

## **Безопасность и контроль: интеллектуальный подход к обеспечению соответствия стандартам и защиты от вредоносного ПО**

Непрерывающееся развитие угроз вредоносного программного обеспечения, в сочетании с необходимостью обеспечения большей гибкости применяемых на практике решений, ставят сложные задачи перед ИТ отделами компаний, которые стремятся снизить нагрузку на службу технической поддержки и повысить отдачу от своих инвестиций в безопасность. В данном документе рассматриваются основные преимущества комплексного, основанного на применении политик, подхода к обеспечению безопасности сети на всех уровнях, а также управлению доступом и действиями пользователей.

## Безопасность и контроль: интеллектуальный подход к обеспечению соответствия стандартам и защиты от вредоносного ПО

### Новые вызовы системам безопасности

От отделов информационных технологий всегда требуют снижения затрат за счет уменьшения нагрузки на службу технической поддержки и обеспечения максимальной рентабельности инвестиций в обеспечение защиты и управления сетью. В то же время, компании и частные лица ожидают большей гибкости применяемых на практике решений – от обеспечения мобильных и удаленных соединений до предоставления веб-доступа и функций мгновенного обмена сообщениями (IM). Однако в настоящее время равновесие между производительностью и безопасностью сетей, по всей видимости, нарушено. Необходимость повышения эффективности деятельности компаний приводит к все большей открытости сетей, что в свою очередь ставит под угрозу их безопасность.

Таким образом, основной задачей отдела информационных технологий является обеспечение достаточной гибкости информационной системы компании в условиях быстро изменяющегося окружения. К внешним факторам, оказывающим влияние на информационную систему компании, можно отнести значительное увеличение числа узконаправленных угроз и все возрастающую строгость требований к обеспечению соответствия законам и стандартам аудита. Среди внутренних факторов можно выделить увеличение затрат на работу службы технической поддержки, а также все большую неоднородность сетей, в которых задействовано несколько уровней безопасности, различные операционные системы и типы устройств.

Затраты на внедрение антивирусных решений и решений по защите от спама составляют значительную долю ИТ бюджета и ресурсов компании. В частности, это касается устранения неполадок и проблем, связанных с внедрением некоторых таких решений. Максимальная защита и повышение рентабельности достигается не только за счет управления очевидными угрозами, связанными с вредоносным ПО и нежелательными сообщениями. Важная роль в этом процессе отводится управлению доступом пользователей к сети – управлению порядком подключения, используемыми компьютерами и системами безопасности, выполняемыми приложениями.

### Эволюция угроз вредоносного ПО

Отсутствие контроля над действиями пользователей – лишь одна из нескольких существующих проблем. Основная проблема, связанная с быстрым развитием вредоносного ПО, заключается в том, что подобное ПО становится все более быстродействующим, сложным и узконаправленным. Как никогда ранее, сегодня важно обеспечить многоуровневую защиту информационной системы компании от шлюза до любой конечной точки, включая все точки доступа. На рис. 1 приведены обобщенные данные по новым образцам вредоносного ПО, обнаруженных компаниями Sophos в 2006 году. Всего было зафиксировано около 40000 новых кодов. Пик активности пришелся на ноябрь месяц (более 7600 случаев), что практически в 4 раза превышает аналогичный показатель за ноябрь 2005 года. Данный всплеск связан с появлением нового семейства сетевых червей Stratio, распространяемых путем массовой почтовой рассылки и насчитывающих несколько тысяч разновидностей с целью затруднить их обнаружение. Хотя данное значение является пиковым, отчетливо просматривается общая тенденция увеличения числа атак.

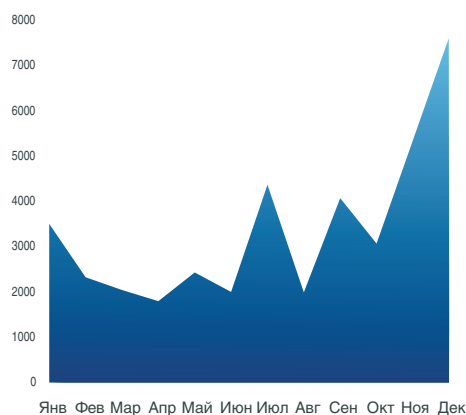


Рис. 1. Число атак нового вредоносного ПО в 2006 г.

## Угрозы, исходящие из всемирной сети

Большинство администраторов считают сеть интернет наибольшей угрозой безопасности и производительности для своих информационных систем.<sup>1</sup> Некоторые веб-узлы могут не только содержать очевидно нежелательное содержимое, но и скрывать в себе шпионское и рекламное ПО. За последнее время произошел резкий рост числа размещаемых на веб-узлах программ загрузки, содержащих шпионское ПО. На рис. 2 показано процентное соотношение между сообщениями электронной почты, содержащими шпионское ПО, и сообщениями, в которых есть ссылки на веб-узлы, с которых может быть загружено шпионское ПО. Данные исследования свидетельствуют о явном увеличении доли вредоносного ПО загрузки, произошедшем в 2006 году.

