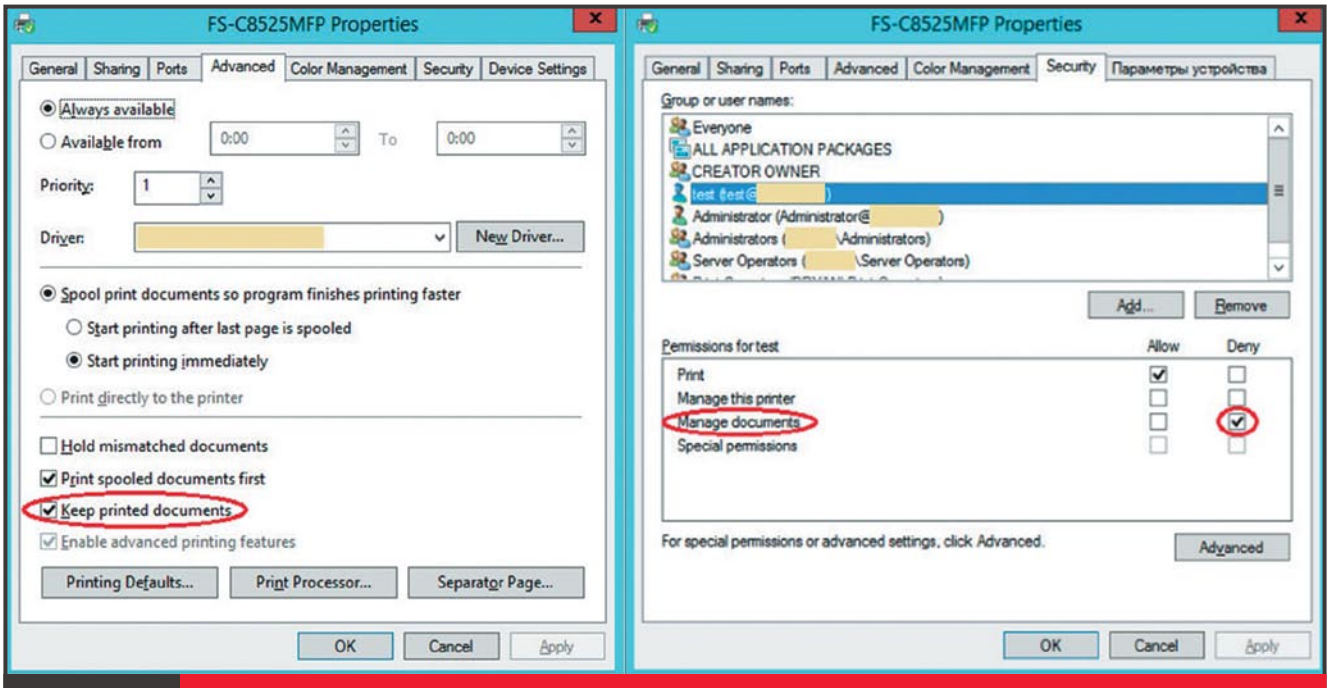
Создание системы предотвращения утечек информации с помощью решений Microsoft

Автоматизация процессов контроля санкционированных действий и попыток несанкционированной передачи конфиденциальных документов в электронной форме

Александр Кузнецов
Андрей Брянцев

Сегодня системы предотвращения утечек данных (Data Loss Prevention, DLP) представлены на рынке колоссальным количеством решений, которые постоянно развиваются. Аналитическое агентство Gartner уже много лет ведет отдельный «Магический квадрант» (Magic Quadrant) для данного класса решений. В этом году ФСТЭК России планирует выпустить классификацию и целевые требования для таких систем.

Несмотря на бурное развитие данного сегмента рынка, стоимость подобных решений остается достаточно высокой, особенно для небольших компаний, в том числе только начинающих свою деятельность. В связи с этим мы хотели бы рассмотреть функции, которые на первом этапе можно задействовать для решения задач автоматизации процессов контроля санкционированных действий и/или попыток несанкционированной передачи конфиденциальных документов в электронном виде. Прежде всего, это позволит техническим специалистам познакомиться с функция-



Экран 1 Контроль печати

ми контроля на практике, а также понять, насколько они совместимы с существующими в их компании бизнес- и технологическими процессами. И самое важное, что для этого не потребуется знания продуктов Open Source и/или инсталляции каких-либо дополнительных технических решений. Интерес к данным решениям вызван в первую очередь тем, что молодые компании столкнутся именно с ними, а кроме того, политика производителя с ограничением периода поддержки определенных версий программных продуктов становится все более жесткой, что подталкивает пользователей к переходу на актуальные версии.

