ТЕМА 2.1. Совместимость программного обеспечения

Лекция. Проверка ПК

План занятия:

1. **Проверка компьютера на наличие вирусов и шпионских программ.**
2. **Запуск обозревателя Internet Explorer в режиме «без дополнения».**

1. Проверка компьютера на наличие вирусов и шпионских программ.

Вредоносное ПО

Компьютеры и хранящиеся на них данные необходимо защитить от вредоносного ПО:

Вредоносное ПО (от английского malware (**mal** icious soft**ware**, то есть «вредоносное ПО») — это программное обеспечение, созданное для выполнения вредоносных действий.

Как правило, такие программы устанавливаются на компьютер без ведома пользователя. Эти программы открывают дополнительные окна на компьютере или меняют его настройки.

Вредоносное ПО может изменять настройки веб-браузера для открытия определенных веб-страниц, которые не нужны пользователю. Это называется перенаправлением браузера.

Они также могут собирать сведения, хранящиеся на компьютере, без ведома пользователя.

Первым и наиболее распространенным типом вредоносного ПО являются компьютерные вирусы. Вирус передается на другие компьютеры по электронной почте, на USB-накопителях, через обмен файлами и мгновенными сообщениями. Вирус

Вирусы могут:

- Изменить, повредить, удалить файлы и даже стереть все данные на жестком диске компьютера.
- Блокировать загрузку компьютера, препятствовать загрузке приложений или их правильной работе.
- Использовать учетную запись электронной почты пользователя для рассылки вируса на другие компьютеры.
- Бездействовать, пока их не активирует хакер.
- Фиксировать нажатия клавиш для захвата конфиденциальной информации, такой как пароли и номера кредитных карт, а затем отправлять собранные данные хакеру.

Компьютерный вирус – вид вредоносного программного обеспечения, способный создавать копии самого себя и внедрятся в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.

Компьютерные вирусы могут существовать в системе в разных **стадиях функционирования:**

1. **Латентная стадия.** На этой стадии код вируса находится в системе, но никаких действий не предпринимает. Для пользователя не заметен. Может быть вычислен сканированием файловой системы и самих файлов.

2. **Инкубационная стадия**. На этой стадии код вируса активируется и начинает создавать свои копии, распространяя их по устройствам хранения данных компьютера, локальным и глобальным компьютерным сетям, рассылая в виде почтовых сообщений и так далее. Для пользователя может быть заметен, так как начинает потреблять системные ресурсы и каналы передачи данных, в результате чего компьютер может работать медленнее, загрузка информации из Интернет, почты и прочих данных может замедлятся.

3. **Активная стадия**. На этой стадии вирус, продолжая размножать свой код доступными ему способами, начинает деструктивные действия, на которые ориентирован. Заметен пользователю, так как начинает проявляться основная функция вируса – пропадают файлы, отключаются службы, нарушается функционирование сети, происходит порча оборудования.

На сегодняшний день существует много компьютерных вирусов. Ежедневно появляется тысячи новых. Однако все это множество поддается классификации.

По **среде обитания** вирусы можно разделить на такие **виды**:

1. **Загрузочные вирусы.**
2. **Файловые вирусы.**
3. **Файлово-загрузочные вирусы.**
4. **Сетевые вирусы.**
5. **Документные вирусы.**

Загрузочные вирусы проникают в загрузочные сектора устройств хранения данных (жесткие диски, дискеты, переносные запоминающие устройства). При загрузке операционной системы с зараженного диска происходит активация вируса. Его действия могут состоять в нарушении работы загрузчика операционной системы, что приводит к невозможности ее работы, либо изменении файловой таблицы, что делает недоступным определенные файлы.

Файловые вирусы чаще всего внедряются в исполнительные модули программ (файлы с помощью которых производится запуск той или иной программы), что позволяет им активироваться в момент запуска программы, влияя на ее функциональность. Реже файловые вирусы могут внедрятся в библиотеки операционной системы или прикладного ПО, исполнительные пакетные файлы, файлы реестра Windows, файлы сценариев, файлы драйверов. Внедрение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии. Таким образом, вирус, находясь в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой ОС. Файловые вирусы – наиболее распространенный вид компьютерных вирусов.

Файлово-загрузочные вирусы объединяют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе компьютера.

