти нові cookies при виході з Opera».

Очищення кешу може знадобитися в різних ситуаціях, але в основному це потрібно або, щоб приховати сліди перебування на чужому комп'ютері, або у вебмайстрів дуже часто виникає необхідність очищення кеша для показу браузером оновленої інформації на сторінці, коли просте оновлення сторінки з утримуваної клавішою Shift не приносить бажаного результату.

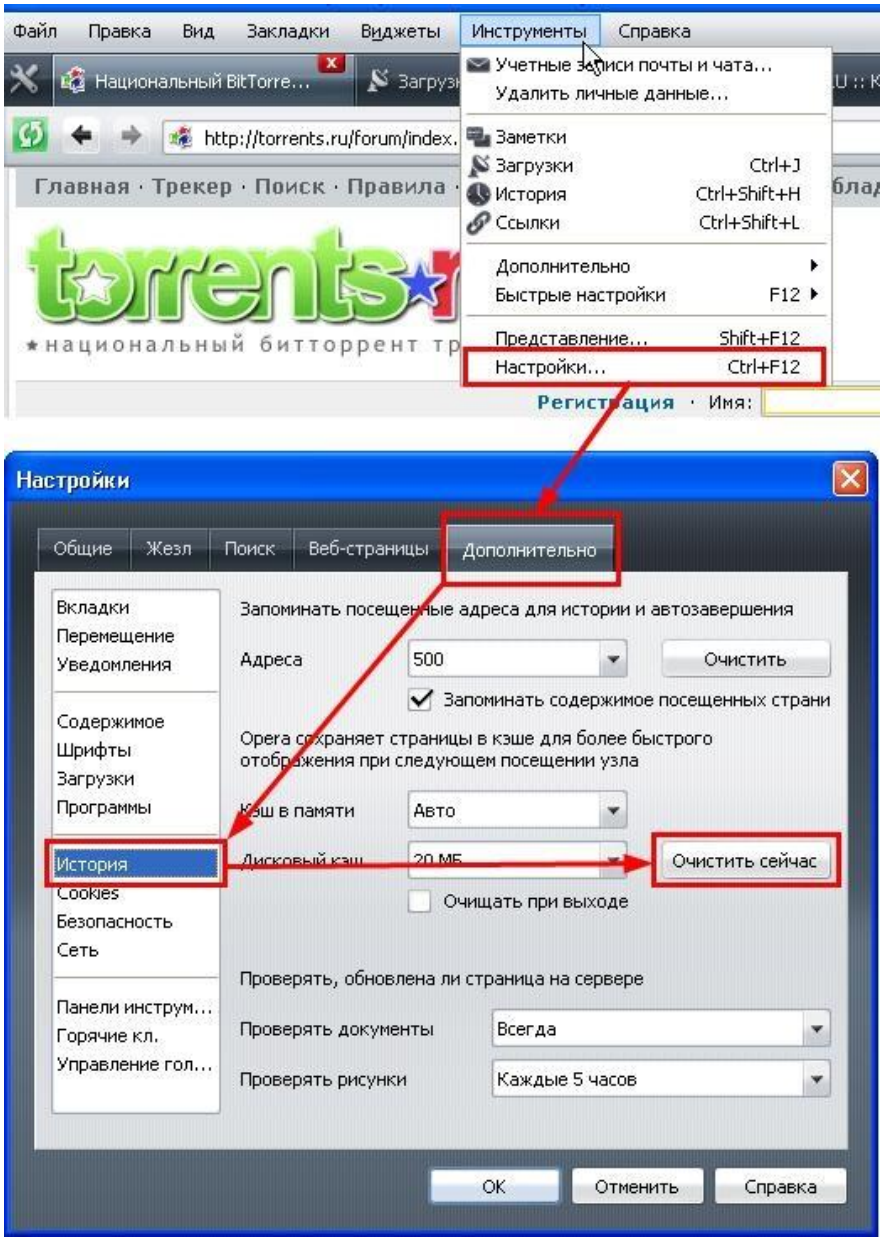
Насправді, почистити кеш в Опері просто і зробити це можна двома способами:

1. Якщо потрібно саме прибрати сліди свого перебування на чужому комп'ютері, то тут краще підійде не звичайне очищення кешу, а повне видалення всієї особистої інформації, яка могла залишитися після Вас в браузері. Для цього Вам потрібно буде вибрати з верхнього меню «Opera» - «Налаштування» - «Видалити особисті дані ...»:



Натиснувши на кнопку «Детальне налаштування», Ви зможете вказати, що саме крім кешу Ви хочете видалити, а потім натиснути відповідну кнопку внизу вікна.