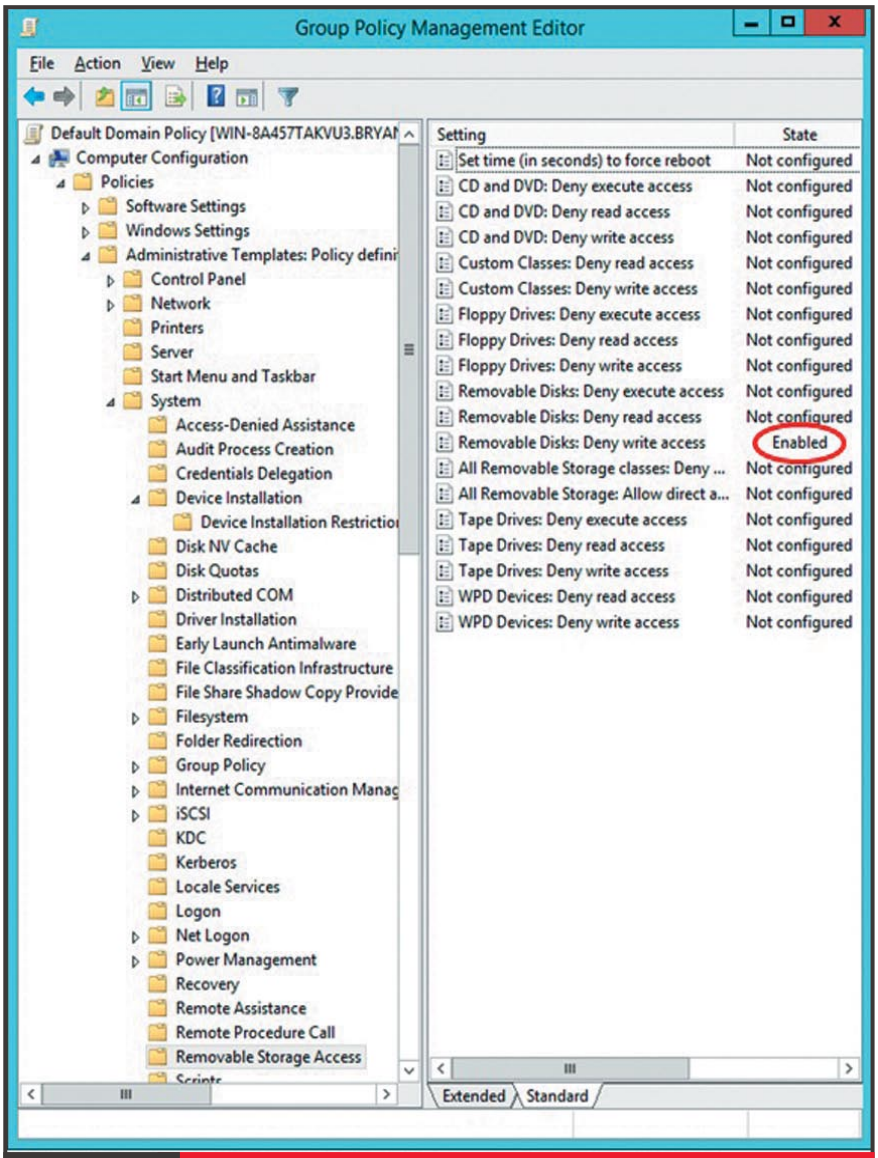
Для уточнения области охвата мы рассмотрим только последние версии программных решений от Microsoft Corp:

- Microsoft Windows Server 2012 R2;
- Microsoft Exchange 2013 R2;
- Microsoft Windows 8.1;
- Internet Explorer (IE) 11;
- Microsoft Office 2013;
- Skype версии от 6.x.

Кроме того, в поле нашего внимания попадут следующие наиболее распространенные каналы утечек данных:

- вывод на печать;
- копирование на съемные носители информации (прежде всего USB-носители);
- пересылка по корпоративной электронной почте;
- передача через Skype;
- публикация в Интернете.

Сразу стоит отметить, что мы не ставили своей целью формирование руководства по созданию DLP-системы «своими руками», а хотели представить экспертный взгляд и указать направления для дальнейших инженерных задач.