Согласно данным исследования, около 20% времени, проводимого сотрудниками компаний в интернете, приходится на использование ресурсов в личных или развлекательных целях.<sup>2</sup> Это существенно повышает риск непреднамеренной загрузки вредоносного ПО, в особенности шпионского ПО или троянских программ-загрузчиков. Неконтролируемый просмотр интернет-страниц и передача личных данных по сети с использованием ресурсов компании играют на руку спамерам и авторам вредоносного кода. Подобные действия подвергают адреса электронной почты компании опасности сетевых мошенничеств, включая спам, сбор информации о действующих адресах электронной почты – харвестинг, а также и фишинг. По данным исследований SophosLabs в 2006 году, более 75% всех фишинговых сообщений электронной почты было нацелено против пользователей систем электронной торговли PayPal или eBay.<sup>3</sup>

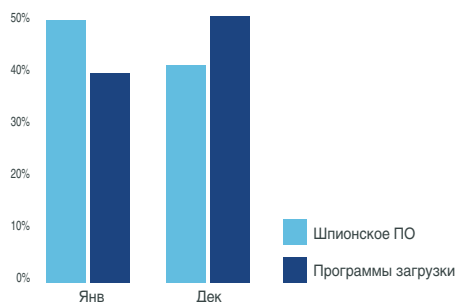


Рис. 2. Шпионское ПО и программы загрузки в 2006 г.

Эффективное решение по обеспечению интернет-безопасности для современной компании должно предусматривать не просто защиту от всех видов вредоносного ПО, но и определение и удаление потенциально нежелательных приложений (PUA), а

также автоматическое предотвращение несанкционированного просмотра интернет-страниц путем управления доступом к заранее известным ненадежным веб-узлам. Подобные решения должны дополняться средствами постоянного анализа интернет-трафика по всему миру в целях определения категорий веб-сайтов, анализа вредоносного кода и поведения различных интернет-страниц.

## Угрозы со стороны электронной почты

Важную роль играет обеспечение постоянной защиты в компании системы обмена электронными сообщениями. Для этого необходимо обеспечить защиту шлюзов электронной почты, серверов коллективного пользования и баз данных сообщений (например, Lotus Domino или Microsoft Exchange) от угроз, содержащихся в сообщениях электронной почты. Вредоносное ПО маскируется и распространяется все более изощренными способами. Наблюдается все меньше случаев простого включения вредоносного кода во вложения электронной почты (1 из 337 сообщений в 2006 году по сравнению с 1 из 44 сообщений в 2005 году).

На сегодняшний день многие нежелательные сообщения содержат вложенные изображения, что увеличивает вероятность их прочтения конечными пользователями и снижает эффективность тех спам-фильтров, которые в основном анализируют текстовое содержимое. Данные сообщения большого размера засоряют почтовые ящики и могут содержать ссылки на веб-узлы, содержащие вредоносные коды. Так, нежелательные сообщения, распространение которых велось в ноябре 2006 года, предлагали бесплатный просмотр изображений и видеоклипов откровенного характера, а в действительности через веб-ссылку перенаправляли на троянскую программу Psyme-DL, которая могла перехватить управление компьютером пользователя. Современные спам-сообщения могут видоизменяться, чтобы избежать обнаружения, и распространяться через зомби-сети, состоящие из инфицированных вредоносным ПО компьютеров, практически без лишних затрат и риска блокировки IP-адресов.

Действительно эффективная защита обеспечивается решениями, поддерживающими возможность определения не только отдельных экземпляров нежелательных сообщений или вирусов, но также спам-кампаний и семейств вредоносного ПО в целом. Подобные решения должны предусматривать возможность применения политик, соответствующих запросам различных групп пользователей, а также обеспечения соответствия требованиям стандартов.

## Угрозы оконечным компьютерам

По-прежнему важную роль играет обеспечение защиты от вредоносного ПО, попыток взлома и нежелательных приложений на уровне оконечных рабочих станций. В качестве примера можно привести три масштабные атаки с применением распространяемых по электронной почте сетевых червей, доля которых составила около 40% от всех зафиксированных в ноябре 2006 года атак. Используемые в них вирусы Stratio-Zip, Netsky-D и MyDoom-O успешно атаковали также и компьютеры с операционной системой Windows Vista. Однако теперь больше нет необходимости управлять множеством продуктов для защиты от различных угроз. Современные продукты по обеспечению безопасности в конечных точках сети предусматривают не просто защиту от шпионского ПО, вирусов, троянских программ, сетевых червей и потенциально опасных приложений. В настоящее время уже применяются политики под управлением одной центральной станции сети, что обеспечивает защиту от несанкционированного доступа за счет использования персонального межсетевого экрана. Это позволяет заблокировать вредоносную программу до ее выполнения (система предотвращения локальных вторжений – HIPS) и контролировать доступ к неразрешенным приложениям.