2. Якщо Вам потрібно почистити тільки кеш браузера для того, щоб на сторінці відображалась коректна інформація, а не дані з цього самого кешу, то Вам потрібно буде зайти в налаштування з верхнього меню Opera - «Налаштування» - «Загальні налаштування» - «Розширені» - «Історія» та натиснути кнопку «Очистити…» в полі «Дисковий кеш»:



Тут же Ви зможете задати необхідні Вам параметри для кешуванню даних зі сторінок і кешуванню введених Url адрес в адресному рядку браузера.

Також рекомендується поставити два додаткових розширення, які будуть блокувати небажану рекламу і спливаючі вікна: "NoAdds" і "Opera AdBlock".

Для цього переходимо в меню Opera, яке відкривається відповідною кнопкою у лівому верхньому куті браузера, переходимо до пункту "Розширення" > "Вибрати розширення", і на сторінці, що з'явилася, вводимо в область пошуку по черзі зазначені розширення. Далі натискаємо Встановити. І у нас додається два корисних модуля для підвищення безпеки:

НАЛАШТУВАННЯ БЕЗПЕКИ MOZILLA FIREFOX

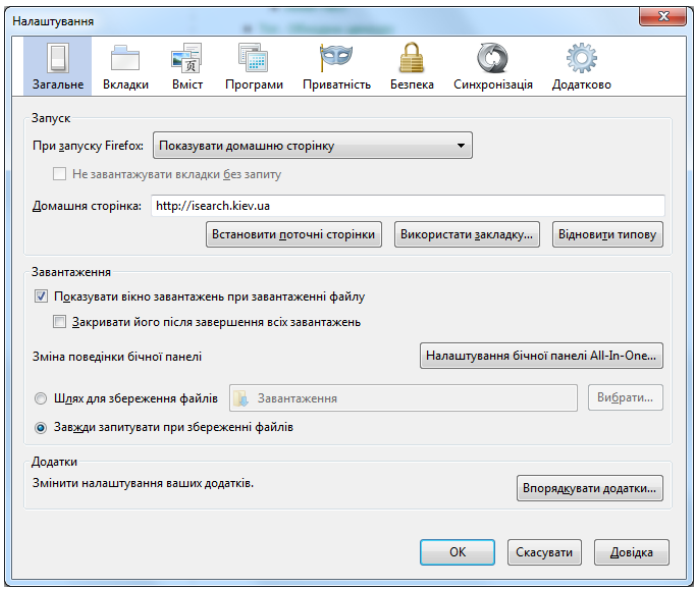
Firefox користується особливою популярністю в профессіоналів і ... хакерів. Чому? Незліченні доповнення, відкритий вихідний код, багато налаштувань і, перш за все, - браузер поважає Ваше приватне життя і приділяє багато уваги для підтримки безпеки.

Як правильно налаштувати браузер? Дозволити браузеру робити все, що його творці визнали можливим, покладаючись на їхній досвід і знання в області інформаційної безпеки? Або, навпаки, заборонити все, що можна заборонити, і звести таким чином ризики до мінімуму? Навряд чи є потреба вдаватися до крайнощів. Одна справа, якщо Ви працюєте на домашньому комп'ютері, доступ до нього є тільки у Вас, і про безпеку системи печеться десяток-другий корисних програм. Зовсім інша справа - якщо Ви підключаєтеся до малознайомої локальної мережі зі своїм ноутбуком або, скажімо, сидите за комп'ютером в Інтернет-кафе.

Розглянемо рекомендації з налаштування безпеки, які автор використовує вже тривалий час.

