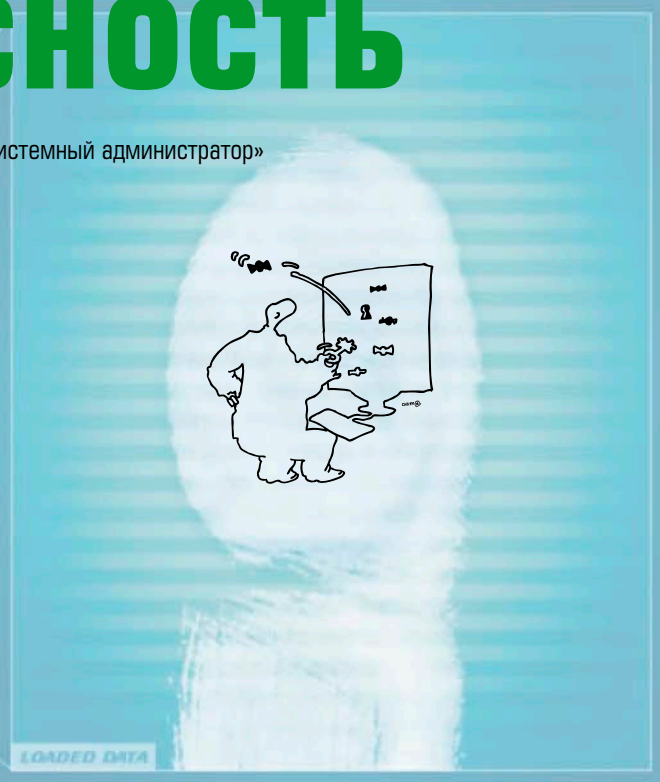
№5 июнь 2011

Безопасность

Спецвыпуск-приложение к ежемесячному журналу «Системный администратор»



Щит и меч
Основные проблемы ИТ-безопасности

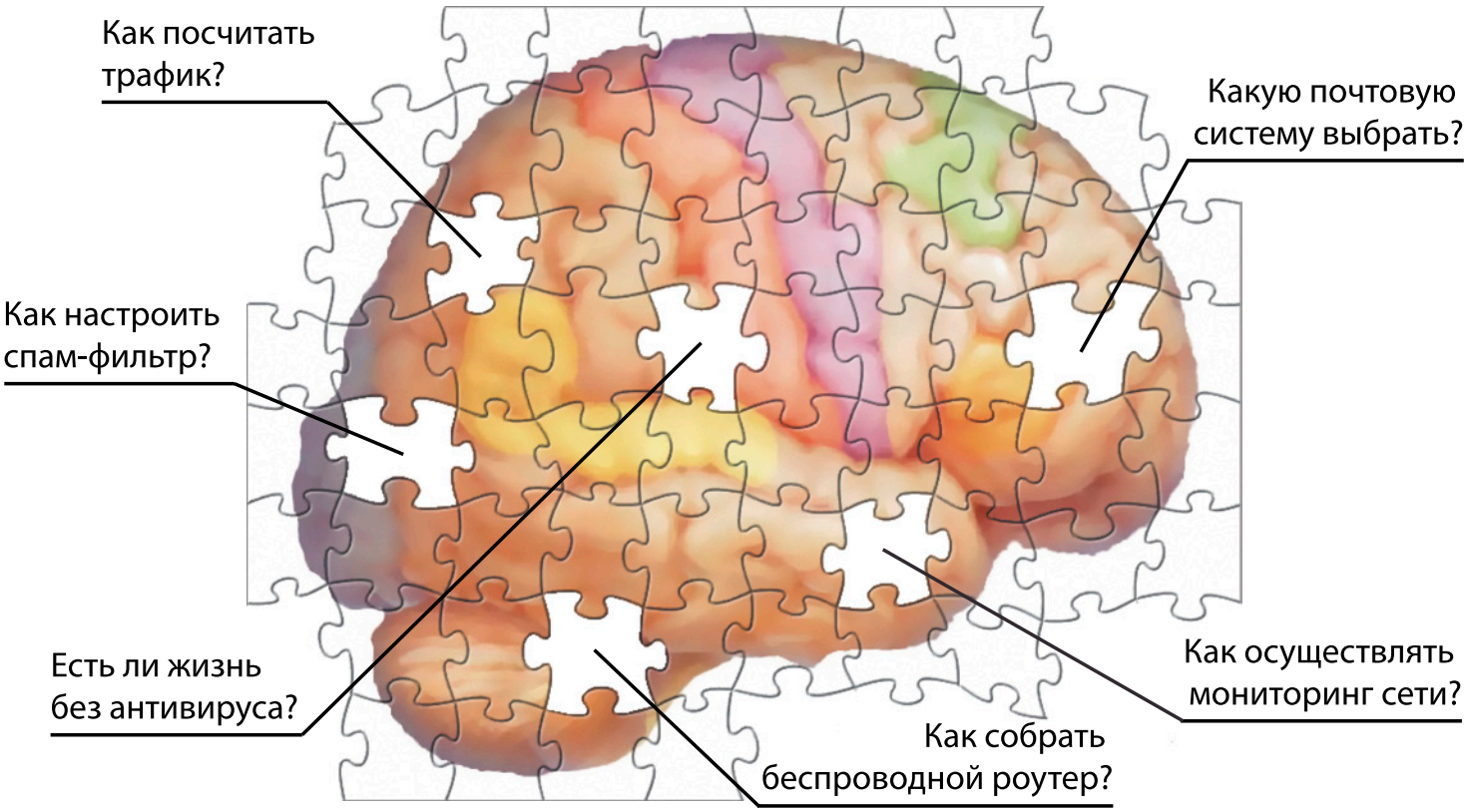
Что умеют DLP?
Современные технологии защиты от утечек

