

Руководство по безопасности Internet Explorer®8

Набор средств для управления соответствием требованиям безопасности

**Версия 1.0**

Дата опубликования: октябрь 2009 г.

Последние изменения см. на microsoft.com/ssa

Copyright © 2009 Корпорация Майкрософт. Все права защищены. Читатель несет ответственность за соблюдение применимого законодательства в области охраны авторских прав. Используя настоящую документацию или предоставляя отзыв на нее, вы соглашаетесь со следующим лицензионным соглашением.

Если эта документация используется исключительно в некоммерческих целях внутри ВАШЕЙ компании или организации, то на нее вам предоставляется лицензия Creative Commons Attribution-NonCommercial License. Копию текста этой лицензии можно получить на веб-сайте http://creativecommons.org/licenses/by-nc/2.5/ или отправив запрос по адресу Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

Настоящая документация предоставляется исключительно в целях ознакомления и исключительно по принципу «как есть» («AS IS»). Использование вами настоящей документации не может расцениваться как полноценная замена тем услугам и информационным материалам, что корпорация Майкрософт может разработать и предоставить вам, отталкиваясь от ваших специфических условий работы. В максимальной степени, разрешенной законом, КОРПОРАЦИЯ МАЙКРОСОФТ ОТКАЗЫВАЕТСЯ ОТ ЛЮБЫХ ГАРАНТИЙ, ЯВНЫХ, ПОДРАЗУМЕВАЕМЫХ ИЛИ ПРЕДПИСАННЫХ, И НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБОЙ УЩЕРБ, ВОЗНИКШИЙ В СВЯЗИ С ДАННЫМИ МАТЕРИАЛАМИ ИЛИ ЛЮБОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ, СОДЕРЖАЩЕЙСЯ В НИХ.

На материалы, содержащиеся в этой документации, может распространяться действие патентов, заявок на патенты, товарных знаков или других прав на интеллектуальную собственность корпорации Майкрософт. Без отдельного соглашения с корпорацией Майкрософт использование этого документа не предоставляет вам никаких прав на эти патенты, товарные знаки или иные объекты интеллектуальной собственности.

Сведения, приведенные в документе, включая URL-адреса и иные ссылки на веб-сайты, могут быть изменены без предварительного уведомления. Все компании, организации, продукты, доменные имена, адреса электронной почты, логотипы, люди, места и события, упомянутые в примерах, являются вымышленными, если не указано обратное.

Microsoft, Access, Active Directory, ActiveX, Authenticode,Excel, InfoPath, Internet Explorer, Internet Explorer 8, JScript,MSDN,Outlook, PowerPoint, Visual Basic, Windows, Windows Server, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista и Windows XP являются либо зарегистрированными товарными знаками, либо товарными знаками корпорации Майкрософт в США и (или) в других странах.

Упомянутые названия реально существующих компаний и продуктов могут быть торговыми марками их владельцев.

Вы не обязаны предоставлять в Майкрософт какие бы то ни было комментарии, предложения или иные отзывы («Отзывы») по данной документации. Однако, если вы представляете в Майкрософт какой-либо Отзыв, вы тем самым безвозмездно наделяете Майкрософт правом использовать этот Отзыв, передавать его другим лицам и извлекать из него прибыль, любым способом и с любой целью. Вы также безвозмездно предоставляете третьим лицам любые патентные права, необходимые, чтобы их продукты, технологии или услуги могли использовать или взаимодействовать с любыми частями программного обеспечения или услуг Майкрософт, включающими этот Отзыв. Вы не можете представить Отзыв, который подразумевает обязанность Майкрософт в случае использования этого Отзыва в каком-либо ее продукте или документации передавать этот продукт или документацию третьим лицам только по лицензии.

Содержание

Обзор 1

Кому адресовано это руководство 3

Навыки и уровень подготовки 3

Назначение и область применимости руководства 3

Аннотация к главам 4

Способы оформления 6

Дополнительные сведения 6

Поддержка и отзывы 6

Благодарности 7

Авторский коллектив 7

Приняли участие 8

Глава 1. Создание базовой конфигурации безопасности для Internet Explorer 8 9

Ограничивайте привилегии пользователей 10

Среда корпоративных клиентов 10

Среды с особыми параметрами безопасности и ограниченной функциональностью 11

Администрирование Internet Explorer 8 11

Основные сведения о зонной модели 13

Изменение параметров зон 15

Определение зоны 16

За пределами зонной модели: общие параметры безопасности 16

Проектирование подразделений для применения политик безопасности Internet Explorer 8 17

Подразделение отдела 18

Подразделение пользователей Windows 7 18

Подразделение компьютеров с Windows 7 19

Схема объектов групповой политики для политик безопасности 19

Средства обеспечения безопасности и конфиденциальности в Internet Explorer 8 22

Фильтр SmartScreen 23

Защита от фишинга и вредоносных программ 23

Защита от ClickJacking 24

Фильтр запуска сценариев между узлами (XSS) 25

Выделение домена 25

Защищенный режим Internet Explorer 25

Явное согласие на запуск элементов ActiveX 26

Просмотр в режиме InPrivate 27

Фильтрация InPrivate 27

Дополнительные сведения 28

Отзывы 28

Глава 2. Рекомендации по обеспечению безопасности Internet Explorer 8 29

Управление надстройками 29

Ограничение элементов ActiveX 30

Управление настройками ActiveX на уровне узла 30

Использование элементов ActiveX, подключаемых модулей и предварительно утвержденных списков 31

Отключение активных сценариев 31

Поддержка сценариев 33

Включение ограничений безопасности для обрабатываемых сценариями окон 33

Обеспечение безопасности с помощью зон 34

Включение защиты от повышения уровня зоны 34

Не разрешайте пользователям добавлять в зону узлы или удалять узлы из зоны 35

Не разрешайте пользователям изменять политики для зон безопасности 36

Обеспечение безопасности с помощью сертификатов 37

Запрещайте пользователям доступ к узлам с ошибочными сертификатами 37

Понижение уровня привилегий приложения 38

Включайте защищенный режим 38

Используйте приложение DropMyRights в Windows XP 39

Прочие параметры безопасности 40

Возможность пробной проверки MIME 40

Ограничение безопасности для MK-протокола 40

Не сохраняйте зашифрованные страницы на диске 41

Задавайте параметры прокси для компьютера, а не для пользователя 42

Отключайте обнаружение аварийных сбоев 43

Включайте ограничение загрузки файлов 44

Запрещайте загрузку файлов для зоны «Ограниченные узлы» 45

Пользуйтесь функцией защиты кэшируемых объектов 46

Разрешения Java 46

Дополнительные сведения 47

Отзывы 47

Глава 3. Рекомендации по настройке конфиденциальности 49

Просмотр в режиме InPrivate 50

Фильтрация InPrivate 50

Удаление истории обзора 51

Перемещение ползунка конфиденциальности в положение «Средний» или «Умеренно высокий» 51

Автоматическая очистка папки временных файлов Интернета 52

Отключение автоматического заполнения форм 53

Задание параметров входа для каждой зоны 55

Включение фильтра SmartScreen 57

Фильтр запуска сценариев между узлами (XSS) 59

Дополнительные сведения 60

Отзывы 60

Приложение А. Контрольный список параметров безопасности Internet Explorer 8 61

Дополнительные сведения 62

Отзывы 62

Обзор

Приглашаем вас ознакомиться с *Руководством по безопасности* *Internet Explorer 8*. В настоящем руководстве содержатся инструкции и рекомендации о том, как повысить безопасность настольных и портативных компьютеров, на которые установлен обозреватель Windows®Internet Explorer® 8.

Одна из самых сложных проблем при определении задаваемых по умолчанию параметров веб-обозревателя заключается в том, как соблюсти баланс между необходимой функциональностью и сопряженными с этой функциональностью рисками. Если установленные по умолчанию параметры обозревателя излишне ограничительны, то пользователь постоянно будет испытывать при работе различные помехи и сложности из-за несовместимости и потому просто перестанет обращать внимание на предупреждения и уведомления. Если же параметры недостаточно ограничительны, то пользователь уязвим для атак со стороны многочисленных эксплойтов. Отыскание разумного баланса между двумя вышеупомянутыми аспектами исключительно важно для обеспечения безопасности и простоты работы.

Разработчики веб-обозревателей обычно определяют действующие по умолчанию параметры безопасности, так чтобы обеспечить максимальное удобство работы при точно рассчитанном риске. Принимая решения с учетом известных сценариев атак, взвешивая факторы, необходимые для эксплуатации потенциальных уязвимостей, разработчик подбирает параметры безопасности по умолчанию, которые позволяли бы обозревателю работать в широком диапазоне условий. Параметров обозревателя по умолчанию обычно достаточно для удовлетворения потребностей большинства пользователей домашних компьютеров и защиты их от большей части атак.

Однако у некоторых потребителей и корпоративных пользователей могут возникать специфические требования, обусловленные особенностями бизнеса, законодательством или внутриведомственными инструкциями. Например, иногда сотрудники крупных организаций обязаны соблюдать постановления правительства о защите тех финансовых данных и информации о клиентах, которая хранится на сетевых серверах.

Параметры безопасности и конфиденциальности в Internet Explorer 8 спроектированы для работы при самых разных требованиях, что еще больше упрочивает лидирующие позиции корпорации Майкрософт в сфере безопасности. Мы принимаем во внимание как право пользователей на защиту частной жизни, так и потребность организаций в контроле над использованием данных, и вытекающий отсюда спрос на рекомендации по соблюдению баланса между тем и другим. Internet Explorer 8 предлагает улучшенные средства обеспечения безопасности по сравнению с предыдущими версиями обозревателя, а также новые возможности по обеспечению конфиденциальности, позволяющие пользователю управлять своими личными данными. Дополнительные сведения о новых средствах и параметрах можно найти на веб-узле [Internet Explorer 8](http://go.microsoft.com/fwlink/?LinkId=122516).

В настоящем руководстве рассматриваются некоторые средства и параметры, изменив которые, можно организовать более «защищенную от изменений» конфигурацию безопасности, необходимую части пользователей и предприятий. Здесь вы не найдете полного обзора всех параметров безопасности обозревателя, а предлагаемые рекомендации отнюдь не эквивалентны тем, что реализованы в конфигурации Internet Explorer Enhanced Server Configuration (IE ESC) в операционных системах Windows Server® 2003 и Windows Server® 2008. Для обсуждения в настоящем руководстве отобраны те параметры и средства, которые могут быть полезны максимально широкой аудитории пользователей и администраторов на предприятиях, нуждающихся в повышенной безопасности.

Здесь обсуждаются параметры безопасности Internet Explorer® 8 для Windows® 7, Windows Vista® и Windows® XP. ИТ-профессионалы могут воспользоваться настоящим руководством для усиления параметров безопасности обозревателя в соответствии с потребностями предприятия.

**Примечание:**  Во многих случаях администраторы могут воспользоваться набором средством Internet Explorer Administration Kit (IEAK), чтобы создать заказную сборку Internet Explorer, развернуть ее на предприятии и затем организовать принудительное применение новых параметров с помощью групповой политики. В этом руководстве набор средств IEAK подробно не рассматривается, но многие из описанных здесь параметров можно использовать при создании заказного пакета.

# Кому адресовано это руководство

*Руководство по безопасности Internet Explorer 8* адресовано, прежде всего, ИТ-специалистам широкого профиля, специалистам в области безопасности, проектировщикам сетей, консультантам и других сотрудникам сферы ИТ, кто занят проектированием или развертывания приложений либо инфраструктуры на настольных и портативных ПК с одной из поддерживаемых клиентских операционных Windows в широком спектре организаций.

## Навыки и уровень подготовки

Руководство рассчитано на читателей, занятых разработкой, развертыванием и обеспечением безопасности клиентских компьютеров с установленным обозревателем Internet Explorer 8, обладающих следующих навыками и опытом:

* Сертификация MCSE по Windows Server 2003 или более поздняя и опыт работы не менее двух лет в области обеспечения безопасности, либо эквивалентный уровень подготовки.
* Глубокое понимание домена предприятия и рабочей среды Active Directory.
* Опыт работы с консолью управления групповой политикой (GPMC).
* Опыт администрирования групповой политики с помощью консоли GPMC, единого инструмента по управлению всеми задачами, связанными с групповой политикой.
* Опыт работы с такими средствами администрирования, как консоль управления (MMC), Gpupdate и Gpresult.

Опыт развертывания приложений и клиентских компьютеров в корпоративной среде.

## Назначение и область применимости руководства

Основные цели настоящего руководства:

* предоставить готовые методики эффективного создания и внедрения проверенных параметров безопасности с помощью групповой политики;
* объяснить причины, стоящие за теми или иными рекомендуемыми параметрами безопасности, а также последствия от их установки;
* выявить и рассмотреть типичные сценарии обеспечения безопасности и показать, как заложенные в Internet Explorer 8 средства позволяют реагировать на них в конкретной среде.

Руководство построено так, чтобы можно было с успехом изучить лишь ту его часть, что актуальна для конкретного предприятия. Однако наибольшую пользу читатель получит, ознакомившись с руководством целиком. Оно посвящено вопросу создания и поддержания безопасной среды для компьютеров с установленным Internet Explorer 8. Здесь же описываются различные этапы обеспечения безопасности двух совершенно различных сред. В руководстве содержатся как предписания, так и рекомендации. На клиентском компьютере может быть установлена операционная система Windows 7 или Windows Vista с пакетом обновлений SP1 или выше. Однако на компьютере, с которого производится управление клиентскими компьютерами, должна быть установлена ОС Windows Server 2008, Windows Server 2003 R2 или Windows Server 2003 SP2.

Имеются различия между параметрами, присутствующими в редакторе групповых политик и в окне конфигурации Internet Explorer – **Свойства обозревателя**. Так, многие параметры, реализуемые с помощью групповых политик, отсутствуют в окне **Свойства обозревателя**, например, все параметры в папке **Конфигурация компьютера\Административные шаблоны\Компоненты Windows \Internet Explorer\Панель управления обозревателем\Страница безопасности\Заблокированная зона Интернета**.

Отметим также, что многие параметры, присутствующие в папке «Административные шаблоны» редактора групповых политик, хранятся в специальных разделах реестра:

HKEY\_LOCAL\_MACHINE\Software\Policies

HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Common\DRM

Настройки, установленные в окне **Свойства обозревателя**, сохраняются в другом разделе, например, HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1. Групповая политика устроена таким образом для того, чтобы избежать проблем, связанных с параметрами, составляющими *постоянную сигнатуру* системы (tattoo). Однако такое соглашение может вводить в заблуждение при попытке сравнить результаты конфигурирования с помощью групповых политик и окна **Свойства обозревателя**.

**Примечание.**  Термин *постоянная сигнатура* в этом контексте описывает ситуацию, когда некоторые параметры групповых политик продолжают действовать даже после того, как компьютер или учетная запись пользователя вышли из области действия групповой политики. Например, все настройки в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности** входят в состав постоянной сигнатуры системы, если она конфигурируется посредством доменной групповой политики.

# Аннотация к главам

*Руководство по безопасности Internet Explorer 8* состоит из трех глав и одного приложения.

Глава 1. Реализация базовой конфигурации безопасности для Internet Explorer 8

В этой главе предлагается набор процедур для реализации предписанных параметров безопасности, усиливающих уровень безопасности, установленный по умолчанию для Internet Explorer 8 на клиентских компьютерах. Здесь же детально обсуждается рекомендованная конфигурация развертывания групповой политики и рассматривается поддержка двух сред с разными требованиями к безопасности.

Глава 2. Рекомендации по обеспечению безопасности Internet Explorer 8

В этой главе приводится подробная информация об относящихся к безопасности средствах Internet Explorer 8 и связанных с ним параметров групповой политики. Рекомендации по использованию средств и параметров разбиты на шесть категорий:

управление надстройками;

отключение активных сценариев;

обеспечение безопасности с помощью зон;

обеспечение безопасности с помощью сертификатов;

понижение уровня привилегий приложения;

прочие параметры безопасности;

Для каждого параметра приводятся пояснения, в которых описано, для чего он предназначен, как установлен по умолчанию и как его рекомендуется установить в средах с различными требованиями к безопасности.

Глава 3. Рекомендации по настройке конфиденциальности

В этой главе подробно описываются средства и параметры групповой политики для Internet Explorer 8, относящиеся к конфиденциальности. Речь идет главным образом о просмотре в режиме InPrivate и функции SmartScreen.

Приложение A. Контрольный список параметров безопасности Internet Explorer 8

В этом приложении содержится контрольный список всех рассмотренных параметров, на которые мы рекомендуем обратить внимание в процессе обеспечения безопасности клиентских компьютеров с установленным Internet Explorer 8 на конкретном предприятии.

## Способы оформления

В настоящем руководстве применяются следующие способы оформления.

| Оформление | Значение |
| --- | --- |
| **Полужирный шрифт** | Так выделяется текст, который следует вводить буквально, в том числе команды, флаги и имена файлов. Так же выделены элементы пользовательского интерфейса. |
| *Курсив* | *Курсивом* выделяются названия книг и других существенных публикаций, а также новые термины при первом упоминании. |
| *<Курсив>* | Курсивом в угловых скобках, например *<имя\_файла>*, обозначают переменные. |
| Моноширинный шрифт | Таким шрифтом записываются примеры кода и сценариев. |
| **Примечание** | Обращает ваше внимание на сопутствующую информацию. |
| **Важно** | Важная информация, необходимая для успешного выполнения задачи. |
| Exclam **Внимание!** | Обозначает особо важное примечание, которое не стоит игнорировать. |
| ‡ | Этим символом обозначены конкретные изменения в параметрах групповой политики или рекомендации. |
| § | Этим символом обозначены параметры групповой политики, впервые появившиеся в Windows 7. |

## Дополнительные сведения

Подробнее о вопросах безопасности Internet Explorer 8 можно узнать из следующих источников на Microsoft.com:

Домашняя страница [Internet Explorer 8](http://go.microsoft.com/fwlink/?LinkId=122516).