Экран 2 Запрет записи на внешние носители

Вывод на печать

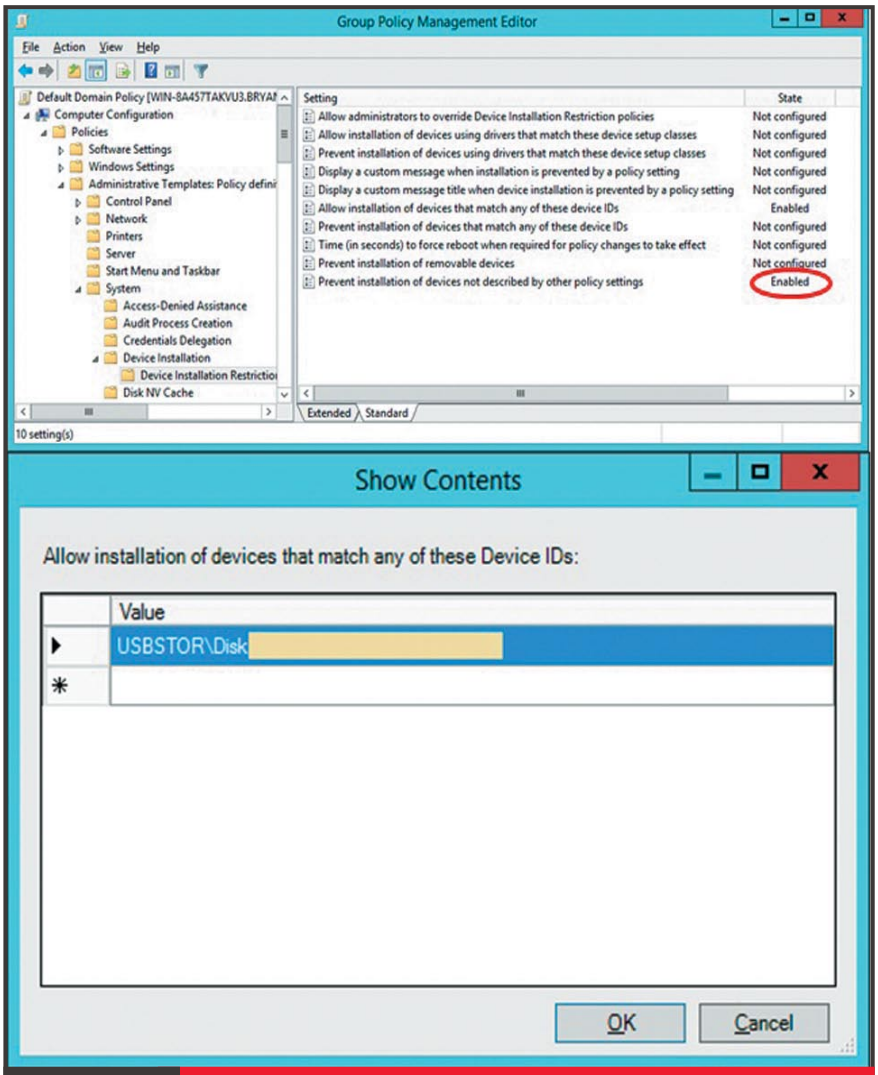
Контроль печати всегда сопряжен с риском прерывания или задержек в подготовке документов. Как показывает практика, вероятность таких рисков при использовании DLP ненулевая. Многие DLP-вендоры официально признают, что задержка может достигать нескольких минут, а попытки пользователя завершить или повторить операцию печати приводят к полноценному «зависанию» приложения. В связи с этим активно развивается концепция только мониторинга этого и других каналов утечек и использования полученных данных в случаях «разбора полетов».

Мы можем реализовать такой мониторинг путем сохранения очереди печати (Print Queue): <Имя принтера> Properties/Advanced/Keep printed documents — отметить.

Для того чтобы пользователи не смогли очистить очередь печати, необходимо запретить права Manage Documents контролируемым пользователям или группам (<Имя принтера> Properties/Security/<Имя группы контролируемых пользователей>/Manage documents/Deny — отметить). Однако надо быть внимательным с разрешением Deny (см. экран 1) и не допускать попадания в эти группы учетных записей администраторов, чтобы сохранить возможность управления очередью в случае необходимости.

Кроме того, для ведения журнала событий печати включается соответствующий аудит (<Имя принтера> Properties/Security/кнопка Advanced/Auditing/кнопка Add/<Имя группы контролируемых пользователей>/Print — отметить).

Просмотр «подозрительных» заданий печати возможен с помощью



Экран 3 Запрет использования внешних носителей

повторной отправки задания на принтер пользователем с правом Manage Documents.