Сетевые вирусы распространяются посредством сетевых служб и протоколов. Таких как рассылка почты, доступ к файлам по FTP, доступ файлам через службы локальных сетей. Что делает их очень опасными, так как заражение не остается в пределах одного компьютера или даже одной локальной сети, а начинает распространятся по разнообразным каналам связи.

Документные вирусы (их часто называют **макровирусами**) заражают файлы современных офисных систем (Microsoft Office, OpenOffice…) через возможность использования в этих системах макросов. **Макрос** – это заранее определенный набор действий, микропрограмма, встроенная в документ и вызываемая непосредственно из него для модификации этого документа или других функций. Именно макрос и является целью макровирусов.

По **методу существования в компьютерной среде** вирусы делятся на такие **виды**:

1. **Резидентные**
2. **Нерезидентные**

Резидентный вирус, будучи вызван запуском зараженной программы, **остается в памяти даже после ее завершения**. Он может создавать дополнительные процессы в памяти компьютера, расходуя ресурсы. Может заражать другие запущенные программы, искажая их функциональность. Может “наблюдать” за действиями пользователя, сохраняя информацию о его действиях, введенных паролях, посещенных сайтах и т.д.

Нерезидентный вирус является неотъемлемой частью зараженной программы и **может функционировать только во время ее работы**.

Однако не все компьютерные вирусы представляют серьезную угрозу. Некоторые вирусы тяжелых последствий после завершения своей работы не вызывают; они могут завершить работу некоторых программ, отображать определенные визуальные эффекты, проигрывать звуки, открывать сайты, или просто снижать производительность компьютера, резервируя под себя системные ресурсы. Таких вирусов подавляющее большинство. Однако есть и действительно опасные вирусы, которые могут уничтожать данные пользователя, документы, системные области, приводить в негодность операционную систему или даже аппаратные компоненты компьютера.

По **принципу своего функционирования** вирусы можно разделить на несколько **типов**:

1. **Вирусы-паразиты (Parasitic)** – вирусы, работающие с файлами программ, частично выводящие их из строя. Могут быть легко выявлены и уничтожены. Однако, зачастую, файл-носитель остается не пригодным.

2. **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится по всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются

3. **Трояны (Trojan)** – получили свое названия в честь “Троянского коня”, так как имеют схожий принцип действия. Этот вид вирусов маскирует свои модули под модули используемых программ, создавая файлы со схожими именами и параметрами, а так же подменяют записи в системном реестре, меняя ссылки рабочих модулей программ на свои, вызывающие модули вируса. Деструктивные действия сводятся к уничтожению данных пользователя, рассылке СПАМа и слежения за действиями пользователя. Сами размножатся зачастую не могут. Выявляются достаточно сложно, так как простого сканирования файловой системы не достаточно. «Троянский конь», или троян, обычно замаскирован под полезную программу, которая, однако, содержит вредоносный код. Например, трояны зачастую можно найти в бесплатных онлайн-играх. Пользователи загружают такие игры на компьютеры. Таким образом трояны попадают на компьютер. Во время игры троян устанавливается в систему и продолжает работать даже после закрытия игры. В таблице перечислены некоторые типы троянов.

Виды действий троянов	Описание
Удаленный доступ	Троян делает возможным несанкционированный удаленный доступ.
Отправка данных	Троян позволяет хакеру получить доступ к конфиденциальным данным, таким как пароли.
Разрушение данных	Троян повреждает файлы или удаляет их.
Прокси-сервер	Троян использует компьютер жертвы как источник для новых атак и противоправных действий.
FTP	Троян делает возможным несанкционированный обмен файлами на конечных устройствах.
Вывод из строя защитного ПО	Троян останавливает работу антивирусных программ или брандмауэров.
Отказ в обслуживании (DoS-атака)	Троян замедляет обмен данными по сети или полностью блокирует его.

4. **Вирусы-невидимки (Stealth)** – названы по имени самолета-невидимки "stealth", наиболее сложны для обнаружения, так как имеют свои алгоритмы маскировки от сканирования. Маскируются путем подмены вредоносного кода полезным во время сканирования, временным выведением функциональных модулей из работы в случае обнаружения процесса сканирования, сокрытием своих процессов в памяти и т.д.

5. **Самошифрующиеся вирусы** – вирусы вредоносный код которых хранится и распространяется в зашифрованном виде, что позволяет им быть недоступными для большинства сканеров.