## Поддержка и отзывы

Группа Solution Accelerators – Security and Compliance (SA–SC) ценит все отзывы об этом и других своих продуктах.

Просьба направлять замечания по следующему адресу:

Электронная почта [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).

Нам очень важно ваше мнение.

# Благодарности

Группа Solution Accelerators – Security and Compliance (SA–SC) выражает благодарность группе, работавшей над созданием *Руководства по безопасности* Internet Explorer 8. Следующие лица принимали непосредственное участие или внесли значительный вклад в написание, разработку и тестирование настоящего решения.

## Авторский коллектив

Авторы текста

Курт Диллард (Kurt Dillard) – *kurtdillard.com*

Ричард Харрисон (Richard Harrison) – Content Master Ltd.

Разработчики

Барри Хартман (Barry Hartmann)

Джеральд Гербо (Gerald Herbaugh)

Хай Кун Чжан (Haikun Zhang) – *Beijing ZZZGroup Co. Ltd*

Джефф Сигман (Jeff Sigman)

Джим Гроувз (Jim Groves)

Жозе Маллдонадо (José Maldonado)

Майкл Тэн (Michael Tan)

Жи Киянь Юань (ZhiQiang Yuan) – *Beijing ZZZGroup Co. Ltd*

Редакторы

Джон Кобб (John Cobb) – Wadeware LLC

Стив Уэкер (Steve Wacker) – Wadeware LLC

Менеджеры группы

Мишель Арни (Michelle Arney)

Шрути Кала (Shruti Kala)

Стефани Чачарон (Stephanie Chacharon) – *Xtreme Consulting Group Inc.*

Руководитель проекта

Том Клоуорд (Tom Cloward)

Выпускающие менеджеры

Чери Альбек (Cheri Ahlbeck) – *Aquent LLC*

Карина Ларсон (Karina Larson)

Менеджер по тестированию

Саммит Парих (Sumit Parikh)

Тестеры

Жайдип Бахадур (Jaideep Bahadur) – *Infosys Technologies Ltd.*

Манси Шарма (Mansi Sharma) – *Infosys Technologies Ltd.*

Раксит Гайяр (Raxit Gajjar) – Infosys Technologies Ltd.

## Приняли участие

Арон Маргосис (Aaron Margosis), Блейк Франц (Blake Frantz) – *Center for Internet Security*, Дэн Фокс (Dan Fox), Дэниэл Тэйлор (Daniel Taylor), *Агентство по оборонным информационным системам* (*DISA*), Фиделис Экезю (Fidelis Ekezue), Грег Коттингэм (Greg Cottingham), Гай Хант (Guy Hunt), Кэти Ламберт (Kathy Lambert), Лори Кингери (Lori Kingery), Мэнди Тидвелл (Mandy Tidwell), Нэйт Морин (Nate Morin), Пит Лепаж (Pete LePage), Рик Манк (Rick Munck), Роджер Граймс (Roger Grimes), Роджер Подвоски (Roger Podwoski), Сьюзан Фоссельман (Susan Fosselman), Стивен Рольник (Steven Rolnick), Тим Кларк (Tim Clark), Ти-Джей Онишил (TJ Onishile), Юнь Чоу (Yung Chou)

**Примечание.** По просьбе Майкрософт в рецензировании этого руководства принимал участие директорат информационной безопасности Агентства национальной безопасности США, замечания которого были учтены в опубликованной версии.

**Примечание.** В разработке настоящего руководства и соответствующих параметров безопасности приняли участие члены сообщества Center for Internet Security, чьи замечания были учтены в опубликованной версии.

Глава 1. Создание базовой конфигурации безопасности для Internet Explorer 8

Версия Windows® Internet Explorer® 8 базируется на усовершенствованиях в области безопасности, которые были включены в Internet Explorer 7. В очередную версию корпорация Майкрософт включила несколько новых средств и проектных решений, например защищенный режим и функцию ActiveX® Opt-In, чтобы обеспечить несколько уровней защиты в соответствие с концепцией глубоко эшелонированной обороны. Другие новые функции, например фильтр фишинга, помогают защитить пользователя от атак, направленных на получение личной информации. Подробное описание усовершенствований в области безопасности, появившихся в предыдущих версиях Internet Explorer, выходит за рамки настоящего руководства. Дополнительные сведения об этих усовершенствованиях см. на веб-странице [Internet Explorer TechCenter](http://technet.microsoft.com/ie).

Улучшения, включенные в Internet Explorer 8, направлены на защиту пользователей от многих новейших сетевых угроз и предоставление более простого и понятного интерфейса, облегчающего принятие решений о безопасности. Настройки, установленные в Internet Explorer 8 по умолчанию, призваны обеспечить соотношение между удобством работы и безопасностью, подходящее для широкого круга пользователей по всему миру. Кроме того, в Internet Explorer 8 добавлен совершенно новый набор средств и элементов управления конфиденциальностью, которые дают пользователю возможность контролировать свои действия в сети и сохраняемую о них информацию.

В настоящем руководстве рассматриваются способы повысить безопасность работы с обозревателем путем изменения параметров, разбитые на шесть основных категорий:

элементы управления ActiveX;

элементы управления конфиденциальностью;

прочие настройки безопасности;

зоны безопасности;

настройки безопасности (safety settings);

фильтр SmartScreen.

В настоящем руководстве упор делается на параметры безопасности в Internet Explorer 8. Однако любой документ, посвященный оптимальной настройке безопасности конкретного приложения, обязательно должен включать сведения о безопасности на уровне всего компьютера. Этой теме посвящены руководства по безопасности Windows® 7 и Windows Vista®. Кроме того, чтобы не стать жертвой уязвимости в обозревателе, надстройках над ним и операционной системе, необходимо регулярно обновлять их. Мы рекомендуем устанавливать все обновления операционной системы с помощью таких средств, как Windows Server® Update Services (WSUS), Systems Management Server (SMS) 2003, System Center Configuration Manager 2007 или «Автоматическое обновление», поддерживая систему в актуальном состоянии. Добавим еще, что клиентам рекомендуется подписаться на рассылку технической информации по вопросам безопасности с веб-узла [Microsoft Technical Security Notifications](http://go.microsoft.com/fwlink/?LinkId=21163). Дополнительные сведения см. в приложении A «Контрольный список параметров безопасности для Internet Explorer 8».

Ужесточить заданную по умолчанию конфигурацию обозревателя позволяют объекты групповой политики (GPO). Все рекомендованные параметры групповой политики документированы в файле Excel® Internet Explorer 8 Security Baseline Settings.xls, прилагаемом к настоящему руководству.

Для развертывания параметров, описанных в этой главе, понадобится:

создать нужную структуру подразделений (OU);

с помощью средства GPOAccelerator создать нужные объекты групповой политики;

с помощью консоли управления групповой политикой (GPMC) связать и упорядочить объекты групповой политики.

Exclam **Внимание!**Необходимо тщательно протестировать созданные подразделения и объекты групповой политики перед их развертывание их в производственной среде.

Базовые объекты GPO, прилагаемые к настоящему руководству, содержат сочетание проверенных настроек, которые повышают уровень безопасности клиентских компьютеров с установленной ОС Windows 7 в следующих двух средах с разными требованиями к безопасности:

**Корпоративный клиент** (Enterprise Client, EC)

**Особые параметры безопасности и ограниченная функциональность (**Specialized Security – Limited Functionality, SSLF**)**

# Ограничивайте привилегии пользователей

Одна из самых эффективных мер по защите компьютеров, работающих под управлением ОС Windows® XP, Windows Vista и Windows 7, состоит в том, чтобы при повседневной работе пользователи входили в систему от имени стандартных учетных записей. Использовать записи с дополнительными привилегиями следует лишь для выполнения административных задач. То же самое относится и к веб-обозревателям. При обычных условиях пользователь должен запускать Internet Explorer со стандартными привилегиями, тогда он будет работать в защищенном режиме, снижая тем самым риск того, что вредоносные программы смогут нанести вред компьютеру. В этом режиме гарантируется, что если даже компьютер подвергся атаке вредоносной программы, она сможет воздействовать лишь на профиль данного пользователя, так как работает с его привилегиями. Еще один важный момент состоит в том, что пользователь с привилегиями администратора способен изменить обсуждаемые в настоящем руководстве настройки и тем самым увеличить риск компрометации.

# Среда корпоративных клиентов

Среда корпоративных клиентов (среда EC), как она понимается в настоящем руководстве, — это домен на основе AD DS, в котором компьютеры с ОС Windows Server® 2008 R2, Windows Server® 2008, Windows Server® 2003 R2 или Windows Server® 2003 с пакетом обновления 2 (SP2), а также службы AD DS управляют клиентскими компьютерами с ОС Windows 7, Windows Vista SP2 и Windows XP Professional SP3. Управление клиентскими компьютерами осуществляется через групповую политику, которая применяется на уровне сайтов, доменов и подразделений. Групповая политика представляет централизованную инфраструктуру в рамках AD DS, которая позволяет выполнять изменения на уровне каталогов и управлять настройками пользователей и компьютеров, в том числе безопасностью и пользовательскими данными. Базовая конфигурация среды EC предусматривает повышенную безопасность и уровень функциональности операционной системы и приложений, достаточный для большинства предприятий.

# Среды с особыми параметрами безопасности и ограниченной функциональностью

Базовая конфигурация среды с особыми параметрами безопасности и ограниченной функциональностью (среды SSLF) предусматривает создание высокозащищенной среды для компьютеров с ОС Windows 7 и обозревателем Internet Explorer 8 – и только для таких. В таких средах вопросам безопасности уделяется настолько серьезное внимание, что можно пойти на значительное ограничение функциональности и управляемости.

Exclam **Внимание!**Параметры безопасности SSLF не подойдут для большинства предприятий. Они были разработаны для организаций, где безопасность важнее функциональности.

Если вы решите развернуть параметры SSLF на клиентские компьютеры своей рабочей среды, то может возрасти количество обращений в службу поддержки с жалобами на ограничения в функциональности, вводимые этими параметрами. Хотя степень защищенности данных и сетей в подобной среде будет выше, она также препятствует работе некоторых служб, которые могут быть необходимы предприятию. Примером может служить полное отключение элементов управления ActiveX®, что может серьезно ограничить доступ пользователей к специальным средствам некоторых веб-узлов.

Важно отметить, что базовая конфигурация SSLF не является наращиванием EC: SSLF обеспечивает совершенно иной уровень безопасности. Поэтому не пытайтесь одновременно развернуть базовые конфигурации SSLF и EC на одних и тех же компьютерах. С точки зрения настоящего руководства, *обязательно* сначала оценить уровень безопасности, необходимый предприятию, а только потом решать, какую базовую конфигурацию применять: EC *или* SSLF. Сравнение параметров в базовых конфигурациях EC и SSLF можно найти в файле Internet Explorer 8 Security Baseline Settings.xls, прилагаемом к настоящему руководству.

**Важно.** Если конфигурация SSLF кажется вам подходящей, обязательно проведите обширное тестирование компьютеров, на которых она развернута, чтобы убедиться, что требуемая для работы функциональность не пострадала.

# Администрирование Internet Explorer 8

В зависимости от размера и сложности структуры предприятия можно воспользоваться одним из двух основных способов централизованного администрирования параметров Internet Explorer 8: набор средств [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx) и объекты групповой политики (GPO) в инфраструктуре Active Directory. Существуют параметры, которые можно задать с помощью либо IEAK, либо GPO, но не того и другого одновременно. Однако в этом руководстве мы всюду, где возможно, будем сообщать информацию, применимую к обоим способам.

Для выбора оптимального способа задания параметров администратор должен знать о том и другом подходе. В общем случае IEAK лучше приспособлен к нуждам тех организаций, в которых администрирование среды выполняется без привлечения инфраструктуры Active Directory, или тех, которым требуется заказная версия обозревателя вместе со всеми параметрами и дополнениями. IEAK позволяет администратору без особого труда создать файл со специальными параметрами, который будет использован на этапе установки. Администратор, который применяет IEAK для создания заказных пакетов, может задать значения многих, но не всех параметров Internet Explorer 8. В продукте, установленном с помощью пакета, созданного в IEAK, параметры сохраняются лишь до тех пор, пока их не изменит пользователь. Если пакет создан в режиме внутреннего дистрибутива для корпоративной интрасети, то можно применять настройки IEAK с заданным интервалом, чтобы конфигурация клиентских компьютеров гарантированно соответствовала определенным на предприятии стандартам. Применение новой функции **Сброс параметров настройки** **Internet Explorer**  восстанавливает заказные настройки, определенные на предприятии, возвращает заданные по умолчанию параметры ActiveX Opt-In и деактивирует, но не удаляет все панели инструментов и расширения, установленные на компьютере.

Применение объектов групповой политики открывает возможность создавать конфигурации, которые регулярно копируются средствами политики на компьютеры пользователей, чтобы воспрепятствовать их изменению. С помощью объектов групповой политики можно управлять сотнями различных параметров Internet Explorer 8. Но работать с параметрами, задаваемыми в GPO, сложнее, чем использовать IEAK. После того как шаблон GPO определен и применен, заданная в нем конфигурация распространяется на все системы, подпадающие под его действие, пока не будет изменена администратором. Многие попытки пользователя внести изменения просто игнорируются или запрещаются. Значения некоторых параметров все же можно изменить, но они будут возвращены в исходное состояние при очередном применении политики.

Мы рекомендуем корпоративным клиентам по возможности применять GPO в инфраструктуре Active Directory, чтобы гарантировать неизменность заданных параметров безопасности.

# Основные сведения о зонной модели

Internet Explorer предлагает администраторам уникальное средство контроля безопасности, отсутствующее в большинстве других обозревателей: возможность определять параметры безопасности для различных классов веб-узлов. В отличие от многих других обозревателей, Internet Explorer определяет уровень безопасности данной веб-страницы, исходя из того, к какой зоне безопасности относится ее адрес URL.

Всего существует пять зон безопасности: **Локальный компьютер** (не видна в пользовательском интерфейсе Internet Explorer), **Интернет**, **Местная интрасеть**, **Надежные узлы** и **Ограниченные узлы**. Все веб-узлы на данном компьютере попадают в зону «Локальный компьютер», удаленные серверы относятся к зоне «Интернет», а веб-узлы в пределах локальной сети – к зоне «Местная интрасеть». Веб-узлы, которые пользователь или администратор счел потенциально опасными, помещаются в зону «Ограниченные узлы». Веб-узлы, которые пользователь или администратор счел надежными, помещаются в зону «Надежные узлы».

**Примечание.** Для компьютеров, которые не входят в домен, зона «Местная интрасеть» отключена, и те узлы, которые при обычных условиях попали бы в эту зону, оказываются в зоне «Интернет». Зона «Локальный компьютер» отсутствует в пользовательском интерфейсе Internet Explorer.

Для каждой зоны определяются соответствующие ей параметры безопасности. Чтобы упростить решение этой задачи, в Internet Explorer используются шаблоны зон безопасности. По умолчанию имеется пять шаблонов: высокий, выше среднего, средний, ниже среднего и низкий. Между зонами безопасности и шаблонами устанавливается следующее соответствие, помогающее определить уровень безопасности.

Таблица 1.1. Соответствие между зонами безопасности и шаблонами

| **Зона безопасности** | **Уровень безопасности (шаблон, соответст­вующий зоне)** | **Описание** |
| --- | --- | --- |
| Локальный компьютер | Другой | Содержимое, находящееся на компьютере пользователя (за исключением того, что Internet Explorer кэшировал на локальной системе), считается заслуживающим полного доверия. Эту зону невозможно конфигурировать в Internet Explorer. |
| Интернет | Выше среднего | В зону «Интернет» входят все веб-узлы, не включенные в другие зоны. |
| Местная интрасеть (доступна только для компьютеров, входящих в домен) | Ниже среднего | Все узлы, помещенные в эту зону, должны находиться за брандмауэром, а прокси-серверы должны быть сконфигурированы так, чтобы ни одно внешнее DNS-имя не попадало в эту зону. |
| Надежные узлы | Средний | Узлам в зоне «Надежные узлы» разрешено выполнять более широкий спектр операций, чем другим Интернет-узлам, и у пользователя реже запрашивается разрешение. Внешние узлы следует помещать в эту зону, только если вы доверяете их содержимому и уверены, что они не станут выполнять операций, способных нанести вред находящимся в вашем ведении компьютерам. |
| Ограниченные узлы | Высокий | Эта зона предназначена для узлов, не заслуживающих никакого доверия. По умолчанию настройки для нее заданы так, что некоторые возможности веб ограничены, но доступ к узлам не заблокирован полностью. Узлы в эту зону могут добавляться как пользователем, так и групповой политикой. |

Помимо этих зон, существуют соответствующие им заблокированные зоны, которые не видны в пользовательском интерфейсе Internet Explorer. Настройки заблокированных зон для зоны локального компьютера используются впервые появившейся в Windows XP SP2 функцией, которая называется «Блокировка зоны локального компьютера» (Local Machine Zone Lockdown – LMZL). Если зона локального компьютера заблокирована, то по умолчанию при открытии любого находящегося в ней узла применяются более ограничительные параметры. По умолчанию параметры в режиме LMZL отключают элементы ActiveX и выполнение сценариев. Если страница попытается выполнить элемент ActiveX или сценарий, то появится информационная панель с вопросом пользователю, следует ли разрешить эту операцию. Если пользователь разрешит доступ к заблокированному содержимому, то Internet Explorer будет применять обычные, менее ограничительные параметры зоны локального компьютера, начиная с этого момента и вплоть до закрытия соответствующей вкладки обозревателя, если речь идет об Internet Explorer 7 или Internet Explorer 8, либо до закрытия окна обозревателя в случае Internet Explorer 6. Прочие заблокированные зоны используются в протоколах, заданных параметром **Блокирование сетевых протоколов** в групповой политике.

