

КОМПЛЕКСНАЯ ЗАЩИТА ДЛЯ КОМПАНИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА SOPHOS SMALL BUSINESS SUITE 2.0

Компания Sophos, Plc. уже более 20 лет создает решения по защите от вирусов, спама и других типов угроз информационным ресурсам. Компания разрабатывает свои решения только для корпоративных клиентов, что дает большие преимущества в практике применения продуктов Sophos именно для защиты корпоративных сетей, так как на всех стадиях жизненного цикла ПО компании Sophos – проектирование, разработка, внедрение и сопровождение – учитываются требования надёжной защиты информационных ресурсов корпоративных пользователей.

Компания Sophos, Plc. выделяет два сегмента корпоративных пользователей – Small Business (до 100 компьютеров) и Enterprise – более 100 компьютеров, для которых предлагает две линейки своих продуктов. В данной статье речь пойдет о решениях для малого бизнеса. В настоящий момент в эту линейку входят Sophos Anti-Virus, Sophos Computer Security (антивирус и персональный сетевой экран, построенный на лицензированной технологии Outpost Firewall) и Sophos Security Suite (антивирус, персональный сетевой экран и антивирусная и антиспамовая защита для почтовых серверов MS Exchange и/или почтовых SMTP-шлюзов на платформе Windows) версии Small Business Edition 2.0.

В версии для малого бизнеса компания Sophos усилила свой фокус на удобстве использования продукта. В Sophos Security Suite 2.0 консоль управления доработана до уровня, когда для установки и администрирования системы защиты от системного администратора требуются минимальные навыки и знания. В случае простой топологии сети, решение Sophos для малого бизнеса может администрировать продвинутого пользователь.

При этом на защищаемых рабочих станциях и серверах устанавливаются такие же средства защиты, как и в версии Enterprise Edition. Таким образом, уровень защиты в версии для малого бизнеса ничем не отличается от более «тяжелой» версии корпоративных решений компании Sophos, Plc. С другой стороны уровень удобства управления в редакции Sophos Small Business существенно отличается от корпоративной версии.

Минимальные требования к квалификации администратора Sophos Security Suite для малого бизнеса следующие: базовые знания в IT, базовые знания администрирования сетей Windows, опыт работы в среде Windows (и Mac OS, если последние используются в корпоративной сети).

Идеально решение Sophos Security Suite Small Business Edition подходит для организаций, у которых от 5 до 100 пользователей, на которых используются ОС Windows 98/Me/2000/XP/Vista, Windows 2000/2003 server, Mac OS X10.2/10.3/10.4, а также есть почтовые

сервера MS Exchange и/или почтовые SMTP-шлюзы на платформе Windows.

Sophos Small Business 2.0

В 2006 году компания Sophos существенно обновила свою продуктовую линейку. Самыми крупными новинками стали: встроенный в антивирус контроль запуска нежелательных приложений (Potentially Unwanted Application, PUA), персональный сетевой экран Sophos Client Firewall, существенно улучшенная система генерации отчетов, встроенная поддержка технологии Network Admission Control (NAC) компании Cisco, централизованная удаленная полная очистка обнаруженных на защищаемых компьютерах угроз, поддержка 64-битных ОС Windows XP/2003, расширенный пользовательский карантин для PUA. Все эти изменения вошли как в линейку продуктов для крупных компаний (Enterprise Edition), так и в линейку Small Business Edition, получившую номер версии 2.0.

Инсталляция продукта проста и не требует от администратора глубоких знаний. Для установки нужно выбрать компьютер, который будет в дальнейшем выполнять функции антивирусного сервера, получать обновление с сайта Sophos (для чего нужно подключение к сети Интернет) и раздавать эти обновления компьютерам в локальной сети (для этого выделенный сервер должен быть доступен для всех компьютеров в сети). Требования к серверу следующие: Windows Server 2003, Windows 2000 Server with SP3, Windows XP Professional with SP1, 1.29 Гб свободного дискового пространства, 256 Мб оперативной памяти (минимум) и 512 Мб оперативной памяти (рекомендовано).

Сама процедура инсталляции включает в себя установку антивирусного сервера, настройку системы обновления (для этого нужна лицензия на продукт, включающая данные для настройки обновления с сайта компании Sophos), установку консоли управления Sophos Control Center 2.0, а также поиск компьютеров в сети и автоматическую централизованную установку на них средств защиты. При этом в сети из 50 компьютеров вся процедура займёт не более получаса. Также есть возможность установить дополнительную консоль управления на другой компьютер в сети (например, на рабочее место администратора системы защиты).

Основным отличием версии для малого бизнеса от корпоративной версии является список поддерживаемых операционных систем. Sophos Security Suite Small Business Edition 2.0 поддерживает только ОС Windows (кроме Windows 95 и Windows NT) и Mac OS (версии X10.2 и выше).

После установки антивирусного сервера и средств антивирусной защиты на компьютерах в сети система

полностью готова к работе. Запускаем консоль управления.