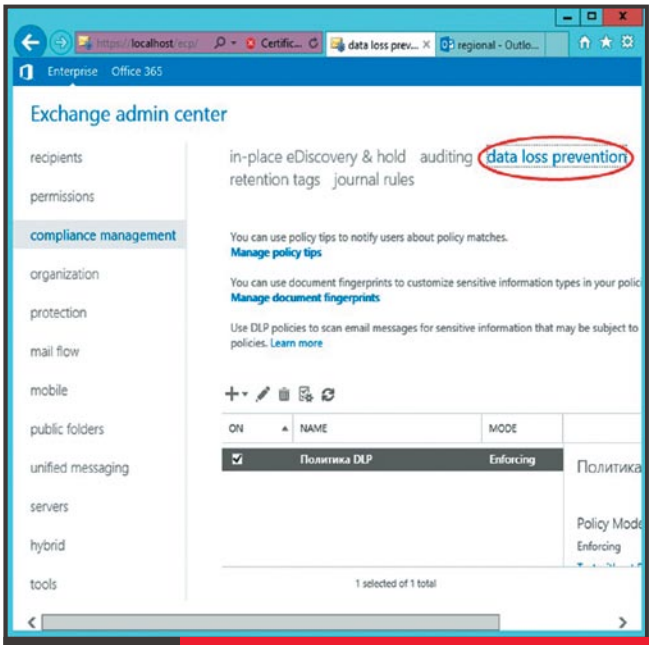
Съемные носители информации

За счет своей доступности USB-носитель является не только одним из лидеров в качестве источника вирусов, но и самым распространенным средством для «слива» информации.

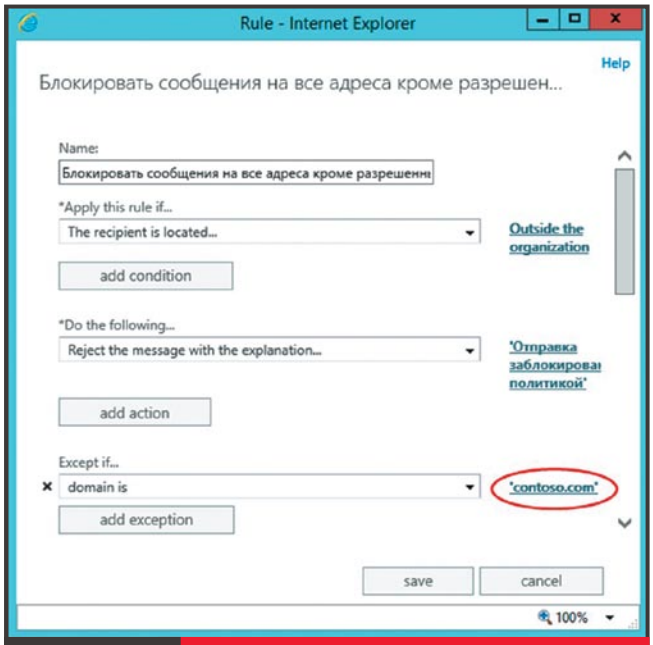
Безусловно, обращение с подобными носителями должно быть регламентировано внутри компании, но рассчитывать только на сознательность персонала, увы, не приходится. В данном случае за счет применения групповых политик (Group Policy) мы можем сформировать список только разрешенных, зачастую корпоративных, USB-носителей. Отметим, что в качестве положительного «побочного эффекта» это позволит частично реализовать и автоматизировать популярное в отечественной нормативной базе требование по учету носителей информации.

Для примера рассмотрим два доступных инструмента.

Запрет записи на любые внешние носители: Computer Configuration/Policies Administrative Templates/System/Removable Storage Access/



Экран 4 DLP в Exchange 2013



Экран 5 DLP-правило № 1 в Microsoft Exchange 2013

Removable Disks: Deny Write Access — Enabled (см. экран 2).

Запрет установки драйвера для внешнего накопителя, не соответствующего перечню Device ID, проводится так: перейти по Computer Configuration/Policies/Administrative Templates/System/Device Installation/Device Installation Restrictions/Allow installation of devices that match any of these device IDs — Enabled и ввести список ID разрешенных устройств (см. экран 3), а также запретить установку драйверов для устройств, не перечисленных в предыдущем параметре: Computer Configuration/Policies Administrative Templates/System/Device Installation/Device Installation Restrictions/Prevent installation of devices not described by other policy settings — Enabled.