Значения параметров хранятся в одном из нескольких разделах реестра в зависимости от того, каким образом параметр был задан и применяется ли он к конкретному пользователю или к компьютеру (см. таблицу ниже).

Таблица 1.2. Разделы реестра, в которых хранятся параметры зон

| **Пара­метр для пользо­вателя** | **Параметр для компью­тера** | **Задан с помощью групповой политики** | **Задан в окне «Свойства обозрева­теля»** | **Раздел реестра** |
| --- | --- | --- | --- | --- |
| ✓ |  |  | ✓ | HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones |
| ✓ |  | ✓ |  | HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Zones\ |
| ✓ |  | ✓ |  | HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Lockdown\_Zones\ |
|  | ✓ |  | ✓ | HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\ |
|  | ✓ | ✓ |  | HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\ |
|  | ✓ | ✓ |  | HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\LockdownZones\ |

В каждом из этих разделов есть подразделы, соответствующие отдельным зонам безопасности.

Эти подразделы кодируются следующим образом:

0 = зона «Локальный компьютер»

1 = зона «Местная интрасеть»

2 = зона «Надежные узлы»

3 = зона «Интернет»

4 = зона «Ограниченные узлы»

Шаблоны зон безопасности определяют, какие действия разрешено выполнять веб-странице. Например, шаблон «Высокий» (уровень безопасности) запрещает веб-странице запускать элементы ActiveX и сценарии. По умолчанию, пользователь, посетивший страницу, находящуюся в зоне «Ограниченные узлы», не сможет воспользоваться этой функциональностью. Дополнительные сведения о зонах безопасности и шаблонах см. в статье MSDN® «[О зонах безопасности URL](http://go.microsoft.com/fwlink/?LinkId=26003)» (на английском языке).

## Изменение параметров зон

Пользователь может тремя способами изменить параметры зон в диалоговом окне **Свойства обозревателя**:

Переместить ползунок на вкладке **Безопасность**, изменив тем самым шаблон, применяемый к данной зоне. Например, можно изменить уровень безопасности для зоны «Интернет» с «Выше среднего» на «Средний».

Задать свои параметры для некоторой зоны, нажав кнопку **Другой** на вкладке **Безопасность**.

Включить в зону дополнительные узлы, нажав кнопку **Узлы** на вкладке **Безопасность**. (Эта кнопка недоступна для зоны «Интернет», потому что та, по определению, содержит узлы, не входящие ни в какие другие зоны.)

Примечание. Для зоны **Местная интрасеть** поведение кнопки **Узлы** отличается. В этом случае кнопка **Узлы** позволяет определить, обнаруживается ли местная интрасеть автоматически (режим по умолчанию) или следует применять заданный пользователем критерий. Вы можете включить в эту зону все узлы интрасети, не перечисленные в других зонах; все узлы, подключаемые минуя прокси-сервер, или все сетевые пути (UNC). Но при этом сохраняется возможность включить в зону **Местная интрасеть** конкретные узлы, для чего достаточно нажать кнопку **Дополнительно** в окне параметров. Если вы захотите идентифицировать узлы интрасети полными доменными именами (FQDN), то должны будете ввести их в зону **Местная интрасеть** вручную. Это связано с тем, что Internet Explorer автоматически помещает адреса URL, содержащие точки, например web.mydomain.com, в зону **Интернет**.

Зачастую администраторы хотят ограничить возможности пользователей по изменению параметров зон. Дополнительные сведения о том, как этого достичь, см. в главе 2 «Рекомендации по обеспечению безопасности Internet Explorer 8».

## Определение зоны

Если сама идея зон безопасности и разрешений для них не вызывает вопросов, то логика определения зоны обычно не объясняется, а понимать ее полезно, чтобы эффективно управлять компьютерами. Процедура определения зоны основана на анализе содержимого адресной строки в Internet Explorer, а не на анализе IP-адреса, полученного от DNS-сервера, или значения маски сети. В общем случае в правилах определения зоны рассматривается адрес URL, введенный пользователем. Для определения той зоны, в которой следует открывать узел, применяются следующие правила:

Все узлы, перечисленные в зоне **Ограниченные узлы**, в этой зоне и открываются.

Все узлы, перечисленные в зоне **Надежные узлы**, в этой зоне и открываются.

Все узлы, перечисленные в зоне **Местная интрасеть**, в этой зоне и открываются.

Узлы, перечисленные в списке тех, что подключаются, минуя прокси-сервер, открываются в зоне **Местная интрасеть**.

Если URL, введенный в адресной строке, не содержит точек, и ему соответствует какой-то узел, то этот узел открывается в зоне **Местная интрасеть** (например, http://local).

Все остальные узлы открываются в зоне **Интернет**.

Примечание. Невозможно включить узел сразу в несколько зон.

Важно отметить, что в соответствии с этими правилами узлы интрасети иногда открываются в зоне **Интернет**. Например, если узел интрасети определен с помощью IP-адреса или полного доменного имени, то он будет открываться в зоне **Интернет**, так как имя содержит точки.

## За пределами зонной модели: общие параметры безопасности

В Internet Explorer 8 имеются также относящиеся к безопасности параметры, никак не связанные с зонами. Эти параметры находятся на вкладках **Конфиденциальность**, **Содержание** и **Дополнительно** диалогового окна **Свойства обозревателя**, которое открывается из меню **Сервис**; более подробно мы обсудим его ниже.

# Проектирование подразделений для применения политик безопасности Internet Explorer 8

Описываемый в этой главе подход к обеспечению основан на понятии подразделения (organizational unit – OU). *Подразделением* называется контейнер в домене, построенном с помощью технологии Active Directory. Подразделение может содержать пользователей, группы, компьютеры и другие подразделения. Если одно подразделение содержит другие, то оно называется родительским. Подразделение, находящееся внутри родительского подразделения, называется дочерним.

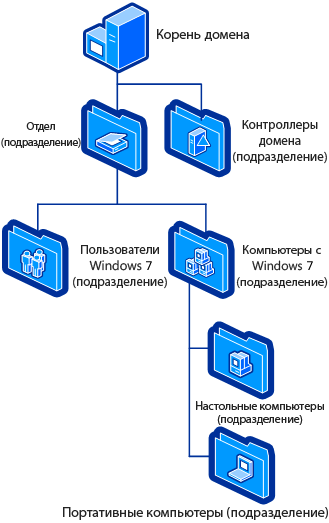
С подразделением можно связать объект групповой политики (GPO) и впоследствии применить параметры, хранящиеся в этом GPO, ко всем пользователям и компьютерам, принадлежащим данному подразделению и его потомкам. А для упрощения администрирования можно делегировать кому-то административные полномочия в каждом подразделении в отдельности. Подразделения – это простой способ сгруппировать пользователей и компьютеры и очертить административные границы.

Внимание! Мы рекомендуем относить пользователей и компьютеры к разным подразделениям, потому что некоторые настройки применяются только к пользователям, а другие – только к компьютерам.

Чтобы делегировать управление отдельным подразделением или их группой, следует воспользоваться мастером делегирования, который входит в состав оснастки «Active Directory – пользователи и компьютеры» для консоли управления (MMC). Ссылки на документацию по делегированию полномочий см. в разделе «Дополнительная информация» в конце этой главы.

Одна из основных целей при проектировании подразделений для любой среды состоит в том, чтобы заложить основы реализации групповой политики, которая будет применяться ко всем клиентским компьютерам, внесенным в каталог Active Directory. Это гарантирует, что все клиентские компьютеры будут отвечать стандартам безопасности, принятым на предприятии. Структура подразделений должна также допускать задание специальных параметров для некоторых типов пользователей. Например, разработчикам необходимы такие виды доступа к своим компьютерам, которые ни к чему среднему пользователю. Или, у пользователей портативных компьютеров требования к безопасности иные, нежели у пользователей настольных ПК.

На рисунке ниже изображена простая структура подразделений, которой достаточно для обсуждения групповой политики в этой главе. Эта структура, в которой используется базовая конфигурация корпоративного клиента (EC), может не соответствовать требованиям, предъявляемым на вашем предприятии.



{0>Figure 1.1 Example OU structure for computers running Internet Explorer 8 for Windows 7<}100{>Рисунок 1.1. Пример структуры подразделений в случае компьютеров, на которых установлен обозреватель Internet Explorer 8 для Windows 7

## Подразделение отдела

Часто в разных структурных подразделениях предприятия требования к безопасности различаются. Поэтому имеет смысл создать одно или несколько подразделений отделов. Такие подразделения можно использовать для применения параметров безопасности к компьютерам и пользователям в соответствующих отделах с помощью объекта групповой политики

## Подразделение пользователей Windows 7

К этому подразделению относятся учетные записи пользователей в среде корпоративного клиента. Параметры, применяемые к этому подразделению, подробно описаны в файле Internet Explorer 8 Security Baseline Settings.xls, прилагаемом к настоящему руководству.

## Подразделение компьютеров с Windows 7

Это подразделение содержит по одному дочернему подразделению для каждого типа клиентских компьютеров с установленным обозревателем Internet Explorer 8 for Windows 7 в среде EC. В *Руководстве по безопасности Windows 7* проводится четкое различие междунастольными и портативными ПК с точки зрения обеспечения их безопасности. Поэтому авторы настоящего руководства создали такие подразделения для компьютеров:

**Настольные компьютеры**. К этому подразделению относятся настольные компьютеры с постоянным подключением к сети. Параметры, применяемые к этому подразделению, подробно описаны в файле Internet Explorer 8 Security Baseline Settings.xls.

**Портативные компьютеры**. Это подразделение включает переносные компьютеры мобильных пользователей, которые не всегда подключены к сети. В файле Internet Explorer 8 Security Baseline Settings.xls Excel описаны также параметры, применяемые к этому подразделению.

## Схема объектов групповой политики для политик безопасности

*Объектом групповой политики (GPO)* называется совокупность параметров групповой политики, которые по сути являются файлами, создаваемыми в оснастке «Групповая политика». Эти параметры хранятся на уровне домена и влияют на пользователей и компьютеры в сайтах, домена и подразделениях.

Объекты групповой политики позволяют обеспечить применение конкретных параметров политики, прав пользователей и поведения компьютеров ко всем клиентским компьютерам или пользователям в подразделении Использование групповой политики вместо настройки вручную упрощает управление изменениями (включая обновление) для большого количества компьютеров и пользователей. Настройка вручную не только неэффективна, так как требует посещения каждого клиентского компьютера, но и потенциально бесполезна: если параметры политики в объектах групповой политики домена отличаются от параметров, применяемых локально, параметры политики объекта групповой политики домена переопределяет примененные локально параметры.



Рисунок 1.2. Очередность применения объектов групповой политики

На предыдущем рисунке показана очередность, в которой объекты групповой политики (GPO) применяются к компьютеру, являющемуся членом дочернего подразделения, от наиболее низкого уровня (1) к самому высокому (5). Сначала применяется групповая политика из локальной политики безопасности каждого клиентского компьютера с установленным Internet Explorer 8 для Windows 7. Затем применяются GPO на уровне сайта, а затем на уровне домена.

Если клиентский компьютер с Internet Explorer® 8 для Windows 7 принадлежит подразделению с несколькими уровнями, то объекты групповой политики применяются в порядке от родительского подразделения до дочернего подразделения самого низкого уровня. Последним применяется объект групповой политики из подразделения, содержащего клиентский компьютер. Описанный порядок обработки объектов групповой политики — локальная политика безопасности, сайт, домен, родительское подразделение и дочернее подразделение — очень важен, так как объекты групповой политики, которые применяются позже, переопределяют примененные ранее объекты. GPO пользователей применяются таким же образом.

При разработке групповой политики необходимо учитывать следующее:

Администратор должен задать порядок, в котором несколько объектов групповой политики привязываются к подразделению, иначе групповая политика будет по умолчанию применяться в том порядке, в котором объекты привязывались. Если один и тот же параметр настроен в нескольких политиках, приоритет будет иметь политика, идущая в списке первой.

Для объекта групповой политики можно включить параметр **Принудительный**. Если выбран этот параметр, другие объекты групповой политики не смогут переопределять параметры, настроенные в этом объекте групповой политики.

Для Active Directory, сайта, домена или подразделения можно установить параметр **Блокировать наследование политики**. Этот параметр блокирует параметры объектов групповой политики, которые расположены выше в иерархии Active Directory, если для них не задан параметр **Принудительный**. Другими словами, параметр **Принудительный** имеет приоритет над параметром **Блокировать наследование политики**.

Параметры групповой политики применяются к пользователям и компьютерам и зависят от места пользователя или компьютера в Active Directory. В некоторых случаях необходимо применять политику к объектам пользователей на основе расположения объектов компьютеров, а не пользователей. Функция замыкания на себя групповой политики позволяет администраторам применять параметры групповой политики для пользователя в зависимости от того, в систему какого компьютера он вошел. Дополнительную информацию об этом параметре см. в статье «[Режим замыкания при обработке групповой политики](http://support.microsoft.com/Default.aspx?id=231287)».

#### Рекомендуемые объекты групповой политики

Для внедрения описанной выше схемы подразделений требуется как минимум два объекта групповой политики:

политика для подразделения пользователей Windows 7;

политика для подразделения компьютеров с Windows 7.

На рисунке ниже показана предварительная структура, в которой отражены связи между этими объектами групповой политики и схемой подразделений.

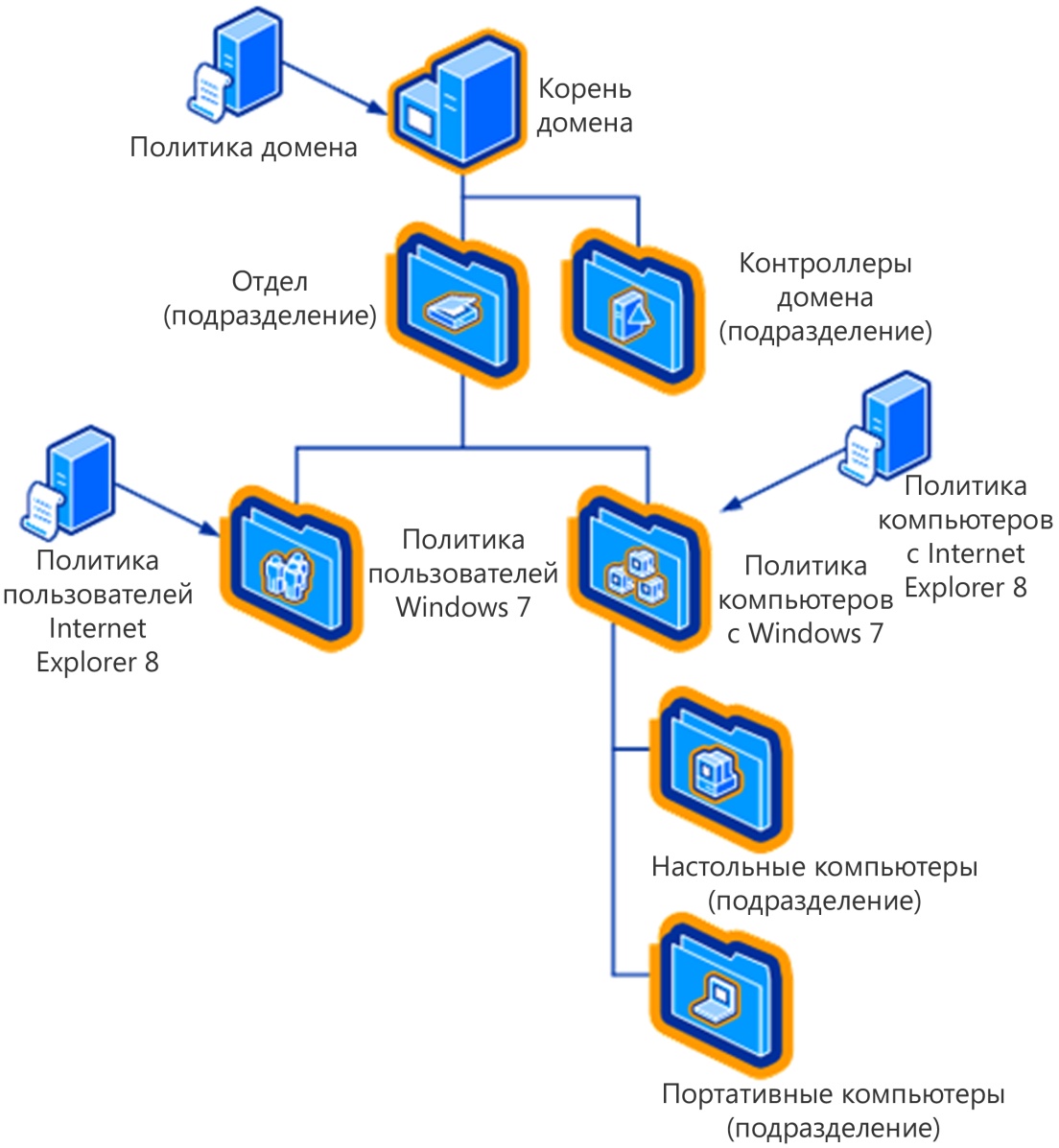


Рисунок 1.3. Пример структуры подразделений и связей объектов групповой политики для компьютеров с установленным обозревателем Internet Explorer 8 для Windows 7

К настоящему руководству прилагается следующий упакованный файл с расширением .zip:

* Internet Explorer 8 GPOs.zip

В этом архиве находятся сохраненные файлы объектов групповой политики, которые можно загрузить в консоль управления групповой политикой (GPMC), и тем самым быстро создать объекты групповой политики со всеми рекомендуемыми параметрами. Чтобы установить консоль управления групповой политикой, загрузите ее со страницы [Средства удаленного администрирования сервера для Windows 7](http://go.microsoft.com/fwlink/?LinkId=130862) (на английском языке) в Центре загрузки Microsoft.