6. **Матирующиеся вирусы** – вирусы не имеющие постоянных сигнатур. Такой вирус постоянно меняет цепочки своего кода в процессе функционирования и размножения. Таким образом, становясь неуязвимым для простого антивирусного сканирования. Для их обнаружения необходимо применять эвристический анализ.

7. **"Отдыхающие" вирусы** – являются очень опасными, так как могут очень продолжительное время находится в состоянии покоя, распространяясь по компьютерным сетям. Активация вируса происходит при определенном условии, зачастую по определенной дате, что может вызвать огромные масштабы одновременного заражения.

Типы угроз безопасности

Вредоносное ПО постоянно совершенствуется. В таблице приведены описания других типов вредоносного ПО.

Режимы безопасности	Описание
Черви	• Червь – самовоспроизводящаяся программа, наносящая вред сетям с целью замедлить операции по сети или блокировать их. • Обычно черви распространяются автоматически, используя известные уязвимости в легальном программном обеспечении.
Рекламное ПО	• Обычно распространяется путем загрузки программного обеспечения онлайн. • Такие программы отображают рекламу во всплывающем окне. • Часто всплывающие окна рекламного ПО трудно контролировать, и новые окна открываются быстрее, чем пользователь может их закрыть.
Шпионское ПО	• Аналогично рекламному ПО, но предназначено для сбора информации о пользователе и отправки полученных сведений другой стороне без ведома пользователя. • Шпионское ПО может представлять собой незначительную угрозу, собирая только данные о посещенных веб-страницах, или достаточно серьезную опасность, если его целью является сбор личной или финансовой информации.
Программы-вымогатели	• Такие программы похожи на рекламное ПО, однако служат для блокирования доступа к зараженной системе. • Зачастую в таких программах отображается сообщение с предложением заплатить злоумышленникам, чтобы снять блокировку.
Руткиты	• Программы, используемые хакерами для получения прав администратора компьютера. • Такие программы достаточно сложно обнаружить, поскольку они могут управлять защитными программами, чтобы скрыть свое существование. • Некоторые руткиты удается удалить с помощью специального ПО, но иногда для полного удаления требуется переустановка операционной системы.

Типы угроз безопасности

Фишинг (phishing)— это вид мошенничества, когда злоумышленник отправляет сообщение электронной почты, звонит по телефону или публикует текст с целью обманным путем получить от пользователя его личную или финансовую информацию. Фишинговые атаки также используются для того, чтобы пользователь сам того не зная установил вредоносное ПО на свои устройства.

Например, пользователь может получить электронное сообщение, которое может выглядеть как отправленное настоящей сторонней организацией, такой как банк. Хакер может обратиться с просьбой уточнить определенные реквизиты, например, пароли, имена пользователей или PIN-код, якобы ради предотвращения крайне нежелательных последствий. Если пользователь предоставил такую информацию, фишинговая атака считается успешной.

Существует также выборочный или прицельный фишинг (spear phishing). В этом случае фишинговая атака нацелена на определенного человека или организацию.

Организациям следует проводить для своих сотрудников обучающие мероприятия, на которых рассматриваются вопросы защиты от фишинговых атак. Как правило, конфиденциальная личная или финансовая информация не запрашивается в интерактивной форме. Настоящие организации не запрашивают конфиденциальную информацию по электронной почте. Будьте бдительны. При возникновении сомнений свяжитесь с организацией по почте или телефону, чтобы убедиться в действительности запроса.

Типы угроз безопасности

Спам, также называемый нежелательной или мусорной почтой, — это несанкционированные сообщения электронной почты. В большинстве случаев спам является одним из вариантов рекламы. Однако в спаме могут содержаться небезопасные ссылки, вредоносное ПО или обманный контент. Цель такого спама — получить конфиденциальную информацию, такую как номер социального страхования или сведения о банковском счете. Большинство спама отправляется множеством подключенных к сети компьютеров, зараженных вирусом или червем. Эти зараженные компьютеры отправляют максимально возможное число сообщений электронной почты.

Остановить спам невозможно, однако существуют способы снизить его поток. Например, большинство интернет-провайдеров блокируют спам до того, как он попадет в почтовый ящик пользователя. Многие антивирусные программы и почтовые клиенты имеют функцию автоматической фильтрации почты, как показано на рисунке. Это означают, что они обнаруживают и удаляют спам из папки входящих писем.

Даже если вы используете все эти функции защиты от спама, полностью исключить нежелательную почту все же не удастся. Ниже приведены некоторые наиболее распространенные признаки спама.