Загальні налаштування

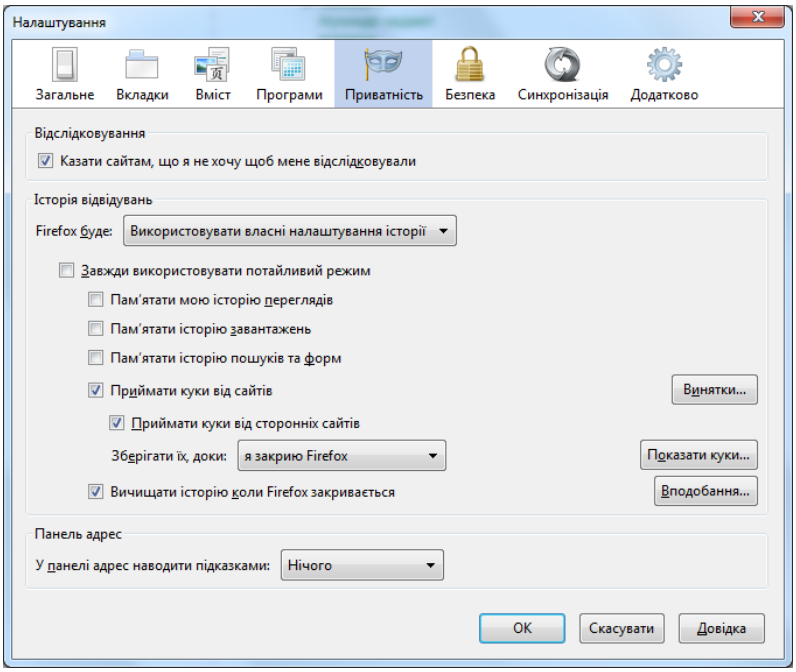
У меню "Інструменти" вибираємо пункт "Налаштування".Відкривається вікно. У його верхній частині видно горизонтальна лінійка основних "настроювальних" пунктів. Почнемо з пункту "Загальне":



Відзначаємо галочкою в розділі завантаження пункт "Завжди запитувати при збереженні файлів". Це не тільки впорядкує завантаження, але і дасть нам зайвий привід подумати перед тим, як завантажити і зберегти на комп'ютері той чи інший файл.

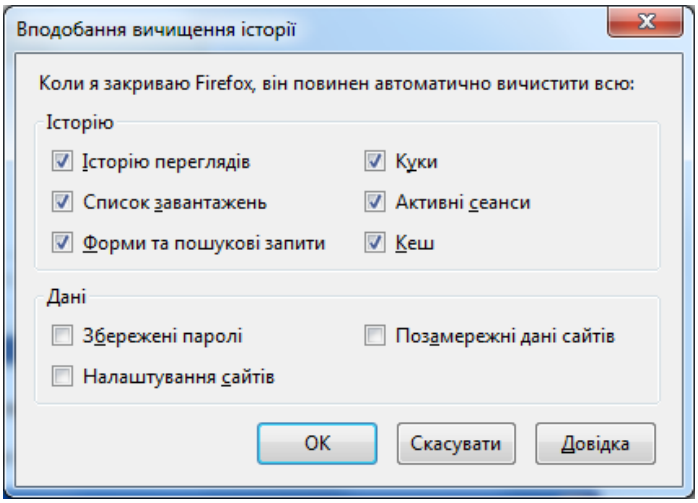
Налаштування приватності

Відкриваємо в налаштуваннях вкладку Приватність:



Перш за все перевіряємо, щоб була позначка для заборони відстежування сайтами. В історії відвідувань найзручніше вибрати «Використовувати власні налаштування історії», заборонити запам’ятовування історії переглядів, завантажень, пошуків та форм, але дозволити приймати куки від сторонніх сайтів. А для збереження куків вибрати термін доти, поки «я закрию Firefox».

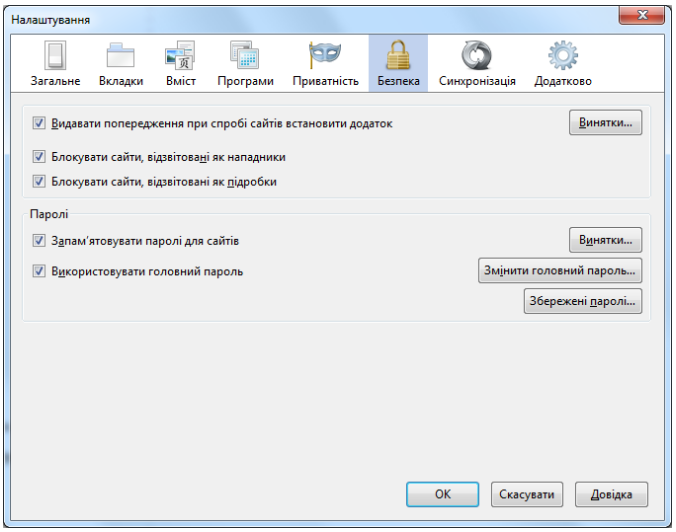
Вибрати пункт «Вичищати історію, коли Firefox закривається» і, натиснувши праворуч даного пункту кнопку «Вподобання», переконатися, що при закриванні Firefox дійсно все видаляється:



Тепер працює комбінація «гарячих клавіш» Shit+Ctrl+Delete, за допомогою якої Ви зможете вичистити все миттєво.