Чтобы создать объекты групповой политики, включающие все рекомендуемые параметры, выполните следующие действия:

Находясь в том каталоге Active Directory, в котором собираетесь создавать объект групповой политики, войдите от имени администратора домена на входящий в этот домен компьютер с установленным Internet Explorer 8 для Windows 7.

Распакуйте содержимое файла InternetExplorer8GPOs.zip в папку на своем компьютере.

С помощью консоли GPMC создайте следующие объекты групповой политики:

политика IE8 EC Computer;

политика IE8 EC User.

ИЛИ

политика IE8 SSLF Computer;

политика IE8 SSLF User.

Воспользуйтесь консолью GPMC для импорта настроек из сохраненных файлов объектов группой политики в объекты группой политики, созданные на шаге 2.

Дополнительную информацию о работе с консолью управления групповой политикой см. на странице [Архивация, восстановление, копирование и импорт](http://technet.microsoft.com/en-us/library/cc759276(WS.10).aspx) узла Windows Server TechCenter.

# Средства обеспечения безопасности и конфиденциальности в Internet Explorer 8

Безопасность работы пользователя, выбор подходящего режима и контроль – это ключевые темы в обозревателе Internet Explorer 8, который содержит много новшеств, призванных придать большую уверенность при посещении веб-страниц. В этом разделе мы рассмотрим некоторые средства и технологии обеспечения безопасности и конфиденциальности, появившиеся в Explorer 8, в том числе:

фильтр SmartScreen;

защита от фишинга и вредоносных программ;

защита от ClickJacking;

фильтр запуска сценариев между узлами (XSS);

выделение домена;

защищенный режим Internet Explorer;

явное согласие на запуск элементов ActiveX;

просмотр в режиме InPrivate;

фильтрация InPrivate.

## Фильтр SmartScreen

В состав обозревателя Internet Explorer 8 включен фильтр SmartScreen – набор технологий, предназначенных для защиты пользователей от новых встречающихся в веб угроз, в том числе реализуемых методами социальной инженерии. Фильтр SmartScreen базируется на функциональности фильтра фишинга в Internet Explorer 7 и расширяет ее.

Фильтр SmartScreen защищает пользователя, просматривающего веб-страницы, от уже известных подставных и вредоносных узлов. Кроме того, фильтр SmartScreen включает средства защиты от техники *ClickJacking*, которую хакеры применяют для перехвата нажатий клавиш, кражи учетных данных пользователя, искажения веб-страниц и других типов атак. Также фильтр SmartScreen содержит новый фильтр запуска сценариев между узлами, предотвращающий атаки типа 1.

### Защита от фишинга и вредоносных программ

*Фишингом* называется техника, которую многие атакующие применяют для того, чтобы обманом заставить пользователя сообщить финансовую или личную информацию в сообщении электронной почты или на веб-узле. *Фишер* маскируется под легитимное физическое или юридическое лицо и выманивает такую информацию, как пароли к учетным записям или номера кредитных карточек. Фильтр SmartScreen в Internet Explorer 8 предупреждает пользователя о подозрительных или уже известных подставных узлах, делая тем самым путешествие по Интернету более безопасным. Фильтр анализирует содержимое веб-узла, пытаясь найти признаки известных технологий фишинга, а также использует глобальную сеть источников данных для определения надежности веб-узла. Кроме того, фильтр SmartScreen Filter обеспечивает динамическую защиту от вредоносного ПО, удерживая пользователей от посещения узлов, замеченных в распространении такого ПО, и от загрузки файлов с вредоносным содержимым.

В состав фильтра SmartScreen входит целый ряд различных технологий и часто обновляемая онлайновая служба, что позволяет ему получать самую актуальную информацию о жульнических веб-узлах и использовать ее для того, чтобы своевременно предупреждать и защищать пользователей, работающих с обозревателем Internet Explorer 8.

Фильтр SmartScreen сочетает анализ веб-страниц на стороне клиента на предмет обнаружения подозрительных характеристик с онлайновой службой, доступ к которой пользователь может разрешить или запретить. Фильтр реализует защиту от подставных и вредоносных узлов тремя способами:

Сравнение адресов известных надежных веб-узлов, на которые пользователь пытается зайти, со списком известных узлов с высоким трафиком, который хранится на компьютере пользователя. Если узел найден в этом списке, больше никаких проверок не производится.

Анализ узла, на который пользователь собирается зайти, на предмет наличия признаков, характерных для подставных узлов.

Отправка адреса узла, на который пользователь собирается зайти, онлайновой службе, поддерживаемой корпорацией Майкрософт, которая тут же ищет узел в часто обновляемом списке узлов, замеченных в фишинге и распространении вредоносного ПО. В этот список входят узлы, вредоносность которых подтверждена авторитетными источниками, сообщившими о них Майкрософт.

Примечание. Доступ к онлайновой службе производится асинхронно по SSL-соединению, так что это не сказывается на загрузке страниц и не мешает работе пользователя. Если обратиться к службе не удалось, то страница отображается как обычно, а в строке состояния появляется всплывающее сообщение о недоступности службы.

Примечание. С помощью Internet Explorer можно проанализировать любой узел и узнать, является ли он подставным; для этого достаточно выбрать из меню **Сервис** пункт **Фильтр** **SmartScreen**, а затем команду **Проверить веб-узел**.

Уважая конфиденциальность пользователя, фильтр SmartScreen спрашивает, хочет ли пользователь включить или отключить эту функцию, – по умолчанию не установлен ни тот, ни другой режим. Пользователя можно лишить возможности выбора, подавив вопрос при первом обращении или собрав с помощью IEAK заказной пакет для предприятия. Чтобы фильтр SmartScreen выполнял свою защитную функцию, мы рекомендуем организациям при конфигурировании системы включать SmartScreen и запрещать пользователям его отключение. Кроме того, мы рекомендуем удалять ссылку **Щелкните чтобы продолжить**, присутствующую в предупреждениях SmartScreen, которые появляются, когда фильтр обнаруживает подставной или вредоносный узел. Дополнительную информацию о том, как запретить пользователям отключать фильтр SmartScreen Filter и не дать им проигнорировать предупреждения, см. в главе 3 «Рекомендации по настройке конфиденциальности».

### Защита от ClickJacking

Фильтр SmartScreen теперь включает новую функцию, призванную обнаруживать и предотвращать ClickJacking. Она является частью основного кода Internet Explorer 8, поэтому всегда включена и не может быть выключена.

*Перехват щелчка*, или *ClickJacking*, происходит, когда атакующему удается обманом заставить ничего не подозревающего пользователя щелкнуть по содержимому, полученному из другого домена. Против техники ClickJacking большинство мер противодействия подделке HTTP-запросов (CSRF – cross-site request forgery) бессильны, и атакующий может использовать ее для изменения конфигурации надстроек над обозревателем небезопасным образом.

Атакующий демонстрирует набор фиктивных кнопок, а затем загружает поверх них другую страницу в прозрачном слое. Пользователь думает, что нажимает видимые кнопки, тогда как на самом деле выполняет какие-то действия на скрытой странице. Возможно, скрытая страница уже прошла процедуру аутентификации, поэтому атакующий может обманом заставить пользователя сделать нечто, что тот делать не намеревался. И проследить такую последовательность событий впоследствии невозможно, так как пользователь честно аутентифицировал себя на другой странице.

Чтобы узел мог воспользоваться дополнительной защитой от атак типа ClickJacking, необходимо включить заголовок X-FRAME-OPTIONS в состав HTTP-заголовков или в тег META HTTP-EQUIV. Дополнительные сведения об атаках типа ClickJacking, см. в блоге [Безопасность IE8, часть VII: защита от ClickJacking](http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx) (на английском языке).

### Фильтр запуска сценариев между узлами (XSS)

Новая функция «Фильтр запуска сценариев между узлами (XSS)», входящая в состав фильтра SmartScreen, защищает пользователя от некоторых видов атак на серверные приложения. Они носят названия «атаки типа 1», или «атаки отражением», и являются наиболее распространенным видом атак посредством запуска сценариев между узлами. Это происходит, когда некоторый код, обычно в форме сценария, передается веб-серверу, а затем возвращается пользователю. Например, если информация, отправленная веб-обозревателем, без какой-либо проверки используется серверным сценарием, для генерации страницы, посылаемой пользователю. Если входная информация не проверяется, то отправленные пользователем данные могут быть включены в результирующую страницу без HTML-кодирования, так что код, введенный на стороне клиента, «отражается» на странице, посылаемой другому пользователю.

Фильтр XSS защищает пользователя от таких атак, анализируя возвращенные ему данные. Путем анализа потока данных Internet Explorer 8 может распознать некоторые действия, которые при обычных обстоятельствах не должны встречаться, и запретить выполнение вредоносного сценария. Дополнительные сведения о параметрах фильтра XSS см. в главе 2 «Рекомендации по обеспечению безопасности Internet Explorer 8».

Примечание. По умолчанию защита от Clickjacking и XSS включена. Защита от ClickJacking является частью стратегии глубоко эшелонированной обороны обозревателя и не может быть отключена. Однако пользователь может отключить фильтр XSS. Также пользователь может включить фильтр SmartScreen для защиты от фишинга и вредоносного ПО (как описано выше).

## Выделение домена

Быть может, наиболее заметным изменением во внешнем виде адресной строки в Internet Explorer 8 является функция *выделения домена*. Internet Explorer 8 автоматически выделяет часть, которую можно считать основным доменом просматриваемого узла. Это помогает пользователю идентифицировать истинный источник узла в случае, когда узел пытается ввести его в заблуждение. Эта новая функция является частью технологии улучшенной адресной строки в Internet Explorer 8, которая дает более отчетливые визуальные признаки происхождения веб-узлов и используемого ими метода шифрования. Выделение домена включено всегда (его нельзя отключить) и видно одновременно со всеми остальными предупреждениями и оповещениями в адресной строке, в том числе о наличии сертификата с расширенной проверкой и о подставном узле. Дополнительную информацию о SSL-сертификатах с расширенной проверкой см. на странице [Internet Explorer и значимость для бизнеса SSL-сертификатов с расширенной проверкой](http://www.microsoft.com/ie/ev) (на английском языке) веб-узла, посвященного Internet Explorer.

## Защищенный режим Internet Explorer

Защищенный режим Internet Explorer доступен на компьютерах с установленным обозревателем Internet Explorer 7 или Internet Explorer 8 для следующих операционных систем: Windows Server 7 и Windows Vista Функция *защищенный режим* реализует дополнительные меры защиты, разрешая приложению доступ только к определенным участкам файловой системы и реестра. Кроме того, защищенный режим не дает вредоносной программе перехватить управление обозревателем и выполнить код с повышенными привилегиями.

Защищенный режим уменьшает риск от наличия известных уязвимостей в расширениях обозревателя, не позволяя использовать их для скрытой установки вредоносного кода. В этой функции используются механизмы с более высоким уровнем целостности, чем в Windows 7 и Windows Vista, которые для достижения поставленной цели ограничивают доступ к процессам, файлам и разделам реестра. Интерфейс прикладного программирования (API) защищенного режима позволяет поставщикам ПО разрабатывать расширения и надстройки над Internet Explorer, способные взаимодействовать с файловой системой и реестром даже тогда, когда обозреватель работает в защищенном режиме.

В защищенном режиме обозреватель Internet Explorer 8 работает с урезанным набором прав, что позволяет предотвратить изменение пользовательских и системных файлов и параметров без получения явного согласия пользователя. Кроме того, защищенный режим стал более дружественным к пользователю, чем было в версии Internet Explorer 7, если использовать его в сочетании с новой архитектурой *Loosely Coupled Internet Explorer (LCIE)*. В двух словах, LCIE разрывает связь между окнами и процессами Internet Explorer, благодаря чему вкладки, работающие в защищенном режиме, могут находиться в одном окне с вкладками, работающими в обычном режиме. Это усовершенствование устраняет необходимость в «процессе-брокере», который имелся в Internet Explorer 7, и передает все функции, требующие расширения, на уровень оконного процесса.

По умолчанию защищенный режим включен для всех пользователей, кроме того, который входит от имени встроенной учетной записи Администратор. Другие учетные записи с правами администратора по умолчанию работают в защищенном режиме. Чтобы отключить защищенный режим, можно либо запустить обозреватель со специальным флагом, либо внести изменения в реестр или объект групповой политики. Чтобы запустить Internet Explorer 8 без защищенного режима на компьютере под управлением Windows 7 или Windows Vista, необходимо щелкнуть правой кнопкой мыши по значку Internet Explorer, выбрать из контекстного меню команду **Запуск от имени администратора**, ввести соответствующие учетные данные и нажать клавишу ENTER.

По умолчанию защищенный режим Internet Explorer 8 включен для зон безопасности **Интернет** и **Ограниченные узлы**. Однако пользователь может его отключить, что негативно скажется на общей безопасности.

## Явное согласие на запуск элементов ActiveX

В Internet Explorer 7 появился механизм явного согласия на запуск элементов ActiveX (ActiveX Opt-in), автоматически отключающий все элементы управления, которые пользователь не разрешил явно, уменьшая тем самым риск злонамеренного использования предустановленных элементов. В Internet Explorer 8 этот механизм защиты получил дальнейшее развитие – стало возможно более точно настраивать параметры ActiveX Opt-in на уровне пользователя и домена. Эти добавочные средства контроля позволяют с большей уверенностью защищать пользователей и их системы от злонамеренных атак.

Перед тем как обратиться к установленному элементу ActiveX, который ранее не использовался при работе в Интернете, Internet Explorer сообщает об этом пользователю на панели информации. Этот механизм уведомления позволяет пользователю разрешить или запретить доступ к каждому отдельному элементу и для каждого узла, что еще больше сужает возможности для атаки. Злонамеренные пользователи не смогут воспользоваться веб-узлами для проведения автоматизированных атак с помощью элементов ActiveX, которые никогда не предназначались для работы в Интернете. Управление параметрами на уровне пользователя усиливает защиту, так как разрешенным элементом сможет воспользоваться только тот, кто его разрешил, что минимизирует воздействие на других пользователей. Управление параметрами на уровне домена гарантирует, что разрешенным элементом можно будет воспользоваться только на тех веб-узлах, к которым пользователь планировал обращаться, а прочие узлы по-прежнему нуждаются в явном разрешении на использование того же самого элемента.

## Просмотр в режиме InPrivate

Режим просмотра InPrivate позволяет запретить обозревателю Internet Explorer 8 сохранение истории обзора, файлов cookie и других данных. Иногда при использовании общего ПК, ноутбука, одолженного у приятеля, или ПК, установленного в общественном месте, вы не хотите, чтобы другие люди знали, какие веб-узлы вы посещаете. Режим просмотра InPrivate в Internet Explorer 8 упрощает конфиденциальное использование обозревателя за счет того, что не сохраняется история, файлы cookie, временные файлы Интернета и другие данные.

Режим InPrivate имеет следующие отличия:

отключаются модули поддержки обозревателя (BHO) и панели инструментов;

не сохраняются новые файлы cookie;

если веб-узел пытается создать сохраняемый файл cookie, то обозреватель преобразует его в сеансовый и удаляет по завершении сеанса;

ранее сохраненные файлы cookie не считываются и не отправляются серверу;

новая функция хранилища DOM ведет себя аналогично;

в историю обзора не добавляются новые записи;

вновь созданные временные файлы Интернета удаляются после закрытия окна просмотра InPrivate;

не сохраняются данные форм;

не сохраняются пароли;

не сохраняются адреса, введенные в адресной строке;

не сохраняются запросы, введенные в поле поиска.

Кроме того, панели инструментов и модули поддержки обозревателя по умолчанию отключены. Пользователь может включить эти функции на вкладке **Конфиденциальность** в диалоговом окне **Свойства обозревателя**, которое доступно с помощью меню **Сервис**.

## Фильтрация InPrivate

Функция фильтрации InPrivate дает пользователю дополнительные средства контроля над сторонними узлами, которым он согласен передавать данные о своем поведении в Интернете. Веб-узлы все чаще обращаются к содержимому из разных источников, что приносит огромную пользу как потребителям, так и самим веб-узлам. Однако пользователи часто не осознают, что фрагменты содержимого, некоторые изображения, рекламные объявления и аналитические данные предоставляются сторонними узлами, и что эти узлы имеют возможность отслеживать (посредством агрегирования и корреляции данных) поведение отдельного пользователя на различных веб-узлах. Фильтрации InPrivate дает пользователю дополнительные средства контроля над тем, какую именно информацию сторонние веб-узлы смогут использовать для отслеживания поведения в сети.

Примечание. Детальный обзор этой функции и пользовательских настроек можно найти в документе [*Руководство по средствам конфиденциальности и контроля со стороны пользователя в Internet Explorer 8*](http://download.microsoft.com/download/D/5/6/D562FBD1-B072-47F9-8522-AF2B8F786015/IE8%20Privacy%20and%20User%20Control-RC1%20Final.pdf) (на английском языке).

# Дополнительные сведения

Подробнее о вопросах безопасности Internet Explorer 8 можно узнать из следующих источников на Microsoft.com:

[О зонах безопасности](http://go.microsoft.com/fwlink/?LinkId=26003) (на английском языке).

Страница [Архивация, восстановление, копирование и импорт](http://technet.microsoft.com/en-us/library/cc759276(WS.10).aspx) узла Windows Server TechCenter.

Блог [Безопасность IE8, часть VII: защита от ClickJacking](http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx) (на английском языке).

[*Руководство по средствам конфиденциальности и контроля со стороны пользователя Internet Explorer 8*](http://download.microsoft.com/download/D/5/6/D562FBD1-B072-47F9-8522-AF2B8F786015/IE8%20Privacy%20and%20User%20Control-RC1%20Final.pdf) (на английском языке).

[*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx).

Страница [Internet Explorer и значимость для бизнеса SSL-сертификатов с расширенной проверкой](http://www.microsoft.com/ie/ev) (на английском языке) веб-узла, посвященного Internet Explorer.