Внедрение служб
управления правами

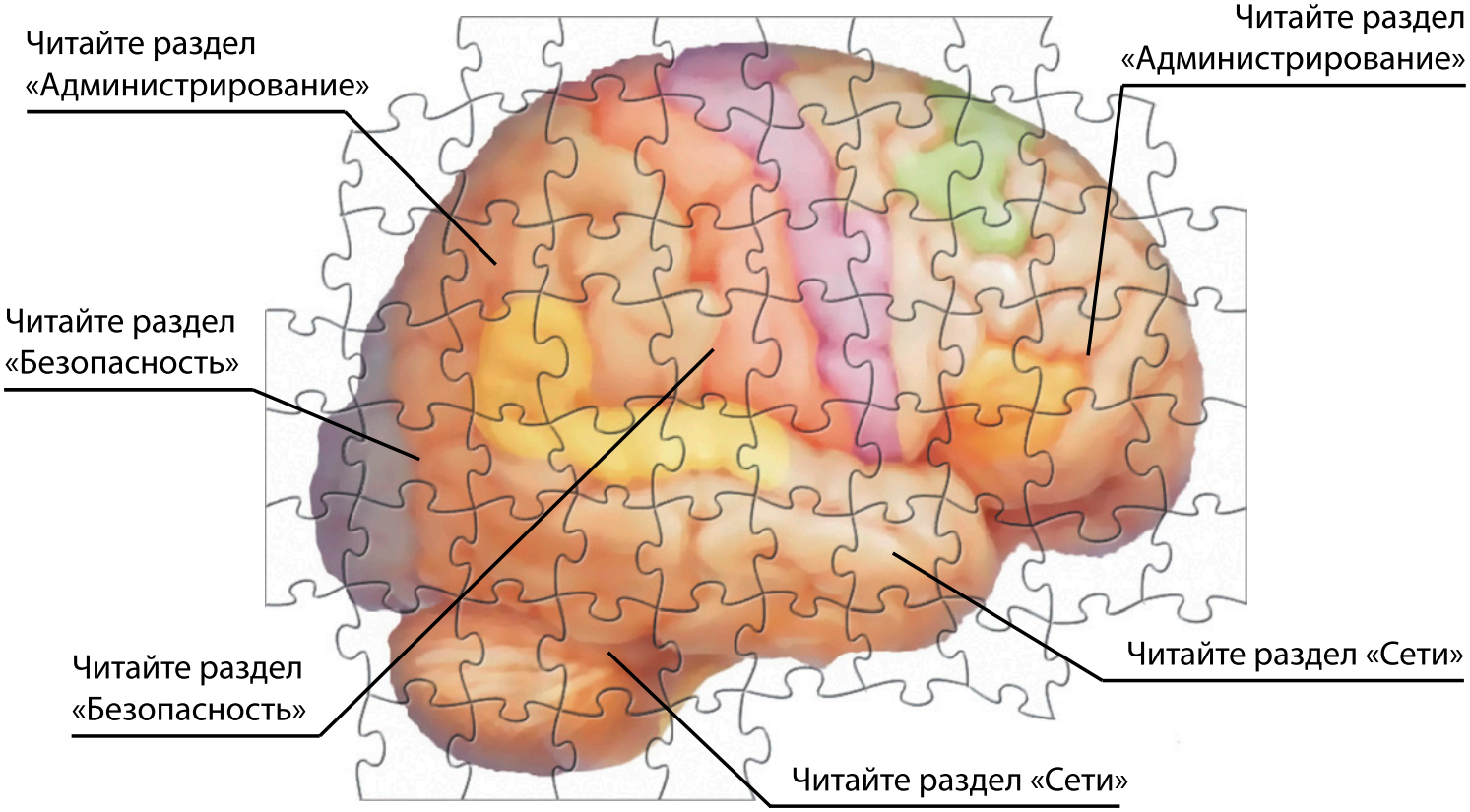
Принцип неуязвимости
Чем руководствуются компании США