Налаштування вкладки *Безпека*

В першу чергу ставимо позначки напроти перших трьох пунктів, які вмикають попередження при спробі сайтів встановити додаток та блокують сайти, які визначаються як нападники чи підробки:

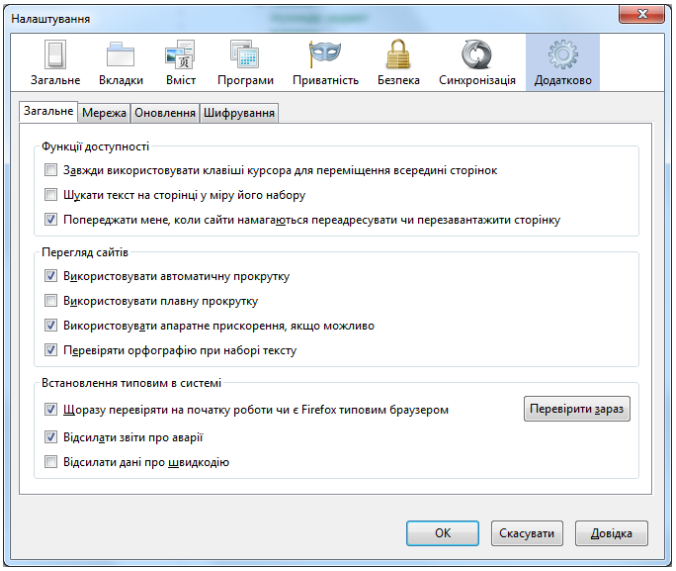


Окремий розділ – паролі. Хочете Ви того, чи не хочете, але при великому різноманітті соціальних мереж, онлайнових поштових скриньок та інших запаролених ресурсів Вам доведеться запам’ятовувати паролі доступу до сайтів. Щоб відразу ж захистити їх – увімкніть використання головного паролю. Цей пароль повинен бути досить складний, але легкий для запам’ятовування, бо при його втраті Ви втрачаєте і всі облікові записи до своїх онлайнових ресурсів.

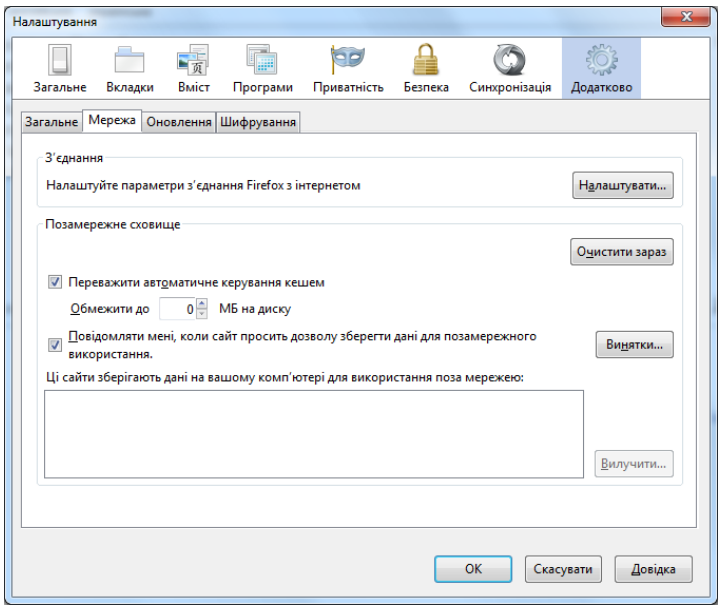
Видаляємо всі винятки безпеки, щоб при необхідності питали дозволу.

Налаштування вкладки *Додатково*

Тут найважливіший з точки зору безпеки пункт «Попереджати мене, коли сайти намагаються переадресувати чи перезавантажити сторінку. Вмикаємо його відповідною позначкою:

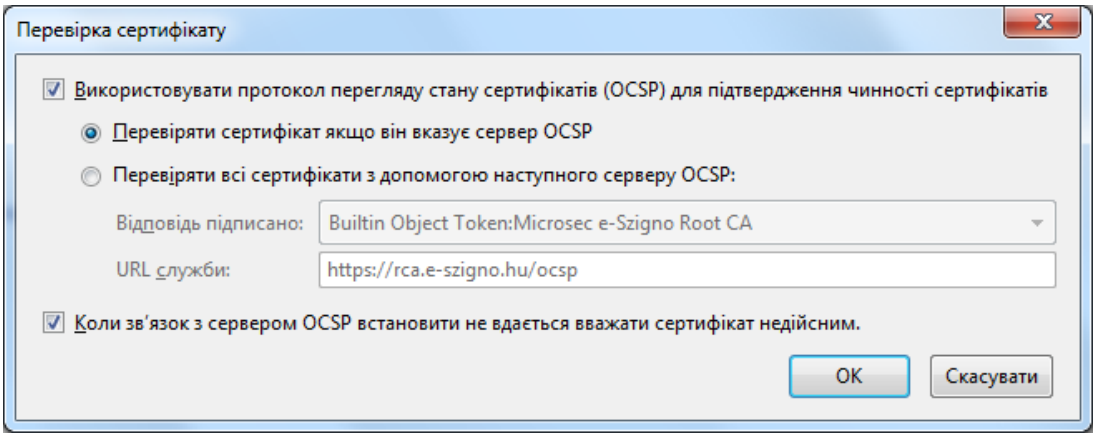


У вкладці Додатково> Мережа> Автономне сховище вимкніть автоматичне керування кешем і встановіть використання під кеш не більше 0 МБ. Так само поставте галочку в пункті "Повідомляти мені, коли сайт просить дозволу зберегти дані для поза мережного використання":



У вкладці Додатково> Шифрування переконайтеся, що обидва пункти "Використовувати SSL 3.0 та Використовувати TLS 1.0" включені. Потім

натисніть кнопку "Перевірка" і відзначте галочкою пункт "Коли зв’язок з сервером OCSP встановити не вдається вважати сертифікат як недійсний":



У вкладці Додатково> Оновлення рекомендується встановити автоматичну перевірку та встановлення оновлення.

Налаштування вкладок *Вміст* і *Програми*

Часто рекомендується в посібниках з безпеки вимкнути використання JavaScript, але краще у вкладці ***Вміст*** дозволити, а більш гнучко керувати такими сценаріями за допомогою додаткових плагінів, про які сказано нижче. Тут же залишити увімкненим пункт «Блокувати виринаючі вікна»

У вкладці ***Програми*** для вмісту на зразок word-документів, презентацій, Adobe Acrobat документів, архівів (і може ще чогось) у випадаючому списку праворуч вибираємо "Зберегти у файл". Так у Вас буде можливість перед відкриттям (запуском) чергового такого документа перевірити його антивірусом.

Управління плагінами.

Відкриваємо вікно управління плагінами: Меню> Інструменти> Додатки> Плагіни. Відключаємо всі плагіни, якими в даний момент не користуємося. Найголовніше - відключаємо підтримку Flash. Але як же тоді відео на ютубі дивитися? А ось так: заходите на ютуб - відкриваєте вікно "Додатки", включаєте Флеш. Поки сидите на ютубі, інші сайти не відкриваєте. Закінчили на ютуб лазити - відключаєте підтримку флеш, закриваєте вікно "Додатки". Ось так, але це ж краще ніж систему перевстановлювати?!

Така ж політика по відношенню до розширень. А саме: якщо якимось розширенням в даний момент не користуєтесь - краще його тимчасово відключити.

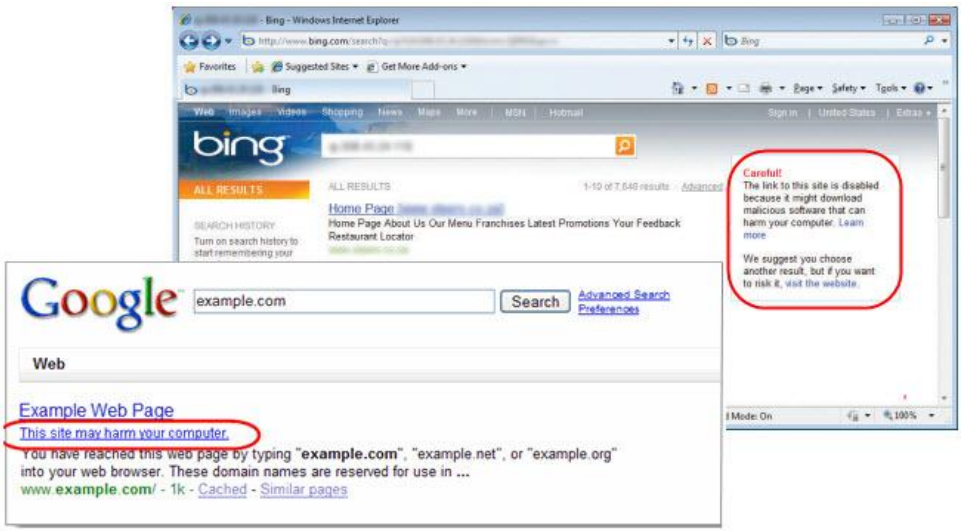
Рекомендовані додатки для Firefox

Adblock Plus - це доповнення на для початківців користувачів. Adblock Plus блокує дратівливі оголошення, але для ефективної роботи вимагає певних навичок в налаштувані.