*Реализация политик безопасности общего назначения в конечных точках сети сама по себе является важным средством защиты от сетевых червей и смешанных атак, представляющих на данный момент одну из наиболее существенных проблем безопасности в корпоративных информационных системах.*

*Скотт Кроуфорд (Scott Crawford),  
Enterprise Management Associates<sup>4</sup>*

## Неразрешенные приложения

Несмотря на преимущества для бизнеса и производительности, которые предоставляют приложения передачи голосового трафика по IP-сетям (VoIP) или приложения обмена мгновенными сообщениями (IM), их несоответствующее использование может привести к возникновению достаточно серьезных проблем. Приложения VoIP, обеспечивающие средства IP-телефонии, а также проекты распределенной обработки данных (например, проект по поиску внеземных цивилизаций SETI@Home) используют дополнительные ресурсы информационной системы компании, снижая тем самым скорость работы сети. Игры и обмен файлами по одноранговому сетям (P2P) также могут быть причиной проблем с вполне законными корпоративными приложениями, что негативно сказывается на производительности сотрудников и информационной системы компании в целом.

## Новые угрозы

В настоящее время возникают новые угрозы безопасности информационных систем, например, запугивающее ПО или вредоносное ПО для мобильных устройств. Запугивающее ПО предоставляет пользователю ПК ложную информацию о заражении или наличии другой проблемы безопасности на его компьютере, предлагая приобрести «полнофункциональную» версию соответствующего защитной программы. Вредоносное ПО для мобильных устройств, поражающее карманные компьютеры и смартфоны, пока представляет собой относительно небольшую проблему по сравнению с числом вредоносных программ, поражающих компьютеры под управлением Windows. Однако данная проблема постепенно становится все более реальной, вынуждая компании готовить эффективные решения по обеспечению безопасности мобильных устройств.

## Контроль над действиями пользователя

Удаленные пользователи и пользователи с правами гостя, осуществляющие подключение к сети с использованием устройств, не отвечающих требованиям политики безопасности компании в области разрешенных приложений, антивирусного ПО и обновления операционных систем, могут поставить под угрозу безопасность информационной системы компании. Угроза безопасности значительно возрастает, если сотрудники подключаются к сети с использованием технологий беспроводного доступа, карманных компьютеров или карт памяти. Деловые партнеры также могут поставить под угрозу безопасность информационной системы компании, если они подключаются к сети с использованием устройств, не соответствующих требованиям корпоративной политики безопасности, на которых могут выполняться неразрешенные приложения, загружаться файлы из интернета (все это, возможно, происходит без соответствующего контроля).

Усовершенствование технологий, используемых различными пользователями для оптимизации производительности, вынуждает компании предпринимать действия по минимизации негативного влияния, которое данные технологии оказывают на безопасность сетей и информационные ресурсы. Это достигается за счет применения политик, управляющих не только доступом пользователей к различным сегментам сети, но и, собственно, самими действиями, доступными данным пользователям при подключении.

## Управление доступом к сети

По мнению аналитиков, внедрение систем управления доступом к сети (NAC) играет важную роль для снижения рисков, связанных с ростом объемов использования мобильных технологий, а также в обеспечении соответствия требованиям законода-

“*Системы управления доступом к сети являются важнейшим средством управления сетью. Неприменение подобных систем равносильно открытым нараспашку дверям в сеть.*”

Лоуренс Орэнс (Lawrence Orans), Gartner Inc<sup>5</sup>

тельства. Реальная система управления доступом к сети (NAC) предусматривает ведение отчетности по состоянию соответствия компьютеров сети принятым стандартам, а также применение политик управ-

ления доступом на различных уровнях. Применение систем управления доступом к сети (NAC) также позволяет компании в полной мере реализовать обозначенную в руководящих документах компании политику безопасности. Реализация политик для различных групп пользователей на достаточно структурированном уровне позволяет обеспечить автоматическую защиту всех точек сети без снижения производительности и увеличения нагрузки на службу технической поддержки.

Более того, применение ПО, сохраняющего и использующего существующие решения по безопасности на разных уровнях сети, позволит не только сохранить информационную инфраструктуру компании, но и повысить эффективность и рентабельность инвестиций в безопасность. На рис. 3 показаны основные преимущества применения комплексных политик, единой системы мониторинга и управления действиями пользователей и безопасностью.