[Internet Explorer TechCenter](http://technet.microsoft.com/ie).

Статья «[Режим замыкания при обработке групповой политики](http://support.microsoft.com/Default.aspx?id=231287)».

Технические извещения о безопасности корпорации Майкрософт:

[Средства удаленного администрирования сервера для Windows 7](http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d)

## Отзывы

Вопросы и замечания по данному руководству просьба направлять по адресу [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).

Глава 2. Рекомендации по обеспечению безопасности Internet Explorer 8

Для повышения безопасности параметров, установленных по умолчанию в обозревателе Windows® Internet Explorer® 8, недостаточно просто поменять какие-то значения на вкладке **Безопасность** в диалоговом окне **Свойства обозревателя** или передвинуть ползунок уровня безопасности для каждой зоны в положение **Высокий**. Такие кардинальные изменения параметров просто не дадут пользователям нормально просматривать веб-узлы и потому сделают обозреватель бесполезным. В этом разделе обсуждаются различные изменения, которые администратор может внести в параметры Internet Explorer 8 на подведомственных компьютерах, чтобы повысить безопасность, не слишком затрагивая функциональность обозревателя.

Параметры Internet Explorer 8 и приводимые в этой главе рекомендации можно разбить на шесть категорий:

управление надстройками;

отключение активных сценариев;

обеспечение безопасности с помощью зон;

обеспечение безопасности с помощью сертификатов;

понижение уровня привилегий приложения;

прочие параметры безопасности;

В приложении A к настоящему руководству приведен контрольный список всех параметров, которые мы рекомендуем реализовать. В этой главе подробно рассматриваются все эти параметры и соответствующие рекомендации.

Примечание. Помимо задания параметров, обсуждаемых в этой главе, можно также воспользоваться групповой политикой, чтобы исключить некоторые вкладки из диалогового окна **Свойства обозревателя**, например **Подключения** и **Дополнительно**. Однако, даже убрав эти вкладки, все равно следует принудительно установить отдельные параметры, чтобы пользователь не мог изменить их путем редактирования локального реестра.

# Управление надстройками

Корпорация Майкрософт реализовала платформу ActiveX®, чтобы дать веб-разработчикам возможность расширять стандартную функциональность обозревателя. С помощью платформы ActiveX разработчикам удалось создать обогащенные интерактивные приложения, способные интегрировать данные практически из любого источника. Хотя при проектировании платформы ActiveX учитывались вопросы безопасности и были включены такие средства, как Authenticode®, позволяющие защищать код, очень важно, чтобы при использовании этого механизма пользователи следовали рекомендациям по обеспечению безопасности обозревателя. Internet Explorer 8 позволяет контролировать расширения с помощью функции управления надстройками. В этом разделе будут приведены рекомендации по работе с элементами ActiveX и другим активным содержимым.

## Ограничение элементов ActiveX

Пользователи зачастую желают устанавливать программное обеспечение, например элементы ActiveX, которое не разрешено политикой безопасности, принятой на предприятии. Это ПО может отрицательно сказаться на безопасности и конфиденциальности сетей. Чтобы не дать пользователям устанавливать неразрешенные элементы ActiveX, мы рекомендуем использовать групповую политику, которая подавит задание вопроса о разрешении установки в процессах Internet Explorer, запретив тем самым установку элементов ActiveX из Internet Explorer. Важно отметить, что это ограничение распространяется также на вполне законные элементы ActiveX controls, которые могут быть необходимы для нормальной деятельности предприятия, например Windows Update. Ограничивая установку элементов ActiveX, не забудьте воспользоваться каким-либо механизмом, например групповой политикой, для помещения всех необходимых элементов ActiveX на рабочие столы пользователей. Дополнительные сведения об этой рекомендации см. в следующем разделе. Применение этого ограничения также требует организации какого-либо альтернативного способа доставки обновлений безопасности, например службы Windows Server® Update Services (WSUS).

В следующей таблице приведено имя объекта политики и его расположение в групповой политике.

Таблица 2.1. Ограничение возможности установки элементов ActiveX

| **Объект политики** | **Расположение** |
| --- | --- |
| Процессы Internet Explorer (ограничение установки элементов ActiveX) | Конфигурация компьютера\Административные шаблоны\Компоненты Windows  \Internet Explorer\Средства безопасности\Ограничение установки элементов ActiveX |

## Управление настройками ActiveX на уровне узла

Internet Explorer 8 дает администраторам возможность управлять элементами ActiveX на уровне отдельного узла и, следовательно, разрешать выполнение таких элементов только на тех узлах, которые были одобрены.

IT-специалисты, отвечающие за администрирование системы, состоящей из компьютеров с установленным Internet Explorer 8, могут при желании заранее установить разрешенные элементы и ассоциировать с ними домены. Реализовать и применить такие параметры можно с помощью каталога Active Directory и групповой политики. Разрешенные домены и элементы управления хранятся в следующем разделе куста реестра HKEY\_CURRENT\_USER:

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{CLSID} \iexplore\AllowedDomains\{Домен или \*}**

Здесь {CLSID} – это Class ID рассматриваемого элемента, а {Домен или \*} –домены, которым разрешено запускать указанный элемент управления (\* представляет все домены).

Допустимы следующие значения:

REG\_DWORD Blocked

REG\_DWORD Count

REG\_DWORD Flags

REG\_DWORD Binary

REG\_DWORD Type

## Использование элементов ActiveX, подключаемых модулей и предварительно утвержденных списков

Вышеупомянутый параметр гарантирует, что элементы ActiveX не смогут работать на клиентском компьютере, если предварительно не были одобрены. Однако в некоторых организациях такая настройка считается чрезмерно ограничительной. В таком случае как минимум отключите параметр **Разрешить запуск элементов управления ActiveX, которые ранее не использовались, без предупреждения** для зон **Интернет** и **Ограниченные узлы**; такая конфигурация установлена в обозревателе по умолчанию. При такой настройке, известной еще как режим ActiveX Opt-In, гарантируется, что элементы управления будут использоваться, как задумано, и система не подвергнется атаке просто из-за того, что пользователь зашел на некий веб-узел. Однако у режима ActiveX Opt-In есть и недостаток, заключающийся в том, что хорошо известные и безвредные узлы не будут функционировать как должно, если пользователь не разрешит запуск элемента управления.

Каким бы образом вы ни ограничивали установку элементов ActiveX, всегда остается риск негативного влияния на необходимую предприятию функциональность. Поэтому мы рекомендуем скопировать заранее одобренные элементы на компьютеры пользователей, которыми вы управляете, например, с помощью групповой политики, и включить их в предварительно утвержденный список для Windows, добавив CLSID (глобально уникальный идентификатор, однозначно определяющий COM-класс) каждого элемента в следующий раздел реестра:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Ext\PreApproved**

Примечание. Если элемент ActiveX содержит уязвимость, представляющую угрозу для пользователей, то Майкрософт может запретить его использование с помощью обновления безопасности, распространяемого через узлы Windows Update, Microsoft Update или Windows Server Update Services. В таком случае элемент отключается, даже если он входит в список предварительно утвержденных.

Установленный элемент можно включать и выключать, манипулируя флагами в разделе реестра, который соответствует глобально уникальному идентификатору (GUID) элемента. Если у вас еще нет каталога GUID'ов, используемых на предприятии, то его нужно обязательно составить. Один из способов составить список GUID’ов таков: установить операционную систему на чистый компьютер, вручную сконфигурировать ее, установить все используемые на предприятии приложения и посмотреть, какие GUID’ы появились в ветви реестра, которая относится к Internet Explorer. Так вы получите минимальный перечень элементов управления, необходимых в вашей среде. Затем этот перечень GUID’ов можно использовать для составления списка предварительно утвержденных элементов.

Для работы с внутренним списком утвержденных элементов управления мы рекомендуем использовать объекты групповой политики, поскольку это повышает безопасность и эффективность функции ActiveX Opt-In. Дополнительные сведения о безопасности элементов ActiveX и о рекомендуемых способах управления ими см. статью [Безопасность ActiveX: усовершенствования и передовой опыт](http://go.microsoft.com/fwlink/?linkid=131978) (на английском языке) в MSDN®.

# Отключение активных сценариев

В 2002 году корпорация Майрософт внедрила методику Security Design Lifecycle (SDL), чтобы повысить качество ПО с точки зрения безопасности и уменьшить последствия обнаруженных уязвимостей. Хотя SDL доказала свою эффективность и привела к существенному уменьшению количества уязвимостей и эксплойтов, все равно совершенных программ и процессов не существует. Новая функциональность, появившаяся в Web 2.0, принесла с собой и новые угрозы безопасности. Да, разработка защищенного кода очень важна, но не менее важно иметь план реагирования на возможную компрометацию или уязвимость. Бывает, что уязвимость начинает эксплуатироваться еще до того, как о ней сообщено компании-производителю. Такие уязвимости получили название *уязвимости нулевого дня*.

Бывает также, что об уязвимости сообщено, но для разработки и надлежащего тестирования устраняющей ее заплаты требуется время. Чтобы уменьшить потенциальный риск, порекомендуйте пользователям не заходить на неизвестные веб-узлы и с осторожностью щелкать ссылки. Кроме того, администраторы могут воспользоваться параметром **Активные сценарии**, чтобы защититься от вновь обнаруженной уязвимости, для которой еще не выпущено обновление. Мы рекомендуем с помощью групповой политики устанавливать для этого параметра значение **Отключить** в качестве реакции на атаки нулевого дня и другие критические атаки посредством сценариев. Однако при обычных обстоятельствах его лучше оставить включенным, чтобы не препятствовать нормальному функционированию веб-узла и не мешать работе пользователей.

Посмотреть и сконфигурировать параметр **Активные сценарии** можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.2. Параметр «Активные сценарии»

| **Объект политики** | **Описание** |
| --- | --- |
| Активные сценарии | Этот параметр определяет, разрешено ли выполнение сценариев в указанной *<зоне>*.  По умолчанию сценарии на страницах, отнесенных к указанной *<зоне>*, запускаются без подтверждения. |

### Поддержка сценариев

В обозревателе Internet Explorer имеется поддержка клиентских сценариев. Так называются программы, загружаемые из веб и выполняемые в обозревателе пользователя. Распространенным частным случаем клиентских сценариев являются внедренные сценарии, которые включены непосредственно в HTML-документ. Другая разновидность – внешние сценарии. Это отдельные файлы, на которые имеется ссылка в документе, где они используются. В Internet Explorer 8 встроена поддержка нескольких языков сценариев, в том числе VBScript, JScript® и ECMAScript.

Клиентские сценарии – необычайно важная особенность обозревателя, так как она позволяет посетителю веб-узла видеть содержимое, динамически изменяющееся в зависимости от тех или иных условий, например: версии обозревателя, времени суток или учетных данных пользователя. Но такая мощь сопряжена с определенными опасностями, а поскольку сценарий поступает с веб-сервера, то следует разрешать его локальное выполнение лишь, если сервер заслуживает доверия. В этом и последующих разделах приведены рекомендации, как уменьшить риск, связанный с запуском клиентских сценариев.

Примечание. В этом разделе рассматриваются клиентские сценарии. Не путайте их с серверными сценариями. Веб-серверы, например Internet Information Services (IIS), обычно поддерживают написание серверных сценариев на таких языках, как VBScript, JScript или Perl. Результат работы серверного сценария доставляется в виде стандартного HTML-содержимого, поэтому для пользователя они не так опасны, как клиентские сценарии.

## Включение ограничений безопасности для обрабатываемых сценариями окон

Internet Explorer позволяет сценариям программно открывать окна разных типов, а также изменять их размер и положение на экране. В частности, таким образом можно открыть всплывающее окно, в котором заголовок и строка состояния либо не видны, либо перекрывают заголовок и строку состояния другого окна.

Мы рекомендуем с помощью групповой политики запретить запуск подобных сценариев в процессах Internet Explorer и Windows Explorer.

Посмотреть и сконфигурировать параметр «Ограничения безопасности для обрабатываемых сценариями окон» можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Ограничения безопасности для обрабатываемых сценариями окон**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.3. Параметр «Ограничения безопасности для обрабатываемых сценариями окон»

| **Объект политики** | **Описание** |
| --- | --- |
| Все процессы | Если этот параметр включен, то на обработку окон сценариями налагаются ограничения во всех процессах.  По умолчанию обработка окон сценариями в обозревателе не ограничена. |

# Обеспечение безопасности с помощью зон

В Internet Explorer большая часть параметров, относящихся к безопасности, сосредоточена в зонах безопасности. По умолчанию пользователь может вносить в зоны изменения следующими способами: изменить назначенный зоне уровень безопасности, задать специальные параметры для каждой зоны или добавить узлы в зоны **Местная интрасеть**, **Надежные узлы** либо **Ограниченные узлы**. Администраторам большинства организаций мы рекомендуем с помощью групповой политики зафиксировать уровни безопасности зон и запретить пользователям вносить многие изменения. В следующих разделах описано, как повысить зонную безопасность в Internet Explorer 8.

## Включение защиты от повышения уровня зоны

Internet Explorer налагает ограничения на каждую открываемую веб-страницу. Ограничения зависят от того, в какой зоне открывается страница: **Интернет**, **Местная интрасеть** или **Локальный компьютер**. На страницы, расположенные на локальном компьютере и отнесенные, следовательно, к зоне **Локальный компьютер**, налагается меньше всего ограничений, что делает их самой заманчивой мишенью для атак злоумышленников.

Если включить параметр **Защита от повышения уровня зоны**, то процессы Internet Explorer смогут защитить любую зону от повышения уровня. Такой подход позволяет предотвратить исполнение содержимого, отнесенного к одной зоне, с повышенными привилегиями, ассоциированными с другой зоной. Если отключить этот параметр политики, то ни одна зона не получит такой защиты.

Из-за серьезности последствий и относительной частоты атак на повышение уровня зоны мы рекомендуем включать параметр **Защита от повышения уровня зоны**.

Посмотреть и сконфигурировать параметр **Защита от повышения уровня зоны** можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Защита от повышения уровня зоны**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.4. Параметр «Защита от повышения уровня зоны»

| **Объект политики** | **Описание** |
| --- | --- |
| Процессы Internet Explorer | Internet Explorer налагает ограничения на каждую открываемую веб-страницу. Ограничения зависят от того, в какой зоне находится страница (Интернет, Местная интрасеть, Локальный компьютер и так далее). На страницы, расположенные на локальном компьютере и отнесенные к зоне **Локальный компьютер**, налагается меньше всего ограничений, что делает их самой заманчивой мишенью для атак злоумышленников. Повышение уровня зоны также отключает переход с помощью JavaScript, если отсутствует контекст безопасности.  Если этот параметр политики включен, то любая зона может быть защищена от повышения уровня процессами Internet Explorer.  Если отключить этот параметр, то ни одна зона не получит такой защиты.  Если этот параметр не задан, то любая зона может быть защищена от повышения уровня процессами Internet Explorer |

## Не разрешайте пользователям добавлять в зону узлы или удалять узлы из зоны

По умолчанию пользователи могут добавлять узлы в зоны **Местная интрасеть**, **Надежные узлы** и **Ограниченные узлы**, а также удалять узлы из этих зон. Добавление узла в зону **Надежные узлы** или удаление его из зоны **Ограниченные узлы** потенциально может привести к запуску вредоносного кода на компьютере.

Мы рекомендуем с помощью групповой политики запретить пользователям добавление и удаление узлов для зоны безопасности. Помимо этого, параметр групповой политики **Не разрешать пользователям добавлять или удалять веб-узлы для зоны безопасности** запрещает пользователям изменять параметры в зоне Местная интрасеть.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.5. Параметр «Не разрешать пользователям добавлять или удалять узлы для зоны безопасности»

| **Объект политики** | **Описание** |
| --- | --- |
| Зоны безопасности: Не разрешать пользователям добавлять/удалять узлы | Этот параметр запрещает пользователям добавлять и удалять узлы для зон безопасности.  Если он отключен или не задан, то пользователи смогут добавлять и удалять узлы для зон **Надежные узлы** и **Ограниченные узлы**, а также изменять параметры в зоне **Локальный компьютер**. |

Хотя мы рекомендуем включать этот параметр, следует понимать, что он может негативно отразиться на работе пользователей, особенно в сочетании с дополнительными ограничениями на зону **Интернет**. В некоторых случаях у пользователя может возникнуть желание добавить узел в менее ограниченную зону, если он не может получить к нему доступ в зоне Интернет. Если такая возможность отключена, то пользователь не сможет зайти на конкретный узел, пока администратор от его имени не поместит узел в менее ограниченную зону.

Примечание. Если включить параметр **Отключить вкладку «Безопасность»** (находится в папке \Конфигурация пользователя\Административные шаблоны\Компоненты Windows \Internet Explorer\Панель управления обозревателем), то вкладка **Безопасность** исчезнет из интерфейса, причем этому параметру отдается приоритет над параметрами зон безопасности.

## Не разрешайте пользователям изменять политики для зон безопасности

По умолчанию пользователь может изменить уровень безопасности для любой зоны, переместив ползунок на вкладке **Безопасность** в окне **Свойства обозревателя**. Кроме того, пользователям разрешено задавать нестандартные параметры для зон. Тем самым пользователь может изменить любой параметр, и, как следствие, понизить уровень безопасности и разрешить выполнение вредоносного кода.

Мы рекомендуем с помощью групповой политики запретить пользователям изменять уровень безопасности или модифицировать настройки для любой зоны, включив параметр **Запретить пользователям изменять политики**.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.6. Параметр «Запретить пользователям изменять политики»

| **Объект политики** | **Описание** |
| --- | --- |
| Зоны безопасности: Запретить пользователям изменять политики для зон безопасности | Этот параметр запрещает пользователям изменять параметры зон безопасности.  Если он отключен или не задан, то пользователи смогут изменять параметры зон безопасности. |

Примечание. Если включить параметр **Отключить вкладку «Безопасность»** (находится в папке \Конфигурация пользователя\Административные шаблоны\Компоненты Windows \Internet Explorer\Панель управления обозревателем), то вкладка **Безопасность** исчезнет из интерфейса, причем этому параметру отдается приоритет над параметрами зон безопасности.