NoScript - також для досвідчених користувачів. Доповнення блокуватиме всі скрипти на веб-сторінці, щоб дати Вам максимальну конфіденційність і безпеку. Якщо Adblock Plus блокує згідно підписки та Ваших вподобань, то NoScript блокує ВСІ сценарії, а Ви приймаєте рішення, що дозволити.

HTTPS Everywhere - це сучасне доповнення розроблене Electronic Frontier Foundation. В принципі, HTTPS Everywhere забезпечує безпечне з'єднання на сторінках, з сертифікатом SSLCertificates. Наприклад, коли Ви використовуєте пошук в Google, то більшість людей використовують незашифровану версію. Це доповнення змусить Google розміщувати свій SSL-сертифікат і у випадках, коли сайт підтримує шифрування, завжди автоматично використовується безпечне з'єднання.

Google і Microsoft не обмежуються рамками браузерів в боротьбі з шахрайськими сайтами, а використовують ще й міць своїх пошукових движків, що, до речі, йде на користь і іншим браузерам. Пошукові сервіси Google і Bing позначають в результатах неблагонадійні сайти, а при переході на них виводять попередження:



Для цього Google користується послугами сервісу StopBadware.org, а Microsoft застосовує свої методи. За даними компанії, в індексі Bing 0,3% сторінок скомпрометовані, при цьому власник сайту може і не знати, що зловмисники використовують уразливість в його движку як майданчик для шахрайства. Уявіть, що движок сайту, блогу чи форуму давно не оновлювався, а хтось використовував відому вразливість, щоб приховано перенаправляти відвідувачів на інший сайт або виконувати шкідливий код.

Тема безпеки в Інтернеті настільки велика, що, навіть не вдаючись в технічні подробиці, ми торкнулися лише маленької частини питань, пов'язаних з браузерами.

Висновок

Виходити в Інтернет нітрохи не страшно з будь-якого браузера. Але при цьому потрібно дотримуватися простих рекомендацій [8]:

- завжди використовувати останню версію браузера і встановлювати оновлення безпеки;
- оновлювати надбудови та плагіни (наприклад, Flash Player) при першому ж повідомленні;
- не змінювати налаштування безпеки браузера і системи в гірший бік (захищений режим і контроль облікових записів);
- застосовувати додаткові засоби захисту браузера;
- при необхідності користуватися конфіденційним режимом.

Від Вас не вимагають ніяких зусиль, щоб дотримуватися цих нескладних порад, які розробники заклали в стандартні налаштування браузера і операційної системи.

Підкреслюю, що ці рекомендації цілком підходять користувачам всіх браузерів. Ви можете убезпечити свою роботу в Інтернеті не докладаючи зусиль. Тільки пам'ятайте про кнопку «Так» ...

Використана література та інші джерела інформації:

1. http://isearch.kiev.ua/index.php/uk/news/internet/1202-ukraine-internet-2011
2. http://www.sidstudio.com.ua/list/ru/articles/0/112.html
3. http://szkti.ru/polezno/browsers
4. http://isearch.kiev.ua/index.php/uk/searchpractice/internetsecurity/605-ie-security
5. http://isearch.kiev.ua/index.php/uk/news/security/1259-the-study-which-concludes-that-firefox-lacks-security
6. http://www.anti-malware.ru/reviews/Internet_Explorer_9
7. http://isearch.kiev.ua/index.php/uk/news/browsers/ie/1047-tweak-ie9
8. http://isearch.kiev.ua/index.php/uk/searchpractice/internetsecurity/605-ie-security
9. http://help.opera.com/Windows/10.54/ru/security.html
10. https://security.ngoinabox.org/ru/firefox_privacy_and_security

ЗМІСТ

Формат 60x84 1/16. Друк цифровий.
Папір офсетний 80 г/м2.
Наклад 500 прим.

Видавництво: ТОВ «Праймдрук»
01023, м. Київ, вул. Еспланадна, 20, офіс 213
Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи
серія ДК № 4222 від 07.12.2011.