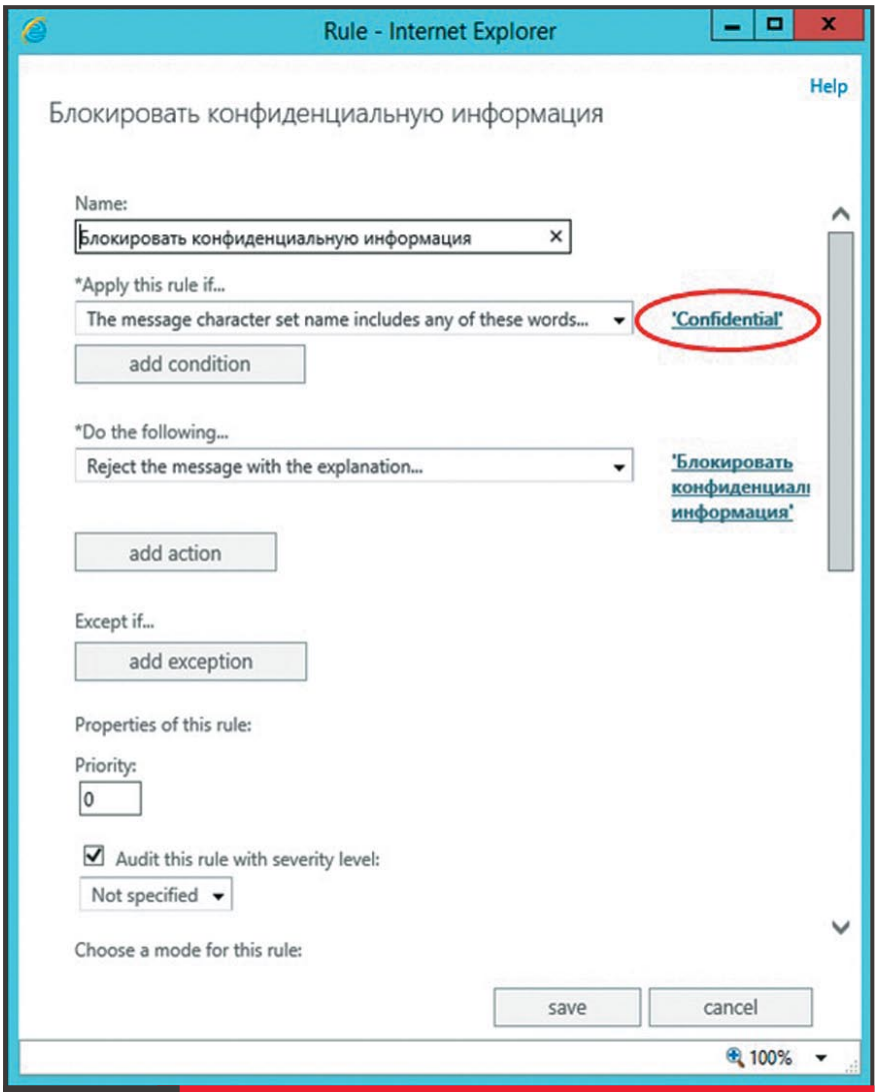
Корпоративная электронная почта

Если в предыдущем разделе мы использовали самый простой принцип контроля на базе белых и черных списков, без контекстного анализа, то здесь все будет на уровне промышленных DLP-решений, за счет наличия одноименной функциональности в Microsoft Exchange 2013 (см. экран 4).

В закладке data loss prevention раздела compliance management доступны перечисленные ниже возможности.

- Manage policy tips — всплывающие уведомления в интерфейсе пользователя о соответствии текущего сообщения электронной почты условиям политик;
- Manage document fingerprints — позволяет создавать отпечатки документов, на основании соответствия которым система будет принимать решения о применении политик;
- сам перечень политик с возможностью редактирования и управления режимами их тестирования/применения.

При редактировании правил и политик функциональность настолько широка, что заслуживает отдельной статьи, мы же приведем пару примеров самых простых правил:



Экран 6 DLP-правило № 2 в Microsoft Exchange 2013

- запрет отправки любого сообщения за пределы домашнего домена, кроме домена contoso.com (см. экран 5);
- запрет отправки любого сообщения, содержащего во вложениях слово Confidential (см. экран 6).

Для оперативного реагирования на инциденты и обработки ложных срабатываний политик настраиваются Incident Reports на почтовый ящик сотрудника службы информационной безопасности, а для более детального разбора существует мощный набор команд PowerShell.