# Обеспечение безопасности с помощью сертификатов

Для безопасной передачи данных между обозревателем и сервером необходимо использовать сертификаты и протокол SSL или Transport Layer Security (TLS). Internet Explorer 8 поддерживает как SSL, так и TLS, причем обозреватель пытается известить пользователя о таких проблемах или ошибках, как истечение срока действия сертификата или несовпадение имен. По умолчанию в Internet Explorer 8 установлен режим, когда в окне красным цветом показывается предупреждение об ошибке сертификата, призывающее пользователя проявить осторожность и, быть может, воздержаться от посещения узла. Но при желании пользователь может продолжить операцию. Существует много причин, по которым сертификат может содержать ошибку, но общедоступные, правильно обслуживаемые узлы не должны генерировать ошибочные сертификаты. Описываемый ниже параметр позволяет администраторам воспрепятствовать игнорированию сообщения об ошибке сертификата и тем самым снизить риск подвергнуться атаке.

## Запрещайте пользователям доступ к узлам с ошибочными сертификатами

Со временем сертификат может быть отозван или у него может истечь срок действия. Бывает также, что для конкретной веб-страницы используется некорректный сертификат или фактический адрес веб-узла не соответствует адресу, указанному в сертификате. По умолчанию обозреватель предупреждает пользователя об ошибках сертификата, но разрешает продолжить переход к веб-странице. Проблема в том, что любой человек может выпустить самозаверенный сертификат, якобы связанный с легитимным веб-узлом, а затем создать свой узел, внешне полностью повторяющий легитимный. Internet Explorer выводит предупреждение, когда обнаруживает сертификат, который не был выпущен доверенным центром сертификации. Однако, если пользователь привык игнорировать сообщения об ошибках и предупреждения, не задумываясь об их важности, то его легко обманом заманить на вредоносный веб-узел. Хотя отозванный или истекший сертификат сам по себе не несет угрозы безопасности, он может свидетельствовать о том, что данному узлу больше нельзя доверять. Поэтому мы рекомендуем с помощью групповой политики включить параметр **Запретить пропуск ошибок сертификата**, чтобы не дать пользователям перейти на узел, для которого выдается сообщение об ошибке сертификата.

Включение этого объекта политики никак не скажется на производительности, но может вызвать обращения в службу поддержки со стороны пользователей, которым не удается зайти на интересующие их узлы. На узлы, перечисленные в зоне **Надежные узлы**, этот параметр не распространяется, поэтому если критически важный для работы предприятия узел имеет сертификат с истекшим сроком действия или не совпадающими именами, то в качестве временной меры, до замены сертификата, его можно поместить в зону **Надежные узлы**.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.7. Параметр «Запретить пропуск ошибок сертификата»

| **Объект политики** | **Описание** |
| --- | --- |
| Запретить пропуск ошибок сертификата | Internet Explorer считает фатальными любые ошибки SSL/TLS-сертификата, например «истек срок действия», «отозван» или «несовпадение имен», и прерывает переход к узлу.  Если этот параметр отключен или не задан, то пользователи смогут игнорировать ошибку и продолжить операцию.  Мы рекомендуем включать этот параметр, чтобы пользователи не могли перейти к узлу с некорректным или не заслуживающим доверия сертификатом. |

# Понижение уровня привилегий приложения

Один из способов обезопасить клиентские компьютеры заключается в том, чтобы уменьшить потенциальные последствия атаки. Эксперты по безопасности часто напоминают пользователям, что входить в систему следует с минимальными привилегиями и повышать их лишь в случае необходимости. *Защищенный режим* обозревателя Internet Explorer® 8 для Windows® 7 и Windows Vista® упрощает следование этому совету. Internet Explorer 8® для Windows® XP предоставляет пользователям полезные средства защиты, которыми можно воспользоваться с помощью приложения DropMyRights. Дополнительные сведения см. в статье [Применение принципа наименьших привилегий к учетным записям пользователей в системе Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx) (на английском языке). Хотя эти решения работают по-разному, то и другое помогает уменьшить последствия атаки с повышением привилегий. Поэтому мы рекомендуем воспользоваться решением, ориентированным на вашу операционную систему. В следующих разделах рассматриваются оба решения.

## Включайте защищенный режим

По умолчанию защищенный режим в обозревателе Internet Explorer 8 для Windows Vista и Windows 7 включен в зонах безопасности **Интернет** и **Ограниченные узлы**. Это средство призвано обеспечить усиленную защиту пользователя и системы за счет того, что возможности приложения по обращению к определенным областям файловой системы и реестра ограничены. Эти ограничения устроены так, чтобы изолировать процесс Internet Explorer и не дать вредоносному веб-узлу или другой программе использовать обозреватель для повреждения информации пользователя или нанесения вреда системе. Однако пользователь может его отключить, что негативно скажется на общей безопасности. Поэтому мы рекомендуем с помощью групповой политики принудительно включить защищенный режим в зонах **Интернет** и **Ограниченные узлы** и запретить пользователям его отключение.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.8. Параметр «Включить защищенный режим»

| **Объект политики** | **Описание** |
| --- | --- |
| Включить защищенный режим | Этот параметр защищает Internet Explorer от уязвимостей путем ограничения тех областей в файловой системе и реестре, куда обозреватель может производить запись.  По умолчанию защищенный режим включен, но пользователь может его отключить. |

Этот параметр применим только к Internet Explorer® 8 для Windows® 7 и Windows Vista®. Кроме того, он не применим к Internet Explorer 8 при работе в режиме Windows XP на компьютере с установленной ОС Windows 7.

Защищенный режим в Internet Explorer 8 действует для следующих областей и зон безопасности:

зона Интернета;

зона интрасети;

зона локального компьютера;

заблокированная зона Интернета;

заблокированная зона интрасети;

заблокированная зона локального компьютера;

заблокированная зона ограниченных узлов;

заблокированная зона надежных узлов;

зона ограниченных узлов;

зона надежных узлов.

Примечание. Если важный для предприятия узел или веб-приложение не может работать правильно из-за того, что установлен защищенный режим, не следует отключать этот режим, поскольку это негативно отразится на общей безопасности обозревателя. Вместо этого обратитесь к владельцу узла и попросите, чтобы он обновил свой узел, так чтобы тот мог корректно работать в защищенном режиме. В качестве временной меры можно добавить узел в зону **Надежные узлы**.

## Используйте приложение DropMyRights в Windows XP

DropMyRights – это простое приложение, предназначенное для пользователей, которые должны работать на компьютере от имени администратора; оно позволяет запускать приложения в гораздо более безопасном контексте, как если бы пользователь вошел в систему от имени неадминистративной учетной записи. Хотя работать от имени стандартного пользователя безопаснее, чем от имени администратора, в тех случаях, когда альтернативы нет, вы можете воспользоваться приложением DropMyRights на компьютерах с установленным обозревателем Internet Explorer 8 для Windows XP, так как в этой среде защищенный режим не реализован.

DropMyRights исключает различные привилегии и идентификаторы безопасности (SID) из текущего маркера безопасности пользователя, а затем запускает другой процесс с измененным маркером. Дополнительную информацию о приложении DropMyRights и его исходный код можно найти на странице MSDN [Безопасный просмотр веб и чтение электронной почты от имени администратора](http://msdn2.microsoft.com/en-us/library/ms972827.aspx) (на английском языке). После того как приложение DropMyRights установлено, для запуска в нем Internet Explorer достаточно создать новый ярлык, указывающий на исполняемый файл DropMyRights, а после него – путь к приложению, которое нужно запустить с пониженными привилегиями.

# Прочие параметры безопасности

Помимо параметров, рассмотренных в других главах настоящего руководства, существуют и иные параметры, позволяющие обезопасить компьютеры в конкретной среде. В этом разделе мы опишем некоторые из них и дадим рекомендации, как следует изменить их значения по умолчанию, чтобы повысить безопасность пользователей, работающих с обозревателем Internet Explorer 8.

### Возможность пробной проверки MIME

Эта функция предотвращает изменение типа файла на другой, более опасный. Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Возможность пробной проверки MIME**

В следующей таблице перечислены параметры, относящиеся к этой функции.

Таблица 2.9. Параметр «Возможность пробной проверки MIME»

| **Объект политики** | **Описание** |
| --- | --- |
| Все процессы | Если этот параметр включен, то возможность пробной проверки MIME будет включена для всех процессов. |
| Процессы Internet Explorer | Если этот параметр выключен, то процессы Internet Explorer будут разрешать пробной проверке MIME обработку файла как файла потенциально более опасного типа.  Значение по умолчанию (**Не задан**) запрещает изменение типа. ‡ |
| Список процессов | Эта политика позволяет администраторам явно определять те приложения, для которых рассматриваемая функция должна быть включена или выключена. |

В этой таблице приведены лишь упрощенные описания значений параметров. Дополнительные сведения можно почерпнуть на вкладке **Объяснение** в редакторе объектов групповой политики.

### Ограничение безопасности для MK-протокола

Политика «Ограничение безопасности для MK-протокола» уменьшает возможности для атаки, запрещая MK-протокол. Если она включена, то для ресурсов, размещенных на MK, произойдет сбой протокола. MK-протокол представляет собой устаревший механизм связывания файлов справки Windows с веб-страницами. Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Ограничение безопасности для MK-протокола**

В следующей таблице перечислены параметры, относящиеся к этой функции.

Таблица 2.10. Параметры политики «Ограничение безопасности для MK-протокола»

| **Объект политики** | **Описание** |
| --- | --- |
| Все процессы | По умолчанию это ограничение для всех процессов отключено. Однако, если включить его, то MK-протокол будет заблокирован для всех процессов, то есть любое использование MK-протокола запрещено. |
| Процессы Internet Explorer | Если этот параметр отключен, то приложения могут использовать API MK-протокола, и для ресурсов, размещенных на MK, протокол будет работать для процессов Проводника Windows и Internet Explorer.  Значение, заданное по умолчанию, запрещает использование MK-протокола для Проводника Windows и Internet Explorer, а ресурсы, размещенные на MK, блокируются. ‡ |
| Список процессов | Этот параметр политики позволяет администраторам явно определять те приложения, для которых рассматриваемая функция должна быть включена или выключена. |

В этой таблице приведены лишь упрощенные описания значений параметров. Дополнительные сведения можно почерпнуть на вкладке **Объяснение** в редакторе объектов групповой политики.

## Не сохраняйте зашифрованные страницы на диске

Чтобы создать дополнительные удобства пользователям при просмотре веб, Internet Explorer может кэшировать содержимое на локальном диске (в папке временных файлов Интернета), чтобы его можно было извлечь немедленно, а не обращаться каждый раз к ресурсу в сети со всеми вытекающими отсюда задержками. Internet Explorer позволяет кэшировать как зашифрованное, так и незашифрованное содержимое, причем по умолчанию кэшируется то и другое.

Хотя при кэшировании зашифрованного содержимого в папке временных файлов Интернета могут остаться конфиденциальные HTTPS-документы, Майкрософт не отключает кэширование зашифрованных файлов, следуя указаниям по кэшированию, полученным от веб-сервера. Кроме того, кэширование зашифрованных данных способствует повышению производительности труда пользователей при повторном просмотре идентичного содержимого, например, изображений. Обычно считается, что риск, сопряженный с дешифрированием файлов в локальном кэше, невелик, поскольку это, во-первых, трудно осуществить, а, во-вторых, информация в этих файлах не представляет большой ценности. Даже если атакующему удастся дешифрировать документ, имя и пароль пользователя он, как правило, не увидит. Он сможет просмотреть лишь содержимое страниц. Однако и сами страницы могут содержать секретную информацию, например, остатки на счетах или детали сделки.

Если необходимо ужесточить параметры безопасности Internet Explorer для пользователей, то можно с помощью политики **Не сохранять зашифрованные страницы на диск** запретить кэширование зашифрованных файлов и лишить злонамеренных пользователей возможности получить к ним доступ. После включения этого параметра могут возникнуть проблемы с производительностью, задержки, увеличение сетевого трафика и дополнительные обращения в службу поддержки. Владельцы общедоступных веб-узлов обычно рассчитывают на то, что этот параметр отключен, и, следовательно, к их серверам будет несколько меньше обращений, но серьезных последствий для работы приложений его включение вызвать не должно.

Включение этого параметра может негативно сказаться на доступе к содержимому, которое генерируется по запросу, например, к отчетам о движении средств на счете. Проблема возникает, когда пользователь получает отчет, затем переходит на какую-то другую страницу, а затем нажимает кнопку **Назад** в обозревателе, чтобы еще раз просмотреть страницу с отчетом. Если веб-сервер сконфигурирован правильно, то пользователь в этом случае увидит сообщение о том, что срок хранения страницы истек, и для просмотра содержимого должен будет нажать кнопку **Обновить**.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница 'Дополнительно'**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица. 2.11. Параметр «Не сохранять зашифрованные страницы на диск»

| **Объект политики** | **Описание** |
| --- | --- |
| Не сохранять зашифрованные страницы на диск | Этот параметр политики позволяет управлять тем, будет ли Internet Explorer сохранять в кэше зашифрованные страницы, содержащие защищенную (HTTPS) информацию, например, пароли или номера кредитных карт, что может быть небезопасно.  Если этот параметр включен, Internet Explorer не будет сохранять в кэше зашифрованные страницы, содержащие защищенную (HTTPS) информацию.  Если этот параметр политики отключен или не задан, Internet Explorer будет сохранять в кэше зашифрованные страницы, содержащие защищенную (HTTPS) информацию.  Мы рекомендуем включать этот параметр только в тех средах, где веб-страницы содержат секретные данные. |

## Задавайте параметры прокси для компьютера, а не для пользователя

Бывает, что после изменения параметры прокси-сервера пользователь не может получить доступ к веб-узлам. Однако мобильным пользователям иногда необходимо изменять параметры прокси-сервера, чтобы получить возможность доступа к веб из разных точек.

Для стационарных компьютеров мы рекомендуем воспользоваться групповой политикой и установить режим, при котором параметры прокси-сервера определяются для компьютера в целом, а не для каждого пользователя в отдельности. Но пользователям мобильных ноутбуков следует оставить возможность настраивания параметров прокси-сервера, чтобы обеспечить необходимую гибкость доступа к Интернету.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.12. Параметр «Задать параметры прокси для компьютера»

| **Объект политики** | **Описание** |
| --- | --- |
| Задать параметры прокси для компьютера (а не для пользователя) | Применяет параметры прокси ко всем пользователям на данном компьютере. Если этот параметр политики включен, то пользователь не сможет задать параметры прокси только для себя. Он должен будет работать с зонами, созданными для всех пользователей данного компьютера.  Если этот параметр отключен или не задан, пользователи этого компьютера могут устанавливать свои собственные параметры прокси.  Этот параметр предназначается для того, чтобы обеспечить единообразное применение параметров прокси на одном компьютере, не позволяя изменять их для разных пользователей.  Мы рекомендуем включать этот параметр для стационарных компьютеров и отключать для портативных. |

## Отключайте обнаружение аварийных сбоев

В Internet Explorer 8 реализована функция обнаружения сбоев, которая генерирует отчет о сбое, полезный для поиска и устранения неполадок в работе обозревателя. Однако отчет может содержать секретную информацию из оперативной памяти компьютера, поэтому большинству предприятий мы рекомендуем эту функцию отключать. Хотя информация, отправляемая в корпорацию Майкрософт, когда эта функция включена, используется исключительно для анализа данных о сбое, в отчет может быть непреднамеренно включена информация, подпадающая под действие законов о защите данных. Отключение этой функции позволит организации соблюсти требования законодательства, относящегося к контролю над доступом к информации. После отключения функции обнаружения аварийных сбоев любой сбой в Internet Explorer будет обрабатываться, как на компьютере с установленной системой Windows XP Professional Service Pack 1 (SP1) или более ранней версией. Точнее, вызывается средство «Отчет об ошибках Windows» и применяются все политики, заданные для этого средства.

Если сбои происходят часто и необходимо отправить отчет для поиска и устранения причин, то можно временно включить эту функцию на подверженных сбоям компьютерах.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.13. Параметр «Отключить обнаружение аварийных сбоев»

| **Объект политики** | **Описание** |
| --- | --- |
| Отключить обнаружение аварийных сбоев | Этот параметр политики позволяет управлять средством обнаружения аварийных сбоев, встроенным в механизм управления надстройками  Если этот параметр отключен или не задан, то средство обнаружения аварийных сбоев будет работать.  Мы рекомендуем включать этот параметр. |

## Включайте ограничение загрузки файлов

В некоторых случаях веб-узел может инициировать появление запроса на загрузку файла без явных действий со стороны пользователя. Такая техника дает сайту возможность помещать нежелательные файлы на жесткий диск пользователя, если тот случайно нажмет не ту кнопку и подтвердит согласие на загрузку.