Рис. 3. Комплексная безопасность и контроль

## Заключение

Стандартные средства безопасности (например, антивирусное ПО и системы веб-блокировки) обеспечивают защиту от индивидуальных источников опасности, но не предусматривают защиту от подключения к сети неизвестных или не соответствующих принятым стандартам устройств. По мере увеличения открытости сетей и возникновения все новых угроз, решения по управлению доступом и действиями пользователей приобретают все более важную роль по сравнению с простым определением и блокировкой угроз.

Максимальная рентабельность инвестиций в безопасность и контроль может быть достигнута за счет внедрения основанных на приме-

нении политик решений, которые обеспечивают дружелюбный, комплексный и автоматизированный подход к обеспечению защиты от угроз и несоответствующего применяемым стандартам поведения за счет использования единого агента и единой системы управления и контроля. Стандартом управления защитой для компаний любых размеров становится применение средств управления приложениями, доступом к сети и доступом к интернету, что позволяет значительно снизить деловые риски и повысить эффективность работы информационной системы и снижения общих затрат. ◆

---

## Решения Sophos

Решения компании Sophos обеспечивают защиту информационной системы компании на всех уровнях – от шлюза до любой конечной точки сети.

Решение по обеспечению безопасности в конечных точках **Sophos Endpoint Security** обеспечивает комплексную защиту от вирусов, шпионского и рекламного ПО, потенциально опасных приложений, попыток вторжения, а также использования неразрешенных приложений с управлением на базе одной центральной станции. Также обеспечивается защита от вирусов и шпионского кода для мобильных устройств Windows.

Система управления доступом к сети **Sophos NAC** блокирует доступ неправомерных пользователей, управляет гостевым доступом и обеспечивает соответствие легальных пользователей политике безопасности компании, – администратор сети всегда знает кто и что подключается к сети.

Решение по обеспечению безопасности для шлюзов **Sophos gateway security** объединяет в себе средства антивирусной защиты, защиты от спама и применения политик для шлюза электронной почты, с возможностью выбора гибкого, масштабируемого ПО и управляемых программно-аппаратных устройств для работы с электронной почтой. Интернет-устройства компании Sophos обеспечивают защиту интернет-шлюзов от вредоносного ПО и нежелательного содержимого, гарантируя безопасный и эффективный просмотр интернет-страниц.

**SophosLabs™** – это глобальная сеть аналитических центров по исследованию угроз безопасности, в которой осуществляется круглосуточный анализ трафика сети интернет и электронной почты в целях обеспечения защиты от известных и новых угроз по всему миру, независимо от места их происхождения.

**Для получения дополнительной информации о продуктах компании Sophos (в том числе, локализованных на русский язык) посетите веб-узел компании «ДиалогНаука» ([www.DialogNauka.ru](http://www.DialogNauka.ru)) – партнера компании Sophos в России.**

## Ссылки

- 1 Security threat report 2007. Sophos.  
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001174051938.txt>
- 2 Burstek releases 2005 internet usage study.  
[www.findarticles.com/p/articles/mi\\_m0EIN/is\\_2006\\_March\\_20/ai\\_n16109780](http://www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780)
- 3 [www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html](http://www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html)
- 4 Скотт Кроуфорд (Scott Crawford), старший аналитик компании Enterprise Management Associates, 2007 г.
- 5 Лоуренс Орэнс (Lawrence Orans), руководитель отдела исследований компании Gartner Inc

## См. также:

Instant Messaging, VoIP, P2P and games in the workplace: how to take back control  
Sophos white paper. February 2007.  
<http://www.sophos.com/security/whitepapers/sophos-app-control-wpus>

Maximizing security and performance for web browsing: the challenge for SMBs  
Sophos white paper. October 2006.  
<http://www.sophos.com/security/whitepapers/sophos-web-security-wpus>

## О компании Sophos

Компания Sophos является мировым лидером в области обеспечения безопасности и контроля в сфере информационных технологий. Компания предлагает комплексные решения по обеспечению безопасности для коммерческих, образовательных и правительственных организаций. Решения компании позволяют обеспечить защиту от известного и нового вредоносного и шпионского ПО, вторжений, опасных приложений, нежелательных сообщений, нарушения политик безопасности, а также всестороннее управление доступом к сети (НАС). Надежные и простые в эксплуатации продукты Sophos применяют для своей защиты более 100 миллионов пользователей более чем в 150 странах. Более чем 20-летний опыт работы и наличие глобальной сети аналитических центров позволяют компании мгновенно реагировать на любые возникающие угрозы и обеспечить полное удовлетворение потребностей заказчиков. Sophos – это глобальная компания со штаб-квартирами в Бостоне (Массачусетс, США) и Оксфорде (Великобритания).

Бостон, США • Майнц, Германия • Милан, Италия • Оксфорд, Великобритания • Париж, Франция

Сингапур • Сидней, Австралия • Ванкувер, Канада • Иокогама, Япония

© Copyright 2007. Sophos Plc.

All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

**SOPHOS**  
WWW.SOPHOS.COM