- В сообщении электронной почты отсутствует строка темы.
- Сообщение электронной почты запрашивает обновление учетной записи.

Типы угроз безопасности

- В тексте сообщения электронной почты содержатся неправильные написанные слова или странная пунктуация.
- Ссылки в сообщении электронной почты слишком длинные и/или непонятные.
- Сообщение электронной почты замаскировано под корреспонденцию от действительной организации.
- Сообщение электронной почты запрашивает открытие вложения.

Организациям также следует предупреждать сотрудников об опасности открытия почтовых вложений, которые могут содержать вирусы или черви. Не предполагайте, что почтовые вложения безопасны, даже если они отправлены от надежного контактного лица. Компьютер отправителя может быть заражен вирусом, который пытается распространить себя на другие компьютеры. Перед открытием почтовых вложений всегда проверяйте их.

Чтобы обнаружить, обезвредить и удалить вредоносное ПО, прежде чем оно успеет заразить компьютер, всегда используйте антивирусное ПО, решения для обнаружения шпионских программ и инструменты для удаления рекламного ПО.

Важно знать, что базы данных таких программ быстро устаревают. Поэтому обязательна установка актуальных обновлений, исправлений и определений вирусов в рамках регулярного обслуживания. Во многих организациях используется письменно зафиксированная политика безопасности, запрещающая сотрудникам устанавливать

Целевые платформы антивирусного ПО

На данный момент антивирусное ПО разрабатывается, в основном, для ОС семейства Windows от компании Microsoft. Это вызвано большим количеством вредоносных программ именно под эту платформу (а это, в свою очередь, вызвано большой популярностью этой ОС, так же, как и большим количеством средств разработки, в том числе бесплатных и даже «инструкций по написанию вирусов»). В настоящий момент на рынок выходят продукты и для других операционных систем, таких, к примеру, как Linux и Mac OS X. Это вызвано началом распространения компьютерных вирусов и под эти платформы, хотя UNIX-подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ.

Помимо ОС для настольных компьютеров и ноутбуков, также существуют платформы и для мобильных устройств, такие, как WindowsMobile, Symbian, AppleiOS, BlackBerry, Android, WindowsPhone 7 и др. Пользователи устройств на данных ОС также подвержены риску заражения вредоносным программным обеспечением, поэтому некоторые разработчики антивирусных программ выпускают продукты и для таких устройств.

Классификация антивирусных продуктов

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким, как: **используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.**

По используемым технологиям антивирусной защиты:

- **Классические антивирусные продукты** (продукты, применяющие только сигнатурный метод детектирования)
- **Продукты проактивной антивирусной защиты** (продукты, применяющие только проактивные технологии антивирусной защиты);
- **Комбинированные продукты** (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные)

По функционалу продуктов:

- **Антивирусные продукты** (продукты, обеспечивающие только антивирусную защиту)
- **Комбинированные продукты** (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)

По целевым платформам:

- **Антивирусные продукты для ОС семейства Windows**
- **Антивирусные продукты для ОС семейства *NIX** (к данному семейству относятся ОС BSD, Linux и др.)
- **Антивирусные продукты для ОС семейства MacOS**
- **Антивирусные продукты для мобильных платформ** (WindowsMobile, Symbian, iOS, BlackBerry, Android, WindowsPhone 7 и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации
- и т. д.

Лжеантивирусы

В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реального функционала для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением. В настоящий момент это распространение приостановлено.

Следует проявлять осторожность при выборе продукта для защиты, поскольку в Интернете встречаются мошеннические антивирусы. Большинство таких мошеннических антивирусов отображают рекламные или всплывающие сообщения, похожие на реальные предупреждения Windows, как показано на рисунке. В таких сообщениях обычно указывается на то, что компьютер заражен и требуется его очистка. При щелчке в любом месте такого окна может начаться загрузка и установка вредоносного ПО.

В случае заражения компьютера выполните указанные ниже действия.

1. Отключите зараженный компьютер от сети.
2. Следуйте политике реагирования на инциденты, которая может включать следующее:
   - Уведомление сотрудников ИТ-отдела
   - Сохранение файла журнала на съемный носитель
   - Выключение компьютера
   - Пользователям домашних компьютеров следует обновить все имеющиеся антивредоносные программы.
3. Необходимо загрузить компьютер с загрузочного диска для проверки. Может потребоваться загрузить компьютер в безопасном режиме.
4. После удаления вредоносного ПО на компьютере необходимо удалить файлы восстановления системы, чтобы исключить повторное заражение.