Мы рекомендуем включать политику **Ограничение загрузки файлов**. Тогда в процессах Internet Explorer будут блокироваться запросы на загрузку файла, не инициированные пользователем.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Ограничение загрузки файлов**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.14. Параметр «Ограничение загрузки файлов»

| **Объект политики** | **Описание** |
| --- | --- |
| Процессы Internet Explorer | Этот параметр политики включает режим блокировки запросов на загрузку файлов, не инициированных пользователем.  Если он включен, то в процессах Internet Explorer будут блокироваться запросы на загрузку файла, не инициированные пользователем.  Если этот параметр отключен, то в процессах Internet Explorer не блокируется появление запросов на загрузку файла, не инициированных пользователем.  Если этот параметр не задан, то появление запросов на загрузку файла, не инициированных пользователем, регулируется пользовательскими настройками.  Мы рекомендуем включать этот параметр. |

## Запрещайте загрузку файлов для зоны «Ограниченные узлы»

По умолчанию загрузка файлов для зоны «Ограниченные узлы» запрещена. Однако мы рекомендуем явно отключить параметр политики **Разрешать загрузку файлов**, чтобы пользователи не могли загружать файлы с узлов, входящих в зону **Ограниченные узлы**.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.15. Параметр «Разрешать загрузку файлов»

| **Объект политики** | **Описание** |
| --- | --- |
| Разрешать загрузку файлов | Этот параметр политики управляет тем, разрешена ли загрузка файлов из зоны **Ограниченные узлы**. Действие параметра определяется той зоной, в которой находится страница со ссылкой, вызывающей загрузку, а не той зоной, из которой доставляется загружаемый файл.  Если этот параметр включен, то можно загружать файлы из этой зоны.  Если этот параметр отключен, будет запрещено загружать файлы из этой зоны.  Если этот параметр не задан, будет запрещено загружать файлы из этой зоны.  Мы рекомендуем отключать этот параметр. |

## Пользуйтесь функцией защиты кэшируемых объектов

Функция защиты кэшируемых объектов предотвращает ссылку на объект, находящийся в кэше, после того как пользователь покинет веб-узел, с которого этот объект был загружен. Она создает новый контекст безопасности для всех программируемых объектов, поэтому доступ к кэшированным объектам блокируется. Доступ блокируется даже тогда, когда пользователь просматривает узлы из одного и того же домена (с одинаковым полным доменным именем). После изменения контекста в результате перехода ссылка на объект перестает быть доступной. Разработчики приложений должны знать о таком ограничении безопасности и не создавать приложения, в которых используются объекты с других веб-узлов, поскольку в этом случае страница может отображаться некорректно. По умолчанию этот параметр включен для процессов Internet Explorer, и мы рекомендуем с помощью групповой политики навязать такое поведение, явно включив политику **Защита кэшируемых объектов**. Включение этой политики уменьшает риск подвергнуться атакам, связанным с междоменным доступом. Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Средства безопасности\Защита кэшируемых объектов**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.16. Параметр «Защита кэшируемых объектов»

| **Объект политики** | **Описание** |
| --- | --- |
| Процессы Internet Explorer | Этот параметр политики определяет, будет ли доступна ссылка на объект при переходе в пределах одного домена или к новому домену.  Если этот параметр включен, то ссылка на объект становится недоступной в процессах Internet Explorer при переходе в пределах одного домена или к новому домену.  Если этот параметр отключен, то ссылка на объект остается доступной в процессах Internet Explorer при переходе в пределах одного домена или к новому домену.  Если этот параметр не задан, то ссылка на объект становится недоступной в процессах Internet Explorer при переходе в пределах одного домена или к новому домену.  Мы рекомендуем включать этот параметр. |

### Разрешения Java

По поводу разрешений Java в Internet Explorer возникла некоторая путаница. Многие полагают, что этот параметр относится только к виртуальной машине Java корпорации Майкрософт (Microsoft Java Virtual Machine – MSJVM). Действительно, Майкрософт не думает, что виртуальные машины Java (JVM) других производителей обращают внимание на этот параметр. Однако же этот параметр блокирует применение элемента <APPLET> в HTML-разметке. Это означает, что при определенных условиях этот параметр может помешать нормальному отображению страницы, которой необходима JVM, даже если установлена JVM стороннего производителя. Другие HTML-элементы могут использовать JVM, так что это поведение зависит от содержимого веб-узла.

По умолчанию этот параметр отключен в зонах **Интернет** и **Ограниченные узлы**.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 2.17. Параметр «Разрешения Java»

| **Объект политики** | **Описание** |
| --- | --- |
| Разрешения Java | Этот параметр политики позволяет управлять разрешениями для приложений Java.  Если он включен, можно выбрать параметры из следующего раскрывающегося списка:  **Особые параметры** управление разрешениями по отдельности.  **Низкая безопасность** разрешает приложениям Java выполнять любые операции.  **Средняя безопасность** приложения запускаются в «песочнице» (участок памяти, за пределами которого программа не может никуда обращаться), и им доступно временное безопасное хранилище на клиентском компьютере и управляемый пользователем файловый ввод/вывод.  **Высокая безопасность** запуск приложений в «песочнице». **Отключить Java** Предотвращается запуск всех приложений путем отключения Java.  Если этот параметр политики отключен, то приложения Java не запускаются.  Если этот параметр политики не задан, предполагается, что для него установлено значение **Высокая безопасность**. |

# Дополнительные сведения

Подробнее о вопросах безопасности Internet Explorer 8 можно узнать из следующих источников на Microsoft.com:

[Безопасность ActiveX: усовершенствования и передовой опыт](http://go.microsoft.com/fwlink/?linkid=131978) (на английском языке).

[Применение принципа наименьших привилегий к учетным записям пользователей в системе Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx) (на английском языке).

[Безопасный просмотр веб и чтение электронной почты от имени администратора](http://msdn2.microsoft.com/en-us/library/ms972827.aspx) (на английском языке).

## Отзывы

Вопросы и замечания по данному руководству просьба направлять по адресу [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).

Глава 3. Рекомендации по настройке конфиденциальности

Часто авторы руководств по безопасности ограничиваются рассмотрением параметров, позволяющих предотвратить манипулирование системой. Однако для полноты обсуждения необходимо включить также анализ параметров, влияющих на конфиденциальность и сохранность личных данных. В Windows® Internet Explorer® 8 появилось несколько усовершенствований с целью защиты личных данных от целой категории угроз несанкционированного раскрытия. К этим усовершенствованиям относится, в частности, фильтр SmartScreen, который извещает пользователя о подставных веб-узлах и узлах, распространяющих вредоносные программы.

Повысить безопасность обозревателя можно также путем изменения подразумеваемых по умолчанию параметров, управляющих удалением данных по завершении работы с обозревателем и обработкой данных форм. Кроме того, удаление временных файлов Интернета гарантирует регулярное стирание личных данных и предотвращает нежелательное раскрытие или считывание информации. Аналогично запрет автоматического заполнения форм и сохранения паролей уменьшает опасность несанкционированного доступа к личным учетным данным и информации.

Параметры конфиденциальности Internet Explorer 8 и приводимые в этой главе рекомендации можно разбить на девять категорий:

просмотр в режиме InPrivate;

фильтрация InPrivate;

удаление истории обзора;

перемещение ползунка конфиденциальности в положение «Средний» или «Умеренно высокий»;

автоматическая очистка папки временных файлов Интернета;

отключение автоматического заполнения форм;

задание параметров входа для каждой зоны безопасности;

включение фильтра SmartScreen;

фильтр запуска сценариев между узлами (XSS).

Некоторым организациям необходима возможность следить за тем, как служащие используют Internet Explorer®. В таком случае необходимо решить, что важнее: сохранять протокол операций обозревателя или соблюдать права служащих на конфиденциальность. Не исключено, что администратор такой организации сочтет более полезным задать для некоторых рассматриваемых в этой главе параметров значения, противоположные нашим рекомендациям, чтобы пользователи не могли удалить историю обзора и другие исторические данные.

# Просмотр в режиме InPrivate

Иногда нежелательно оставлять на компьютере какие-либо следы своего пребывания в веб, например, при покупке с семейного компьютера подарка в Интернет-магазине. Функция *просмотра InPrivate* в Internet Explorer подавляет сохранение обозревателем истории обзора, временных файлов Интернета, данных форм, файлов cookie, а также имен и паролей пользователей, поэтому не остается ни свидетельств, ни истории посещения узлов.

Чтобы начать просмотр в режиме InPrivate, нажмите кнопку **Безопасность** на главной панели окна обозревателя и выберите из меню пункт **Просмотр** **InPrivate**. В ответ Internet Explorer 8 начинает новый сеанс, в котором не сохраняется никакая информация, в том числе о поисках и посещениях веб-страниц. Чтобы завершить просмотр InPrivate, просто закройте окно обозревателя.

Режим просмотра InPrivate отличается следующими особенностями:

отключаются модули поддержки обозревателя (BHO) и панели инструментов;

все новые файлы cookie становятся «сеансовыми» и удаляются при выходе из обозревателя;

уже имеющиеся файлы cookie не считываются;

невозможно внести изменения в существующее хранилище DOM;

в историю обзора не добавляются новые записи;

вновь созданные временные файлы Интернета удаляются после закрытия окна просмотра InPrivate;

не сохраняются данные форм;

не сохраняются пароли;

не сохраняются адреса, введенные в адресной строке;

не сохраняются запросы, введенные в поле поиска.

не сохраняется информация о посещенных страницах;

Организация может разрешить или запретить эту функцию в зависимости от требований бизнеса, правил и законодательства. Просмотр InPrivate можно сделать режимом по умолчанию, если в командную строку запуска обозревателя добавить флаг -private, например:

C:\Program Files\Internet Explorer\iexplore.exe" –private

# Фильтрация InPrivate

Функция *Фильтрация InPrivate* предназначена для отслеживания и блокировки только того содержимого сторонних узлов, которое часто встречается на посещаемых вами узлах. Никакое содержимое не блокируется, пока не будет достигнут некоторый порог, а, кроме того, не блокируется содержимое, генерируемое самим просматриваемым узлом. В зависимости от того какие узлы вы посещаете и как часто, время, необходимое для того, чтобы эффект фильтрации – автоматическая блокировка содержимого – стал виден, может изменяться в широких пределах. Задавать частоту появления отслеживаемых узлов, которые добавляются в список фильтрации, могут как администраторы, так и пользователи; для этого достаточно выбрать значение уровня: число от 3 до 30. Пользователь может также импортировать из корпоративной общей папки или другого источника стандартный набор узлов, содержимое которых следует разрешить или заблокировать. Мы рекомендуем включать фильтрацию InPrivate, если это не мешает работе узлов, необходимых для нормального функционирования предприятия.

# Удаление истории обзора

Хотя возможность удаления истории обзора – не новость в Internet Explorer, в версии 8 она была улучшена в нескольких отношениях. Теперь при удалении истории можно сохранять файлы cookie и временные файлы Интернета для узлов в папке Избранное. Это позволяет защитить свою информацию и оградить конфиденциальность, сохранив в то же время данные с избранных узлов, которым вы доверяете. Ваши настройки и файлы cookie не удаляются, так что впоследствии обращение к избранным узлам будет происходить так же быстро, как и раньше. К числу нововведений относится также возможность удалить данные, собранные функцией фильтрации InPrivate, как показано на рисунке ниже.

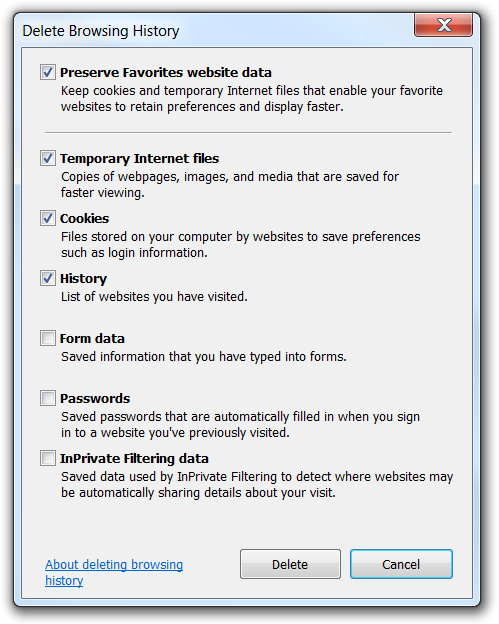


Рисунок 3.1. Удаление истории обзора

В новом интерфейсе удаления истории обзора имеются также флажки, позволяющие избирательно указать, какие данные следует удалить, а какие оставить.

# Перемещение ползунка конфиденциальности в положение «Средний» или «Умеренно высокий»

Некоторые веб-узлы сохраняют на компьютере информацию в виде небольших файлов для того, чтобы предлагать страницы, персонализированные с учетом поведения пользователя в Интернете. Эти файлы, называемые *cookie*, могут быть использованы для корреляции действий конкретного пользователя в сети. Корпорация Майкрософт выступает в поддержку использования файлов «cookie» и полагает, что они не представляют угрозы безопасности и не являются вредоносным программным обеспечением. Однако в Internet Explorer 8 встроено несколько механизмов управления файлами «cookie», позволяющих пользователю контролировать их использование с помощью параметров конфиденциальности.

Существует два вида файлов «cookie». *Основные файлы cookie* либо поступают от веб-узла, который просматривается в данный момент, либо посылаются ему. Эти файлы cookie обычно используются для хранения такой информации, как настройки, заданные пользователем для конкретного узла. *Сторонние файлы cookie* либо поступают, либо посылаются веб-узлу, отличному от просматриваемого. Сторонние веб-узлы как правило поставляют некоторое содержимое просматриваемому узлу. Например, многие узлы пользуются рекламными службами, размещенными на сторонних узлах, которые могут применять файлы cookie. Типичное применение файлов cookie такого рода состоит в том, чтобы отследить какие веб-страницы посещает пользователь, – в рекламных или маркетинговых целях.

Параметры безопасности, влияющие на конфиденциальность, находятся на вкладке **Конфиденциальность** в диалоговом окне **Свойства обозревателя**. На этой вкладке имеется ползунок, который позволяет выбрать один из шести режимов: от **Блокировать все файлы cookie** до **Принимать все файлы cookie**. Действие этого ползунка распространяется только на зону Интернет. От узлов в зонах **Местная интрасеть** и **Надежные узлы** автоматически принимаются все файлы cookie, а от узлов в зоне **Ограниченные узлы** все файлы cookie автоматически блокируются.

Организация должна определить, какая политика применяется к файлам cookie. Мы рекомендуем использовать хотя бы установленный по умолчанию режим **Средний**, в котором выполняются следующие действия:

блокируются сторонние файлы cookie, не удовлетворяющие политике конфиденциальности;

блокируются сторонние файлы cookie, содержащие идентифицирующие пользователя сведения без его явного согласия;

ограничиваются основные файлы cookie, содержащие идентифицирующие пользователя сведения без его явного согласия.

В режиме **Высокий** блокируются все файлы cookie с веб-узлов, не удовлетворяющих политике конфиденциальности, тогда как в других режимах такие файлы при определенных условиях принимаются. В режиме **Низкий** принимаются все файлы cookie без ограничений.

**Примечание.** По умолчанию пользователь может изменить стандартное положение ползунка конфиденциальности, хотя групповая политика позволяет воспрепятствовать этому, вообще исключив вкладку **Конфиденциальность** из диалогового окна **Свойства обозревателя**.

Разрешается добавить узлы-исключения, для которых общая настройка не действует. При добавлении узла можно указать один из двух режимов: **Запретить** или **Разрешить**. Добавлять узлы можно вне зависимости от того, выбрана более или менее ограничительная политика конфиденциальности. Групповая политика позволяет не только навязать параметры обработки файлов cookie, но и добавлять узлы-исключения. Чтобы обеспечить максимально возможную конфиденциальность, не отказываясь от преимуществ файлов cookie (например, сохранение регистрационной информации, настроек и т.д.), мы рекомендуем блокировать все сторонние и разрешить все основные файлы cookie.

# Автоматическая очистка папки временных файлов Интернета

Чтобы увеличить скорость загрузки страниц и уменьшить сетевой трафик, Internet Explorer создает папку временных файлов Интернета (Temporary Internet Files), в которой хранятся копии различных загруженных из веб документов (HTML, видео, изображения и т.д.). Эта область, по определению, временная, и данные в ней могут перезаписываться. Хотя хранящиеся там файлы не считаются дистанционной доступными, просмотр их другими пользователями компьютера может стать причиной раскрытия личной информации и нарушения конфиденциальности. По умолчанию локальные копии файлов помещаются в папку %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files. Однако с помощью набора средств [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx) или объекта групповой политики можно изменить это местоположение, модифицировав параметр в папке «Панель управления обозревателем». Мы рекомендуем изменить установленное по умолчанию значение этого параметра и включить его, чтобы все сохраненные локально файлы удалялись, когда пользователь закрывает обозреватель. Изменение этого параметра не влияет на функциональность, но может отразиться на производительности и стать причиной обращений в службу поддержки.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница 'Дополнительно'**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.1. Настройка папки временных файлов

| **Объект политики** | **Описание** |
| --- | --- |
| Удалять все файлы из папки временных файлов | Этот параметр политики позволяет управлять тем, будет ли Internet Explorer удалять содержимое папки временных файлов (Temporary Internet Files) после того, как все окна обозревателя будут закрыты. Такая политика защищает от сохранения потенциально опасных файлов на компьютере, или конфиденциальных файлов, которые могут стать доступны другим пользователям, а также сберегает место на диске.  По умолчанию Internet Explorer не удаляет содержимое папки временных файлов после того, как все окна обозревателя будут закрыты.  Мы рекомендуем включать этот параметр. |

**Примечание**. В тех организациях, которые обязаны следовать требованиям законодательства о контроле и конфиденциальности данных, эта функция может использоваться для гарантированного регулярного удаления информации. Эта функция не противодействует восстановлению данных с помощью электронно-криминалистических средств. Поэтому рекомендуется проверить, достаточно ли обеспечиваемой ей защиты для удовлетворения требований о соответствии.

# Отключение автоматического заполнения форм

Эта функция, как и предыдущая, позволяет обозревателю запоминать введенные в форму данные для последующего извлечения и отправки. Например, во многих формах есть поле «адрес». Функция автозаполнения позволяет Internet Explorer прочитать запомненные ранее значения и автоматически поместить их в поле, освободив пользователя от необходимости вводить данные снова и снова. Хотя такие поля, как «адрес», не представляют прямой угрозы безопасности, эта информация все же может быть полезна вредоносному веб-узлу.

