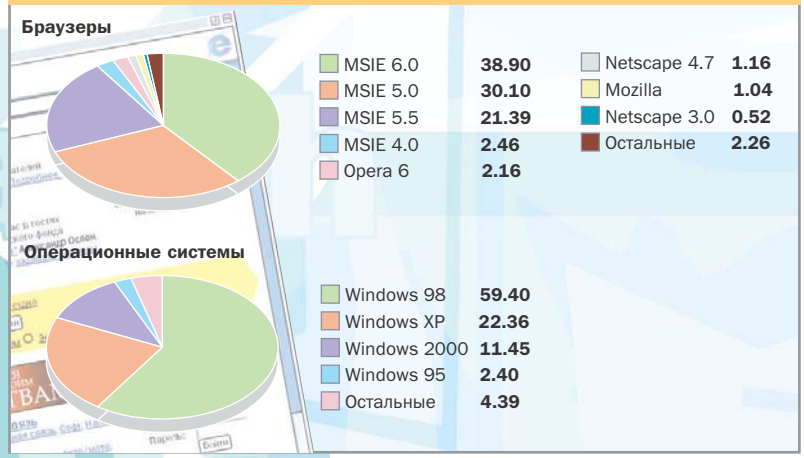
Браузеры

Безопасный серфинг

Любой пользователь, имеющий доступ в Интернет, иной раз задается вопросом собственной безопасности при путешествиях по Сети. Периодически появляющиеся сообщения о новых вирусах или хакерских атаках только усиливают чувство тревоги. А поскольку подавляющее большинство общается со Всемирной паутиной с помощью браузера, то в первую очередь встает вопрос именно о его защищенности.

Вот о средствах безопасности, имеющихся в наиболее популярных браузерах, мы и поговорим. Выбор описываемых браузеров, как и операционных систем, для которых они предназначены, был обусловлен данными статистики от HotLOG.ru. Как видите, самым популярным браузером в течение продолжительного времени вполне заслуженно остается Internet Explorer. А вот последние версии Netscape популярностью на просторах России пока не пользуются. Люди предпочитают более старую, но проверенную временем четвертую версию. Поэтому именно она включена в этот обзор. »

Данные статистики HotLOG.ru за первое полугодие 2002 года

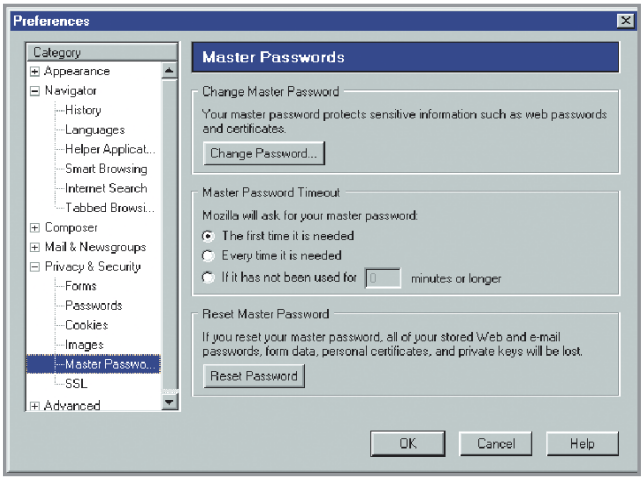


SSL и сертификаты

Secure Sockets Layer (с англ. — «безопасный уровень соединителей») — протокол, предназначенный для защищенной передачи данных. Вспомните, как начинается адрес, который вы набираете в строке вашего браузера? Наверняка в 99% случаев это будет «http», а значит, работая с WWW, вы пользуетесь протоколом пересылки гипертекста (Hypertext Transfer Protocol). Как это ни печально, обычный протокол HTTP не гарантирует должного уровня конфиденциальности, так как вся информация передается в незашифрованном виде по открытым каналам при недостаточном уровне аутентификации (авторизованный вход в какую-либо систему). Пользователь вводит логин и пароль, которые затем передаются web-серверу в незашифрованном виде. Это во-первых, а во-вторых, протокол HTTP не позволяет идентифицировать объекты, участвующие в обмене информацией. Говоря простым языком, мы не можем быть уверены в том, что объекты выдают себя за тех, кем они являются на самом деле, и что по пути злоумышленниками не будет перехвачена никакая информация, будь то PIN-код кредитной карточки или пароль почтового ящика. Протокол HTTPS, аналогичный HTTP, но использующий технологию SSL, позволяет решить данные проблемы.