Программы защиты от вредоносного ПО

Для защиты компьютеров и мобильных устройств важно использовать надежное ПО для защиты от вредоносных программ. Ниже перечислены типы такого ПО, которое доступно на сегодняшний день.

- **Защита от вирусов** — такие программы постоянно отслеживают систему на предмет наличия в ней вирусов. При обнаружении вируса программа уведомляет об этом пользователя и пытается удалить вирус или поместить его в карантин.
- **Защита от рекламного ПО** — программы защиты от рекламного ПО выполняют поиск программ, отображающих рекламу на компьютере.
- **Защита от фишинга** — такие программы блокируют IP-адреса известных фишинговых веб-сайтов и предупреждают пользователя о подозрительных сайтах.
- **Защита от шпионского ПО** — эти программы проверяют компьютер на наличие клавиатурных шпионов и другого шпионского ПО.
- **Надежные/ненадежные источники** — такие программы предупреждают пользователя о небезопасных программах и веб-сайтах, которые он собирается установить или посетить.

Для удаления всего вредоносного ПО может потребоваться использовать несколько различных программ и выполнять поиск несколько раз. Запускайте только одну программу защиты от вредоносного ПО одновременно.

Некоторые авторитетные разработчики, такие как McAfee, Symantec, Kaspersky, предлагают решения для комплексной защиты компьютеров и мобильных устройств.

При появлении подозрительного окна с предупреждением никогда не щелкайте это окно. Закройте вкладку или обозреватель, чтобы убрать окно с предупреждением. Если вкладка или обозреватель не закрываются, нажмите сочетание клавиш **ALT+F4**, чтобы закрыть окно, или используйте диспетчер задач для завершения работы программы. Если окно с предупреждением не закрывается, проверьте компьютер, используя общепризнанную актуальную антивирусную программу, чтобы убедиться, что он не заражен.

К неутвержденному или не соответствующему требованиям программному обеспечению относятся не только программы, которые устанавливаются на компьютер непреднамеренно. Это могут быть программы, предоставленные пользователями с намерением установить их. Возможно, они не вредоносные, однако не исключено, что они могут нарушить политику безопасности. Такая система, не соответствующая требованиям, может нарушить работу программного обеспечения компании или сетевых сервисов. Неутвержденное программное обеспечение следует удалять