Но важнее то, что описываемая функция не способна отличить действительно секретные данные, например сведения о кредитных карточках, от менее конфиденциальной информации, например, номера телефона. Из-за этого может произойти непреднамеренное и нежелательное раскрытие информации о пользователе. Параметры этой функции задаются в диалоговом окне **Настройка автозаполнения**, для открытия которого нужно нажать кнопку **Параметры** в области **Автозаполнение** на вкладке **Содержание** в окне **Свойства обозревателя**.

Internet Explorer 8 умеет также запоминать имена и пароли пользователей, введенные в форме. Для доступа к различным компьютерным системам пользователям приходится запоминать все больше имен и паролей. Internet Explorer предлагает средства для сохранения учетных данных и автоматического ввода их в форму, когда это требуется. Существуют некоторые базовые механизмы защиты, определяющие, какие данные следует вводить в конкретную форму, чтобы избежать передачи веб-узлу не относящихся к нему учетных данных. Однако изобретательно запрограммированный вредоносный веб-узел может обманом убедить пользователя ввести свои учетные данные. Хранилище учетных данных защищено, находится в локальной системе и недоступно извне. Мы рекомендуем отключать функцию автозаполнения форм и запретить пользователям ее применение для ввода имен и паролей в формы.

Изменение этих параметров не влияет на производительность приложения, но может вызвать недовольство пользователей и побудить их придумывать слабые пароли, которые легче запомнить. Администраторам рекомендуется пересмотреть требования к паролям и процедурам контроля, чтобы воспрепятствовать применению небезопасных паролей.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.2. Параметры автозаполнения

| **Объект политики** | **Описание** |
| --- | --- |
| Отключить автозаполнение для форм | Этот параметр предлагает возможные варианты при заполнении форм пользователями. Если этот параметр включен, пользователям не будут предлагаться варианты заполнения форм. Пользователь не сможет изменить его.  Если этот параметр отключен, пользователям будут предлагаться возможные варианты заполнения форм. Пользователь не сможет изменить его.  По умолчанию пользователь имеет право включить или отключить функцию автозаполнения для форм.  Мы рекомендуем включать этот параметр. |
| Включить автозаполнение для имен пользователей и паролей в формах | Этот параметр управляет функцией автозаполнения в Internet Explorer, которая запоминает и предлагает пользователю имена и пароли в формах. Если этот параметр включен, пользователь получит доступ к этой функции и не сможет изменить параметры **Имя и пароль пользователя в формах** или **Запрашивать сохранение пароля**. При включенном параметре пользователь сам должен решить, устанавливать ли флажок **Запрашивать сохранение пароля**.  Если этот параметр отключен, пользователь не получит доступа к этой функции и не сможет изменить параметры.  Если этот параметр не задан, пользователь сможет включить автозаполнение для ввода имен и паролей в формы. Пользователь может включить эти функции, нажав кнопку **Параметры** на вкладке **Содержание** в диалоговом окне **Свойства обозревателя**, которое доступно с помощью меню **Сервис**.  Мы рекомендуем отключать этот параметр. |

**Примечание**. В тех организациях, которые обязаны следовать требованиям законодательства о контроле и конфиденциальности данных, эта функция может использоваться, чтобы гарантированно не сохранять информацию и не разделять ее с неавторизованными пользователями.

# Задание параметров входа для каждой зоны

Корпоративные и коммерческие клиенты могут использовать домены Windows для защиты информации в интрасети, предоставляя в то же время пользователям доступ к хранящимся в сети документам без повторного ввода учетных данных. Internet Explorer может использовать учетные данные для входа в систему и поддерживает NTLM-аутентификацию для узлов в зоне **Местная интрасеть**. Эта функция обеспечивает более высокий уровень контроля, чем обычные установки **Включить** и **Отключить**. По умолчанию для зон **Интернет**, **Местная интрасеть** и **Надежные узлы** установлен параметр **Автоматический вход в сеть только в зоне интрасети**, а для зоны **Ограниченные узлы** – параметр **Запрашивать имя пользователя и пароль**. В результате пользователи могут автоматически входить на узлы интрасети, к которым имеют доступ, но должны вводить учетные данные при заходе на узлы в других зонах безопасности.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация компьютера\Административные шаблоны\Компоненты Windows**

**\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.3. Параметры входа в систему

| **Объект политики** | **Описание** |
| --- | --- |
| Параметры входа в систему  (Зона Интернета) | Этот параметр позволяет управлять настройкой параметров входа. Если он включен, можно выбрать один из следующих вариантов входа.  **Анонимный вход** для отключения проверки подлинности HTTP и использования учетной записи гостя только для протокола CIFS (Common Internet File System).  **Запрос имени пользователя и пароля** - выдача запроса пользователю об учетной записи и пароле. После выдачи запроса эти значения могут повторно использоваться автоматически в течение текущего сеанса  **Автоматический вход только в зону интрасети** –выдача запроса пользователю об учетной записи и пароле для всех остальных зон После выдачи запроса эти значения могут повторно использоваться автоматически в течение текущего сеанса  **Автоматический вход с текущим именем пользователя и паролем** для входа с использованием протокола Windows NT Challenge Response (проверки подлинности NTLM) Если протокол Windows NT Challenge Response поддерживается сервером, то для входа используется сетевое имя пользователя и пароль Если протокол Windows NT Challenge Response не поддерживается сервером, пользователь получает запрос на ввод имени пользователя и пароля.  Если этот параметр политики отключен, параметр входа имеет значение **Автоматический вход только в зону интрасети**. Если этот параметр политики не задан, параметр входа имеет значение **Автоматический вход только в зону интрасети**.  Мы рекомендуем задавать для этого параметра значение **Запрос имени пользователя и пароля**. |
| Параметры входа в систему  (Зона интрасети) | Мы рекомендуем задавать для этого параметра значение **Автоматический вход с текущим именем пользователя и паролем**. |
| Параметры входа в систему  (Зона ограниченных узлов | Мы рекомендуем задавать для этого параметра значение **Анонимный вход**. |
| Параметры входа в систему  (Зона надежных узлов | Мы рекомендуем задавать для этого параметра значение **Автоматический вход только в зону интрасети**. |

**Примечание**. В тех организациях, которые обязаны следовать требованиям законодательства о контроле и конфиденциальности данных, эта функция может использоваться, чтобы гарантированно не сохранять информацию и не разделять ее с неавторизованными пользователями.

# Включение фильтра SmartScreen

Находясь в сети, пользователи подвергаются все большему числу угроз со стороны вредоносных узлов, стремящихся украсть учетные данные. Среди прочих нововведений в Internet Explorer 8 включена функция *Фильтр SmartScreen*, объединяющая в себе эвристический анализ информации на клиентском компьютере с онлайновыми службами, чтобы защитить пользователей от угроз и веб-узлов, стремящихся украсть личную информацию или распространяющих вредоносное ПО. По умолчанию при первом запуске Internet Explorer 8 фильтр SmartScreen предлагает пользователю включить автоматическую проверку или отключить функцию вовсе, оставляя возможность проверить узел вручную, – никакого подразумеваемого по умолчанию режима нет. Таким образом, пользователь получает «все или ничего» – в зависимости от того, включен фильтр или нет. Если фильтр SmartScreen отключен, пользователь все же может воспользоваться этой функцией, вручную затребовав проверку конкретного веб-узла.

Важно, чтобы системные и сетевые администраторы понимали, какие приложения работают в подведомственной им среде. Internet Explorer и фильтр SmartScreen – не исключения; чем лучше вы понимаете принципы их работы, тем больше пользы можете получить от них и тем надежнее защитить себя от загрузки вредоносного ПО или раскрытия личных данных. Это особенно существенно, если принять во внимание важность и потенциальные требования законодательства о защите конфиденциальной информации в современной онлайновой среде.

Защита от вредоносного ПО и фишинга, реализованная в фильтре SmartScreen, основана на службе Microsoft URL Reputation Service (URS), которая круглосуточно предоставляет поддержку и расширенную поддержку. Если фильтр SmartScreen включен, то он просматривает локальный список известных легитимных узлов и отправляет адрес URL узла службе URS для проверки. Во избежание задержек обращения к URS производятся асинхронно, так что на работе пользователя это не отражается. Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список узлы не подвергаются проверке фильтром SmartScreen. В фильтре SmartScreen применяется также механизм локального кэширования адресов URL, позволяющий сохранять ранее полученные рейтинги узлов и избежать лишних обращений по сети. Один из способов выявления потенциально подставных узлов, применяемый службой URS, – сбор отзывов пользователей о ранее неизвестных узлах. Пользователь может решить, следует ли отправлять информацию об узле, добропорядочность которого вызывает у него подозрения.

Для обнаружения и защиты от фишинга и эксплойтов, сложность которых постоянно растет, фильтр SmartScreen исследует строку адреса URL целиком, а не подмножество адресов URL, на которые заходил пользователь. Следует отметить, что службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL. Корпорация Майкрософт приняла масштабные меры для того, чтобы сведения о пользователе оставались защищенными и конфиденциальными, не передавались другим организациям и исключались из полученных данных, как только надобность в них для анализа угрозы отпадет. Дополнительную информацию см. в [Заявлении о конфиденциальности для Windows Internet Explorer 8](http://go.microsoft.com/fwlink/?linkid=128106).

Как уже отмечалось, включить или отключить фильтр SmartScreen необходимо явно – по умолчанию ни тот, ни другой режим не устанавливается. Если фильтр включен, то все узлы, отсутствующие в локальном зашифрованном DAT-файле, проверяются как локально, так и с помощью службы URS. Если же фильтр SmartScreen отключен, то никакие проверки не производятся. Хотя Майкрософт настоятельно рекомендует всегда пользоваться фильтром SmartScreen для защиты пользователей, бывают ситуации, когда администратору необходимо взять управление этой функцией на себя.

**Примечание**: Защита от ClickJacking и запуска сценариев между узлами включена по умолчанию. Поддержка защиты от ClickJacking встроена в продукт и не отключается. Но фильтр запуска сценариев между узлами пользователь может отключить. Пользователь также может включить фильтр SmartScreen для защиты от фишинга и вредоносного ПО (см. выше).

Фильтр SmartScreen можно включать или отключать избирательно для каждой зоны безопасности, но только в случае, когда эта функция включена глобально. По умолчанию фильтр SmartScreen включен для всех зон, кроме **Местной интрасети**. Мы рекомендуем администраторам включать фильтр SmartScreen в подведомственной им среде.

Если вы хотите исключить некоторые узлы из списка проверяемых фильтром SmartScreen (например, узлы экстрасети, которой ваша компания доверяет), а не отключать фильтр полностью, то мы рекомендуем включить фильтр глобально, а затем отключить фильтрацию только для зоны **Надежные узлы**. После этого конкретные узлы можно будет добавить в зону **Надежные узлы**.

Мы также рекомендуем использовать групповую политику, чтобы не дать пользователям отключить фильтр SmartScreen, и установить режим автоматической проверки. Однако администратор должен понимать, что при такой конфигурации обозреватель будет автоматически отправлять информацию в корпорацию Майкрософт, не спрашивая согласия пользователя. Отправленные данные используются исключительно для совершенствования служб Майкрософт и защиты пользователей. Они не передаются другим организациям и не анализируются для установления личности пользователя. Дополнительную информацию см. в [Заявлении о конфиденциальности для Windows Internet Explorer 8](http://go.microsoft.com/fwlink/?linkid=128106).

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.4. Параметры фильтра SmartScreen

| **Объект политики** | **Описание** |
| --- | --- |
| Использовать фильтр SmartScreen | Этот параметр политики определяет, следует ли фильтру SmartScreen проверять страницы в этой зоне на наличие вредоносного содержимого.  Если этот параметр включен, фильтр SmartScreen будет проверять страницы в этой зоне на наличие вредоносного содержимого. Если этот параметр отключен, фильтр SmartScreen не будет проверять страницы в этой зоне на наличие вредоносного содержимого.  По умолчанию пользователю разрешено задавать этот параметрю  Мы рекомендуем включать этот параметр. |

Помимо задания параметров для каждой зоны, есть возможность посмотреть и задать два глобальных параметра фильтра SmartScreen в следующей папке редактора объектов групповой политики:

**Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Internet Explorer**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.5. Глобальные параметры фильтра SmartScreen

| **Объект политики** | **Описание** |
| --- | --- |
| Отключить управление фильтром SmartScreen | Этот параметр позволяет пользователю включить фильтр SmartScreen, который будет предупреждать о том, что посещаемый веб-узел может собирать личные сведения мошенническим путем или содержит вредоносное ПО.  Если включить этот параметр, пользователь не увидит предложения включить фильтр SmartScreen; при этом адреса всех веб-узлов, отсутствующих в списке разрешенных узлов фильтра, автоматически направляются корпорации Майкрософт, не спрашивая согласия пользователя  Если функция отключена или этот параметр не задан, пользователю будет предложено определить режим работы фильтра SmartScreen при первом запуске обозревателя. Мы рекомендуем включать этот параметр. |
| Предотвращение блокировки предупреждений фильтра SmartScreen | Этот параметр управляет поведением фильтра SmartScreen.  Если этот параметр включен, пользователю запрещается переходить на узлы, определенные фильтром SmartScreen как небезопасные.  Если этот параметр отключен или не задан, пользователь может пропустить предупреждения фильтра SmartScreen и перейти на небезопасные узлы.  Мы рекомендуем включать этот параметр. |

# Фильтр запуска сценариев между узлами (XSS)

Фильтр запуска сценариев между узлами (XSS) предназначен для того, чтобы оградить пользователей от непреднамеренного раскрытия информации. Это особенно важно для организаций, которые обязаны соблюдать законодательные предписания или доказывать соответствие требованиям безопасности..

Мы рекомендуем оставлять эту функцию включенной (по умолчанию), чтобы обеспечить защиту пользователей. Если попытка пользователя зайти на веб-узел, важный для деятельности предприятия, приводит к срабатывания фильтра XSS, то необходимо сначала разобраться, в чем причина. В качестве крайней меры можно временно отключить фильтрацию, но затем снова включить при первой возможности.

Посмотреть и сконфигурировать этот параметр можно в следующей папке редактора объектов групповой политики:

**Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления обозревателем\Страница безопасности\<*зона*>**

В следующей таблице приведены сведения о параметрах безопасности, относящихся к этой технологии в Internet Explorer 8.

Таблица 3.6. Параметры фильтра запуска сценариев между узлами (XSS)

| **Объект политики** | **Описание** |
| --- | --- |
| Включить фильтр запуска сценариев между узлами (XSS) | Этот параметр определяет, должен ли фильтр запуска сценариев между узлами (XSS) обнаруживать и предотвращать запуск сценария между узлами в этой зоне.  Если этот параметр включен, фильтр XSS будет пытаться блокировать запуск сценариев между узлами в этой зоне.  Если этот параметр отключен, фильтр XSS разрешает запуск сценариев между узлами в этой зоне.  Мы рекомендуем включать этот параметр. |

# Дополнительные сведения

Подробнее о вопросах безопасности Internet Explorer 8 можно узнать из следующих источников на Microsoft.com:

[*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx).

[Заявление о конфиденциальности для Windows Internet Explorer 8](http://go.microsoft.com/fwlink/?linkid=128106).

## Отзывы

Вопросы и замечания по данному руководству просьба направлять по адресу [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).

Приложение А. Контрольный список параметров безопасности Internet Explorer 8

Следующий контрольный список включает все параметры, на которые мы рекомендуем обратить внимание в процессе обеспечения безопасности клиентских компьютеров с установленным Windows® Internet Explorer 8 на конкретном предприятии.

Таблица A.1. Контрольный список параметров безопасности Internet Explorer 8

|  | Безопасность активного содержимого |
| --- | --- |
|  | Ограничение установки элементов ActiveX®. |
|  | Управление настройками ActiveX на уровне узла. |
|  | Включение элементов ActiveX и подключаемых модулей в предварительно утвержденные списки |
|  | Отключение параметра «Разрешить активные сценарии» в ответ на конкретные угрозы. |
|  | Включение ограничений безопасности для обрабатываемых сценариями окон. |
|  | Обеспечение безопасности с помощью зон |
|  | Включение защиты от повышения уровня зоны. |
|  | Запрет пользователям добавлять или удалять узлы для зоны. |
|  | Запрет пользователям изменять политики для зон безопасности. |
|  | Отказ от конфигурирования зоны безопасности «Локальный компьютер». |
|  | Обеспечение безопасности с помощью сертификатов |
|  | Предотвращение перехода в узел с сертификатом, содержащим ошибки. |
|  | Понижение уровня привилегий приложения |
|  | Использование защищенного режима на компьютерах под управлением Windows Vista®. |
|  | Использование приложения DropMyRights на компьютерах под управлением Windows® XP. |
|  | Параметры конфиденциальности |
|  | Использование просмотра в режиме InPrivate. |
|  | Использование фильтрации InPrivate. |
|  | Удаление истории обзора. |
|  | Перемещение ползунка конфиденциальности в положение «Средний» или «Умеренно высокий». |
|  | Очистка папки временных файлов при выходе пользователя из обозревателя. |
|  | Отключение автоматического заполнения форм. |
|  | Отключение кэширования паролей. |
|  | Задание параметров входа для каждой зоны безопасности. |
|  | Включение фильтра SmartScreen. |
|  | Использование фильтра запуска сценариев между узлами (XSS). |
|  | Прочие параметры безопасности |
|  | Задание параметров прокси для компьютера (а не для пользователя). |
|  | Отключение обнаружения аварийных сбоев. |
|  | Ограничение загрузки файлов. |
|  | Запрет загрузки файлов для зоны «Ограниченные узлы». |
|  | Включение функции защиты кэшируемых объектов |

# Дополнительные сведения

Подробнее о вопросах безопасности Internet Explorer 8 можно узнать из следующих источников на Microsoft.com:

[Заявление о конфиденциальности для Windows Internet Explorer 8](http://go.microsoft.com/fwlink/?linkid=128106).

## Отзывы

Вопросы и замечания по данному руководству просьба направлять по адресу [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).