Основой HTTPS являются сертификаты (своеобразный «паспорт») и криптозащита (шифрование). При инициализации обмена информацией браузер и сервер обменяются сертификатами, тем самым однозначно идентифицируя себя. Дальнейшее взаимодействие осуществляется по зашифрованному каналу. В итоге SSL теоретически может обеспечить полную защиту любого соединения в Интернете. Но только теоретически. На практике же все зависит от безошибочной реализации этой технологии в конкретном браузере. Обнаруженные уязвимости разработчики стараются устранить очередной «заплаткой», или сервис-паком. Выход сервис-паков для ПО, использующего SSL, сейчас вещь нередкая, что говорит о недостаточной степени совершенства реализации SSL-протокола во многих популярных ныне программах.

Теперь о главном — о реализации систем защиты в различных браузерах.

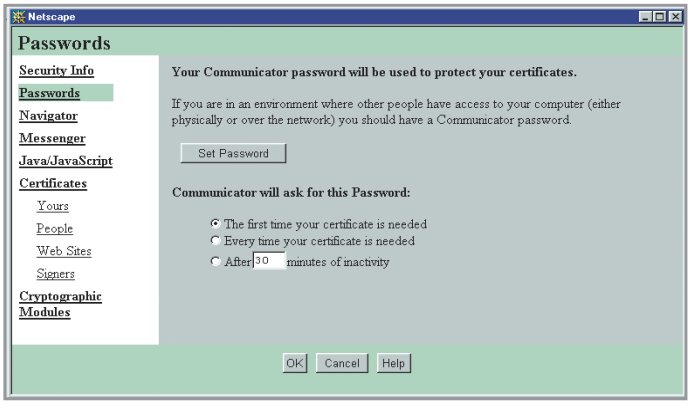


◂ Настройки безопасности в Mozilla 1.0 («Master passwords»)

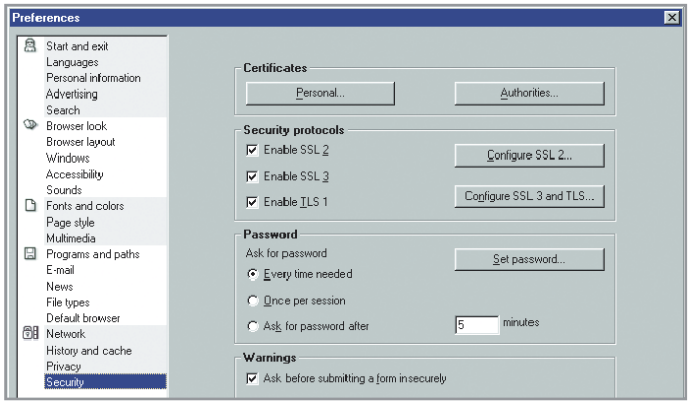
Mozilla 1.0

Браузер, который чрезвычайно долго не мог избавиться от нуля в порядковом номере версии, наконец дорос до финального релиза и теперь существует как в версиях для Linux, так и для Windows. Пункты меню одинаковы для обеих версий, и добраться до них можно следующим образом: «Edit -> Preferences -> Privacy & Security». Нас интересуют следующие из них.

- «Passwords» — менеджер паролей автоматически запоминает и при необходимости сам вводит имена и пароли к указанным в списке сайтам.
- «Master Passwords» — защищает личную информацию (пароли, доступ к сертификатам, работу со смарт-картами и др.). Если посторонний человек пользуется вашим браузером, то, не зная мастер-пароля, он не сможет воспользоваться вашими сертификатами и сохраненными паролями. То есть, злоумышленник, работая с финансовыми или корпоративными web-сайтами, не сможет выдать себя за вас и осуществить какие-либо операции от вашего имени. При вводе мастер-пароля можно проверить устойчивость к подбору комбинаций. Эта функция интересна и сама по себе уже может гарантировать достаточно высокую степень безопасности.
- «SSL» — настройка работы по протоколу SSL (выбор версий, методов шифрования).
- «Certificates» — управление сертификатами и устройствами защиты. В этом пункте можно добавлять или удалять сертификаты сайтов и свои собственные, а также уже имеющиеся в базе браузера сертификаты известных компаний и корпораций и просматривать информацию о них (например, срок действия). Настройки этого пункта »