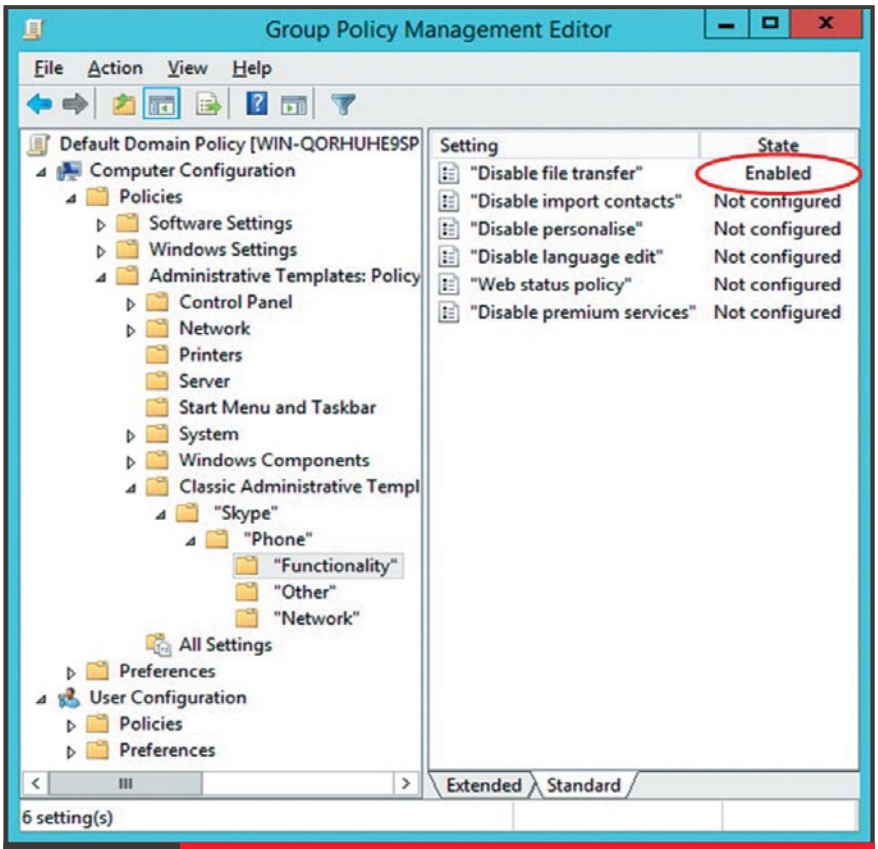
Skype

Возможность использования каких-либо мессенджеров всегда вызывала обеспокоенность специалистов по информационной безопасности, не является исключением и Skype.

Хотя сегодня для многих Skype стал стандартом де-факто корпоративной коммуникации, не все знают, что централизованно можно ограничить передачу документов с использованием данного решения за счет применения административных шаблонов с веб-сайта http://community.skype.com, для групповых политик (см. экран 7). Пользователь в случае попытки отправить файл получит соответствующее уведомление (см. экран 8).

Публикация в Интернете

Прежде чем рассматривать возможности контроля данного канала утечки, нужно уяснить, что программные решения Microsoft в рам-