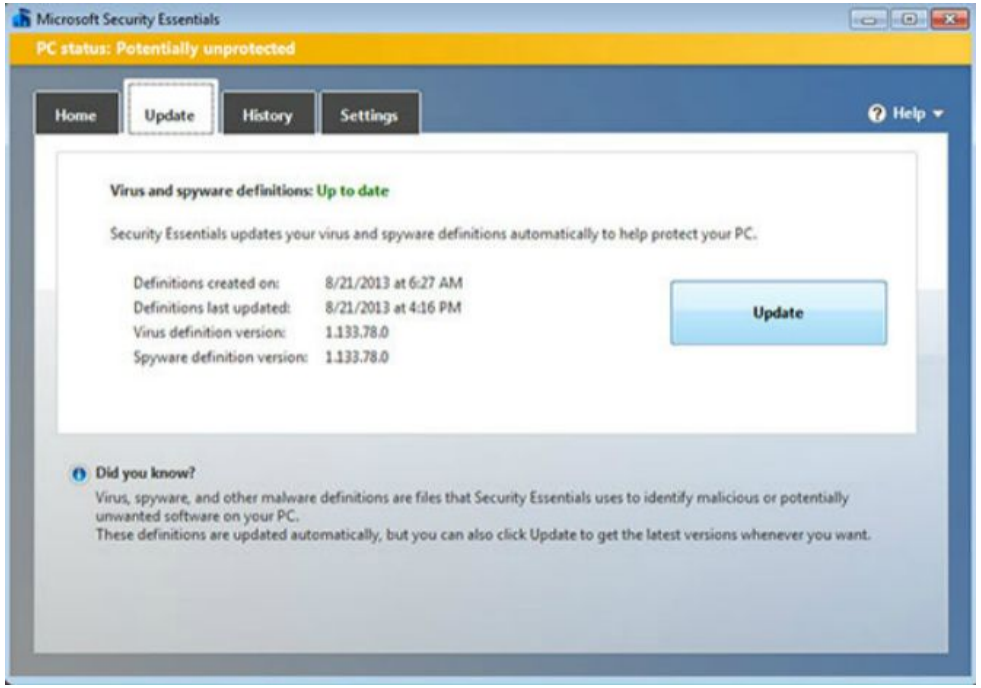
Обновления файлов сигнатур

Производители программного обеспечения должны регулярно создавать и выпускать новые исправления для устранения ошибок и уязвимостей в продуктах. Поскольку постоянно разрабатываются новые вирусы, программное обеспечение безопасности должно постоянно обновляться. Этот процесс может выполняться автоматически, но инженер должен знать, как обновлять любые типы программного обеспечения безопасности и все клиентские программы вручную.

Вредоносные программы ищут шаблоны в коде программного обеспечения на компьютере. Эти шаблоны определяются путем анализа вирусов, перехваченных в Интернете и локальных сетях. Эти шаблоны кода называются сигнатурами. Издатели защитного ПО компилируют сигнатуры в таблицы определений вирусов. Перед обновлением файлов сигнатур для защиты от вирусов сначала убедитесь, что используются файлы сигнатур последней версии. Для проверки состояния файла выберите пункт **О программе** в программе для защиты или запустите средство обновления программы.

Всегда получайте файлы сигнатур с веб-сайта производителя, чтобы обеспечить подлинность обновления и отсутствие повреждений, вызванных вирусами. Это может создать большую нагрузку на веб-сайт производителя, особенно при появлении новых вирусов. Чтобы избежать создания чрезмерного трафика для одного веб-сайта, некоторые производители выпускают файлы сигнатур для загрузки на нескольких сайтах. Эти сайты загрузки называются зеркалами.

ВНИМАНИЕ! При загрузке файлов сигнатур с зеркала убедитесь, что сайт зеркала не является поддельным. Всегда переходите на сайт зеркала с веб-сайта производителя.



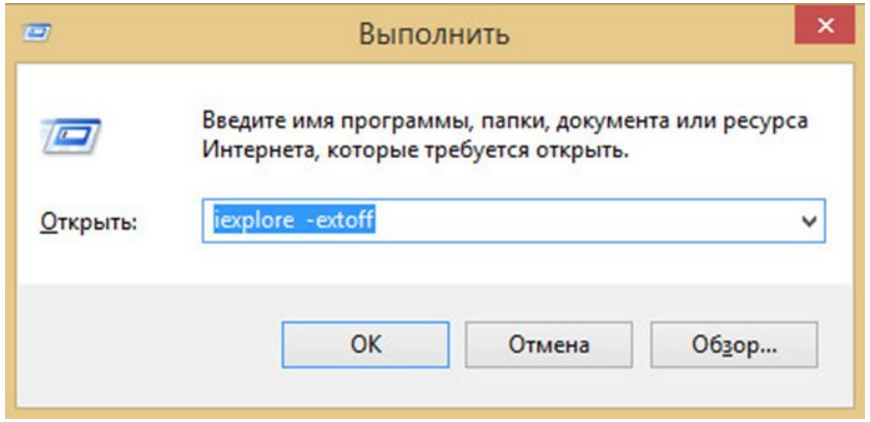
2. Запуск обозревателя Internet Explorer в режиме «без дополнения»