Централизованное управление защитой сети на базе Sophos Control Center 2.0

Общий вид консоли управления напоминает вид проводника Windows XP. Всё удобно и наглядно. Назначение основных панелей понятно с первого взгляда. Рассмотрим подробнее:

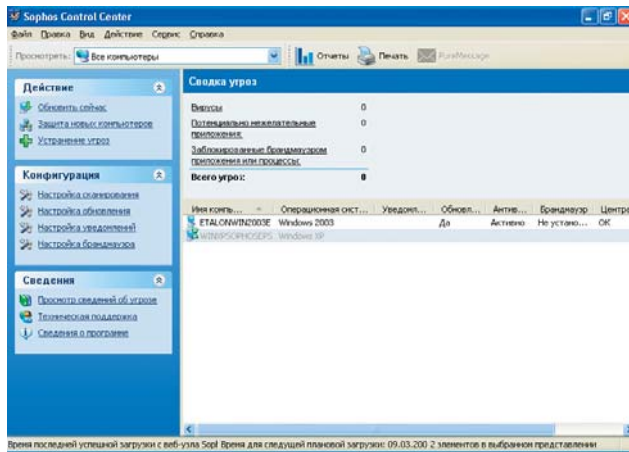


Рис. 1. Основное окно консоли управления Sophos Small Business Edition

Окно содержит самую важную информацию о текущем состоянии системы антивирусной защиты рабочих станций и серверов Windows в корпоративной сети. Основное окно содержит список компьютеров, которые обнаружены в сети, включая те компьютеры, на которые ещё не установлены компоненты Sophos Small Business Suite (антивирус и персональный сетевой экран). Список компьютеров начинается панелью, отображающей текущее состояние системы – общее количество обнаруженных вирусов/других вредоносных программ, потенциально нежелательных приложений и возникших ошибок/сбоев в работе средств защиты.

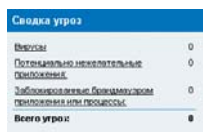


Рис. 2. Панель отображения текущего состояния системы

Компьютеры, на которых возникли какие-либо из указанных проблем, выделяются в общем списке компьютеров с использованием специальных значков:

Computer name	Operating system	Alerts	Up-to-date	Anti-virus	Firewall	Central configuration
GOMER	Windows 2000 Server		Yes	Active	Not installed	OK
VIGOUR	Windows 2000	🚨 Virus detected	Yes	Active	Not installed	🚩 Changed
RAGED	Windows XP	🚨 Error	Yes	Active	Active	OK

Рис. 3. Пример выделения компьютеров в консоли управления

В нижней части окна консоли приводится информация о времени обновления системы: когда было получено последнее обновление с сайта Sophos и когда в следующий раз будет проведен сеанс обновления.

В целом, достаточно нескольких секунд, чтобы получить полную и содержательную информацию о текущем состоянии системы. Таким образом, адми-

нистрирование системы защиты Sophos Security Suite с помощью консоли управления Sophos Control Center 2.0 требует минимального времени и экономит время системного администратора (или другого сотрудника, отвечающего за информационную безопасность). Если же учесть, что большинство операций по лечению вирусов и других вредоносных программ, по обновлению системы антивирусной защиты, по предупреждению использования нежелательного ПО автоматизированы, то в результате применения системы Sophos Security Suite Small Business Edition у системного администратора высвобождается значительное количество рабочего времени, которое он может потратить на выполнение других задач.

Система генерации отчетов

Отдельного внимания заслуживает система генерации отчетов. В новой версии консоли управления Sophos Control Center 2.0, вышедшей в октябре 2006 года, эта система была существенно улучшена. Текущая версия системы генерации отчетов с помощью удобного интерфейса позволяет генерировать сложные отчеты по всем аспектам работы системы защиты.

В отчёте гибко настраиваются фильтры по отчётному периоду, группе компьютеров и типу событий. Отчет можно получить в виде таблицы или в виде диаграммы (круговой или в виде гистограммы):

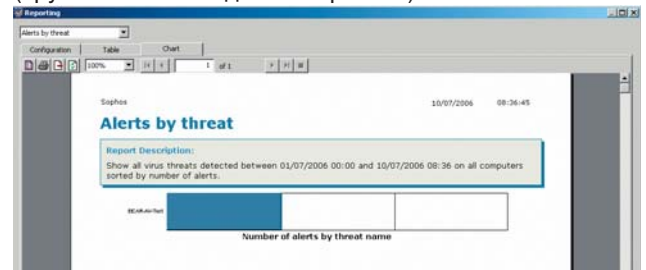


Рис. 4. Пример отчета

Кроме этого, в системе есть очень интересная возможность – автоматическая генерация отчета и отправка его по электронной почте с заданной периодичностью. Этот сервис можно настроить в окне настройки уведомлений на закладке «Reporting».

В целом, система управления настройками средств антивирусной защиты сделана по тем же принципам – максимальная простота и удобство – что и основная часть интерфейса консоли управления.

Русская версия Sophos Small Business

Новая версия системы защиты от вирусов, спама, хакерских вторжений Sophos Security Suite для малого бизнеса вышла 11 октября 2006 года. А уже 18 ноября 2006 года при активном участии ЗАО «ДиалогНаука» вышла русская версия этой системы, в которой на русский язык были переведены инсталлятор, документация, встроенная система помощи и интерфейс консоли управления Sophos Control Center 2.0.

Также ЗАО «ДиалогНаука» является техническим центром компании Sophos, Plc в России и оказывает поддержку своим пользователям на русском языке.