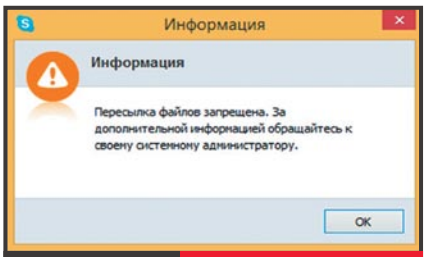


Экран 7 Запрет передачи файлов через Skype

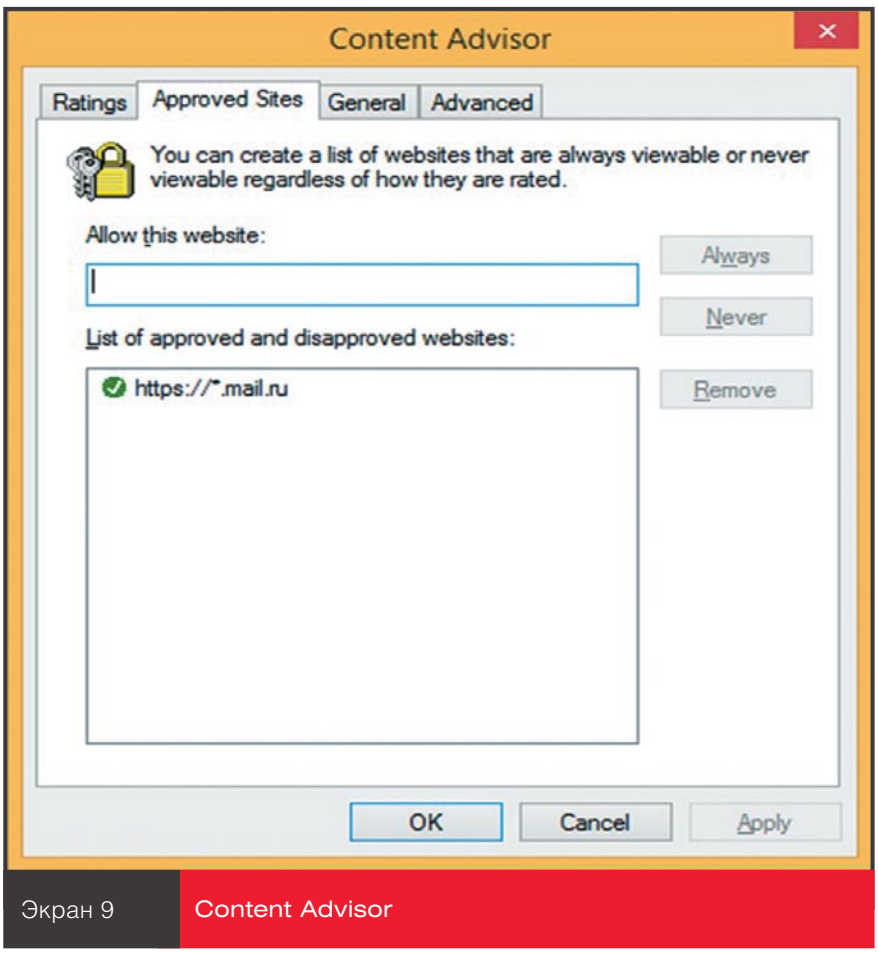
программ, в том числе IE. После этого отключаем правило по умолчанию для исходящих соединений Allow, а затем экспортируем эти настройки в файл с расширением wfw и импортируем в групповую политику: Computer Configuration/Policies/Windows Settings/Security Settings/Windows Firewall with Advanced Security.

В отношении доступа в Интернет мы рекомендуем использовать разрешительный принцип (все, что не разрешено, запрещено), формируя и поддерживая в актуальном состоянии только списки доверенных веб-ресурсов. Для этого необходимо также через групповые политики активировать закладку Content Advisor в настройках IE: Computer Configuration/Policies/Administrative Templates/Windows Components/Internet Control Panel/Content Page/Show Content Advisor on Internet Options — Enable.

В результате мы получаем на компьютерах локальный инструментарий, защищенный своим паролем от изменений пользователем



Экран 8 Уведомление



Экран 9 Content Advisor

ках корпоративных сетей не функционируют изолированно от аппаратного обеспечения и активного сетевого оборудования, а на него в основном и ложится реализация такого контроля.

Однако ряд мер мы можем принять уже на уровне отдельно взятого узла сети за счет централизованной настройки веб-браузеров. В первую очередь необходимо запретить возможность использования альтернативных веб-браузеров за счет применения групповых политик (Group Policy).

На эталонном компьютере создаем настройки брандмауэра (Windows Firewall) с прописанными правилами для всех необходимых

и в нем перечисляем шаблоны имен веб-сайтов, которые может открывать пользователь (см. экран 9).

Для централизованного распространения настроек Content Advisor производитель рекомендует использовать «Пакет администрирования Internet Explorer версии 11 (IEAK 11)». Можно обратиться к подробному описанию IEAK на сайте Microsoft: http://technet.micro-soft.com/ru-ru/library/dn338134.aspx.