▲ Настройки безопасности в Netscape 4.75, пункт «Passwords»



▲ Необходимый минимум защиты в Opera 6.04

» просты и интуитивно понятны, как, впрочем, и в других рассматриваемых браузерах.

- «Validation» — проверка действительности сертификатов и управление аннулированными (отозванными). В браузере предусмотрена автоматизация этого процесса — опция «Online Certificate Status Protocol» (OCSP), — что очень удобно.

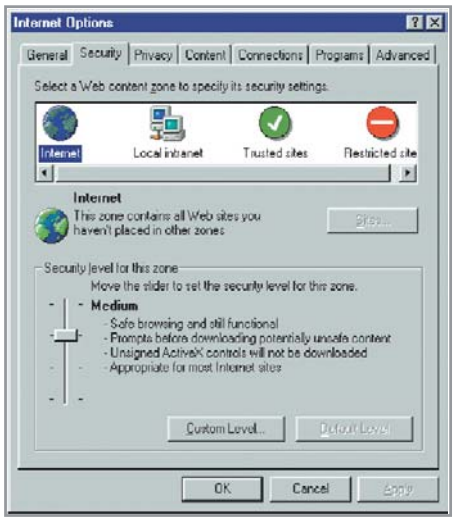
Разработчики этого браузера уделяют безопасности очень серьезное внимание, и, возможно, в дальнейшем Mozilla приобретет существенно большее число поклонников, чем сейчас.

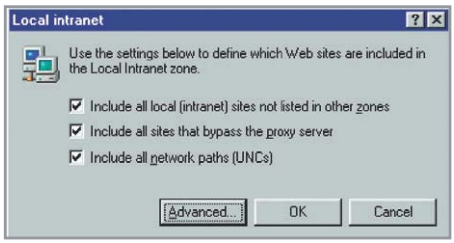
Netscape Communicator 4.75

Этот браузер в последнее время всячески пытается вновь завоевать утраченные позиции. Вышла уже версия под номером 7, но в нашей стране наиболее популярной остается все же старая добрая 4.75, проверенная годами использования. С точки зрения безопасности коренных отличий между ними не существует, поэтому мы смело можем рассматривать Netscape Communicator 4.75.

Итак, открываем настройки безопасности («Communicator -> Tools -> Security Info») и видим следующие пункты.

- «Security Info» — сообщает сведения о состоянии текущего уровня безопасности при работе с браузером (например, осуществляется ли шифрование трафика или нет).
- «Passwords» — назначение опции аналогично пункту «Master Passwords» в Mozilla.
- «Navigator» — настройка параметров работы по протоколу SSL.





▲ Конфигурирование зоны «Local intranet» в IE 6.0

◀ Настройки безопасности в Internet Explorer 6.0 достаточно обширны, и пользователь может сам выбрать тот уровень, который считает приемлемым

- «Messenger» — непосредственно к браузеру этот пункт отношения не имеет, это настройки безопасности для интернет-пейджера Instant Messenger.
- «Java/Java Scripts» — управление сертификатами и активизацией Java-апплетов и скриптов.
- «Certificates» — пункт управления сертификатами, чье содержимое практически полностью аналогично разделу «Manage Certificates» в одноименной опции Mozilla.
- «Cryptographic Modules» — управление криптографическими модулями, используемыми браузером (смарт-карты и другие).

Настройки Netscape Communicator очень похожи на имеющиеся в Mozilla, что неудивительно, поскольку оба браузера построены на одном ядре.