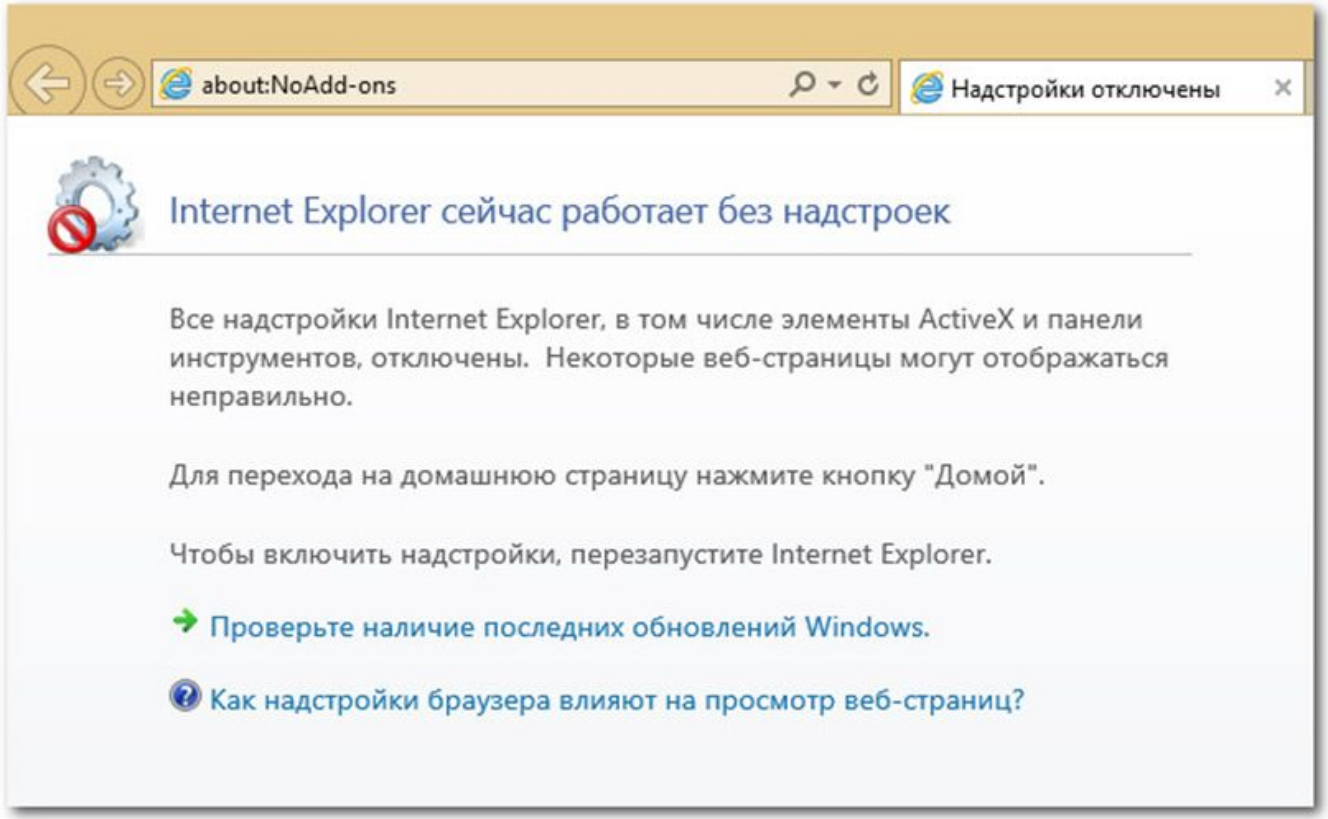
Использование плагинов позволяет существенно расширить возможности современных браузеров. Подавляющее большинство плагинов сторонние, требующие отдельной установки и только очень немногие из них поставляются вместе с браузером. Таковыми, к примеру, являются надстройки и компоненты ActiveX в Internet Explorer. Вряд ли кому-то придёт в голову отрицать полезность браузерных расширений. Расширения, встроенные и сторонние позволяют не только просматривать веб-контент, но и обрабатывать его различными способами.

Но есть у плагинов один общий недостаток. Слишком большое их количество замедляет работу браузера и снижает уровень безопасности. Поэтому в некоторых случаях имеет смысл временного отключения дополнений. Для этого в Internet Explorer предусмотрена специальная опция доступная из пускового меню «**Все программы**». Она так и называется — **Internet Explorer (без надстроек).**

В Windows 8 и 8.1 для запуска IE с отключенными надстройками лучше использовать команду **iexplore –extoff**. Выполнять её следует в окошке «**Выполнить**». Этот простой способ может быть использован в случае внезапного краха IE, вызванного установкой недоброка

После выполнения команды **iexplore –extoff** браузер будет запущен как обычно, но при этом вы получите сообщение о том, что Internet Explorer сейчас работает без надстроек.





Повторный запуск браузера через **Панель управления** или с помощью ярлыка на **Рабочем столе** производится уже в обычном режиме с работающими надстройками.

Обеспечение безопасности веб-трафика

Хакеры используют различные веб-средства (например, ActiveX, Flash), чтобы установить вредоносное ПО на компьютер.

Для предотвращения таких действий в браузерах имеются средства, позволяющие повысить безопасность веб-трафика:

- ***Фильтрация ActiveX***
- ***Программа блокировки всплывающих окон***
- ***Фильтр SmartScreen***
- ***Просмотр InPrivate***