Файловые хранилища

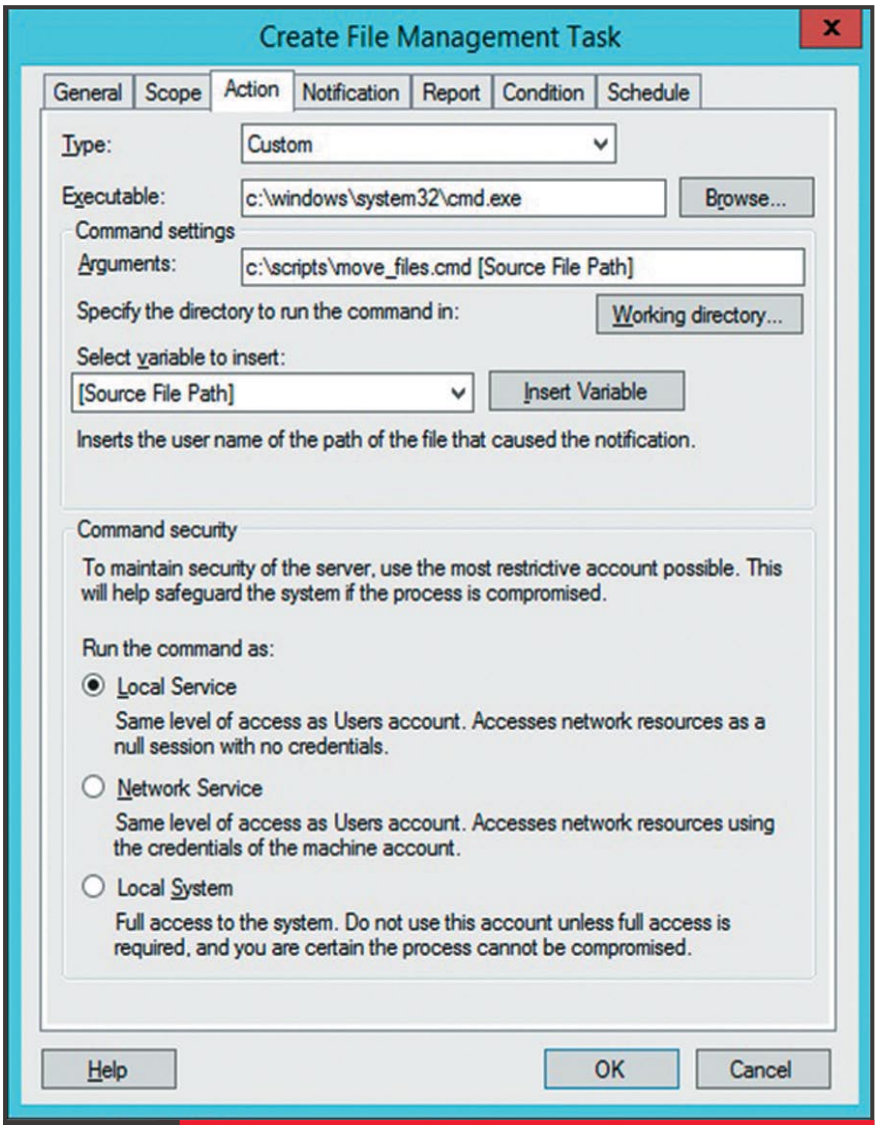
Несколько слов хотелось бы сказать о возможности категорирования файлов, расположенных на файл-серверах, функционирующих под управлением Microsoft Windows Server 2012. Подробно данная функциональность описана в статье Джона Сэвилла «Инфраструктура классификации файлов в Windows Server 2012» (Windows IT Pro/RE № 5 за 2014 год).

Технология File Classification Infrastructure (FCI) позволяет на основании имени файла, его расположения и содержимого присваивать дополнительные атрибуты для последующей обработки. Применение такого инструментария, как File Server Resource Manager (FSRM), к файловым хранилищам совместно со скриптами позволяет на периодической основе или даже в реальном времени выявлять нарушение политик хранения конфиденциальных документов и перемещать эти документы в специально отведенные каталоги на файл-сервере, дабы минимизировать «растекание» конфиденциальных документов внутри корпоративной сети.

Пример настройки запуска сценария на перемещение показан на экране 10. Сценарий move_files.cmd:

```
xcopy%1 d:\confidential_files/X
del%1
```

В закладках Notification и Report реализованы гибкие механизмы оповещения как пользователей, так и администраторов при выполнении операций над файлами, а также при необходимости заблаговременное уведомление о планирующейся «ревизии».



Экран 10 File Management Task

Для централизованного управления используется такой инструментарий, как Data Classification Toolkit for Windows Server 2012 R2.

В заключение

Программные решения непрерывно развиваются и совершенствуются, а взятый Microsoft курс на наращивание функций безопасности, на наш взгляд, будет усиливаться. Для конечного потребителя это в первую очередь означает возможность реализовать необходимые защитные меры без дополнительных материальных затрат, и, что не менее важно, гарантировать их стопроцентную и бесшовную совместимость в корпоративных сетях, построенных на базе решений Microsoft.

Для ИТ-отделов и специалистов по информационной безопасности предложенный подход позволяет взглянуть на задачу контроля над действиями с конфиденциальными документами через призму уже известных им программных решений и, как следствие, минимизировать недопонимание на уровне технологии.

Александр Кузнецов (a.kuznetsov@ntc-vulkan.ru) — CISM, руководитель отдела безопасности информационных систем ООО «НТЦ "Вулкан"»

Андрей Брянцев (a.bryantsev@ntc-vulkan.ru) — MCDBA, MCSE: Security, ведущий инженер отдела безопасности информационных систем ООО «НТЦ "Вулкан"»