Opera 6.04

Все опции безопасности («File -> Preferences -> Security») здесь сведены к необходимому минимуму, умещаются в одном окошке, и их характеристики мало отличаются от тех, что существуют у «собратьев». Так, раздел «Password» фактически полностью аналогичен мастер-паролю в Mozilla. Как уже говорилось, средства безопасности в Opera оставляют пользователю не слишком много возможностей для настройки, поскольку ее сильными сторонами являются скорость загрузки страниц и компактность. Именно этим свойствам браузера и уделяют основное внимание разработчики. Впрочем, не за горами выход Opera 7, движок которого должен быть, по заявлениям создателей, полностью переписан. Возможно, в новой версии мы увидим другие средства безопасности.

Internet Explorer 6.0

В этом браузере с настройками безопасности, сосредоточенными в меню «Tools -> Internet Options... -> Security», дела обстоят поинтереснее: Microsoft, в отличие от других разработчиков ПО, ввела понятия Security Level («уровень безопасности») и Security Zones («зоны безопасности»). Таким образом, для каждой зоны можно установить свой, персональный уровень безопасности. Всего имеется четыре зоны.

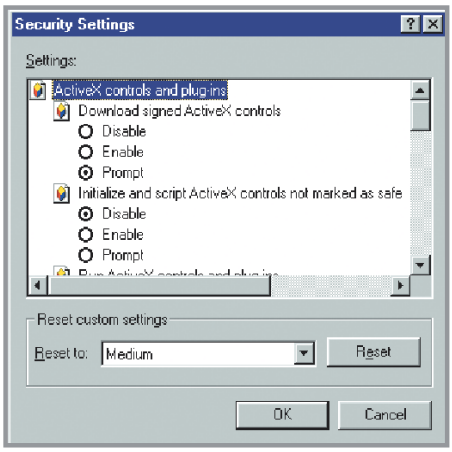
- «Internet», куда входят все web-сайты, не указанные в остальных зонах. В отличие от других зон, добавлять выборочно отдельно взятые сайты сюда нельзя.
- «Local intranet», где устанавливаются настройки безопасности для ресурсов локальной сети. Нажав кнопку «Sites...», можно выбрать, какие именно ресурсы включать в эту зону: »

Internet Explorer 6

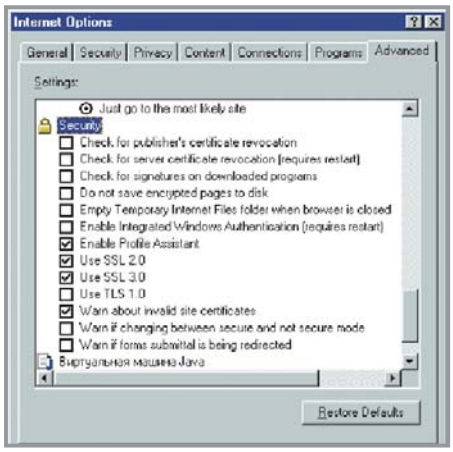
Заплатки для лидера

Вокруг браузера от компании Microsoft постоянно возникали какие-нибудь слухи или скандалы. В первую очередь это было связано с вопросами безопасности, а также с тем, что браузер с самого начала входил в состав операционной системы и избавиться от него легальными методами было практически невозможно. К каждой версией Internet Explorer появлялись дополнения и исправления, призванные повысить уровень его безопасности. Не стал исключением и Internet Explorer 6. 9 сентября 2002 года корпорация Microsoft официально выпустила для него набор исправлений Service Pack 1 (Q326489), который находился на бета-тестировании с начала июля. Среди прочих были исправлены ошибка загрузки файлов по SSL-соединению при некэшированном соединении (Q323308) и ошибка NTLM аутентификации через SSL (Q325662).

SSL представляет собой протокол для обмена информацией в защищенном режиме, и на данный момент существуют версии SSL 2 и SSL 3, между которыми с пользовательской точки зрения не слишком большая разница. Пока неизвестно, появятся ли для самого популярного браузера новые «заплатки», но судя по тому, как растет популярность его конкурентов, разработчикам из Microsoft стоит всерьез побеспокоиться о судьбе своего детища.



▲ Управление параметрами уровней безопасности в IE 6.0 («Custom level»)



▲ Расширенные опции безопасности в IE 6.0 (SSL)

▲ Управление сертификатами и персональной информацией, хранящейся в IE 6.0

» а) Include all local (intranet) sites not listed in other zones — все локальные сайты, не указанные в других зонах. Это те сайты, в имена которых не входят точки (например, http://vasya, но не http://www.vasya.ru);

б) Include all sites that bypass the proxy server — все сайты, подключенные напрямую к прокси-серверу.

в) Include all network paths (UNCs) — все сетевые имена, такие как \\vasya\public\music и прочие.

Также, нажав на «Advanced», вам дается возможность добавить в эту зону необходимые локальные web-ресурсы самостоятельно. Чтобы добавить только поддерживающие HTTPS, активизируйте галочку «Require server verification (https:) for all sites in this zone»

- «Trusted sites» — надежные web-ресурсы, которым можно доверять. Все операции по добавлению сайтов аналогичны тому, как это происходит для зоны «Local intranet». Microsoft настоятельно рекомендует добавлять сюда только сайты с поддержкой HTTPS.
- «Restricted sites» — ненадежные web-ресурсы. Сюда заносятся сайты, содержимое которых может быть опасным для вашего компьютера.

Уровней безопасности предусмотрено тоже четыре, но, выбрав пункт меню «Custom level...», можно изменить настройки по своему вкусу.

- «High» — наивысший. Обеспечивает самый безопасный серфинг. Но некоторые страницы могут отображаться некорректно: отключены ActiveX, Java и другие небезопасные элементы. Данный уровень предназначен для работы с «Restricted sites»
- «Medium» — средний. Обычный уровень безопасности подходит для большинства web-сайтов, поэтому он рекомендуется для зоны «Internet».
- «Medium-low» — пониженный. От среднего уровня он отличается тем, что отключены запросы на загрузку многих компонентов. Рекомендуется для зоны «Local intranet».
- «Low» — низкий. По причине крайне низкой защищенности рекомендуется применять только для «Trusted sites».

Следует заметить, что, несмотря на многочисленные настройки, Internet Explorer заслужил славу дружелюбного, но плохо защищенного браузера. В нем неоднократно обнаруживались «дыры», которые разработчикам приходилось латать.

Вышеперечисленными пунктами настройки безопасности не исчерпываются. На вкладке «Advanced» почти в самом конце списка настроек (раздел «Security») находится управление SSL-протоколом: проверка аннулированных сертификатов, выбор используемых версий SSL и некоторые другие пункты. А на вкладке «Content» осуществляется управление сертификатами («Certificates»), автоматическим вводом паролей («Personal information -> AutoComplete...») и персональными данными («Personal information -> My Profile»).

Стоит отметить, что любой сертификат имеет определенный срок действия, по истечении которого становится недействительным. За этим обязательно нужно следить и вовремя аннулировать такие сертификаты, хранящиеся в базе вашего браузера.

Возможно, какие-либо пункты в IE покажутся вам излишними. Но если разобраться в них и уделить время настройке, то удобная работа в WWW вам обеспечена. По крайней мере, так нас заверяет Microsoft...

Но не стоит забывать, что при всей схожести настроек безопасности в браузерах могут быть допущены ошибки в реализации тех или иных методов защиты. С каким браузером работать — дело вкуса, но в вопросах безопасности ему доверять не приходится. Давать какие-либо рекомендации довольно сложно, поскольку если Internet Explorer более корректно отображает подавляющее большинство страниц, то с безопасностью у него дела обстоят не слишком хорошо. От себя скажу, что предпочитаю пользоваться Internet Explorer за его «адекватное» понимание HTML-кода. И Mozilla — за то, что вопросам безопасности его разработчики уделяют больше внимания, чем остальные.

Константин Николаенко

БРАУЗЕРЫ

Mozilla 1.0
Разработчик: Mozilla.org
http://mozilla.org
Условия распространения: freeware
Операционная система: Windows, Linux

Netscape Communicator 4.75
Разработчик: Netscape Communications Corporation
http://home.netscape.com
Условия распространения: freeware
Операционная система: Windows, Linux

Opera 6.04
Разработчик: Opera Software
www.opera.com
Условия распространения: adware
Операционная система: Windows, Linux

Internet Explorer 6.0
Разработчик: Microsoft
www.microsoft.com
Условия распространения: freeware
Операционная система: Windows