Системный администратор

Какими мыслями занят ИТ-специалист, который не читает свой журнал?



Остальные ИТ-специалисты знают, где искать ответы на вопросы!



Системный администратор

Издается с 2002 года

Генеральный директор
Владимир Положевец
Главный редактор
Галина Положевец, chief@samag.ru
Исполнительный директор
Владимир Лукин, maker@samag.ru

Ведущий рубрики
«Сетевая безопасность»
Александр Емельянов

Главный бухгалтер
Надежда Кан, buch@samag.ru
Главный редактор электронного приложения «Open Source»
Дмитрий Шурупов, osa@samag.ru

Отдел маркетинга и рекламы
Руководитель отдела
Полина Гвоздь, pr@samag.ru, тел.: (495) 687-93-57
Менеджеры по рекламе
Дарья Зуморина, reklama@samag.ru, (495) 687-93-57
Анастасия Гуркина, gurkina@samag.ru, (495) 640-43-13
Распространение
Сергей Ростомов, subscribe@samag.ru, (495) 687-93-57

Дизайн-макет
Марина Рязанцева, Дмитрий Бессонов
Дизайн обложки
Марина Рязанцева
Иллюстрация
Виктор Чумачев

Экспертный совет
Рашид Ачилов
администратор телекоммуникационных систем
Алексей Барабанов
эксперт по вопросам применения информационных технологий
Алексей Бережной
эксперт по администрированию и безопасности
Андрей Бирюков
ведущий системный инженер по информационной безопасности
Александр Емельянов
эксперт по администрированию и безопасности Windows-систем
Иван Коробко
эксперт по автоматизации процессов в Windows-доменах
Валентин Синицын
к. ф.-м. н., инженер-программист, доцент Уральского государственного университета
Кирилл Сухов
ведущий специалист направления интернет-разработки
Сергей Яремчук
эксперт по информационной безопасности

Издатель
ООО «Синдикат 13»

Адрес редакции
129626, г. Москва, проспект Мира, д. 102, корп. 1,
тел.: (495) 687-93-57, тел./факс: (495) 640-43-13
Сайт журнала: www.samag.ru

Отпечатано в типографии
ООО «Периодика»
Тираж 17000 экз.

Ищите сисадмина

Чтобы найти ответ на вопрос, от чего зависит конечная реализация систем защиты, на сайте журнала «Системный администратор» был проведен опрос «Что является основой ИТ-безопасности в компании?».

Результаты его распределились в следующем порядке:

- Хороший сисадмин – 18,31%.
- Управление доступом, распределение ролей и ответственности – 13,15%.
- Хороший антивирус – 12,21%.
- Блокировка интернет-ресурсов (веб, ICQ и т.д.) и фильтрация трафика – 12,21%.
- Хороший межсетевой экран – 10,33%.
- Лицензионный софт – 8,45%.
- Наличие инструкций – 6,1%.
- Отбор сотрудников, подготовка и контроль в процессе работы – 4,69%.
- Аудит, анализ рисков – 4,23%.
- Наличие службы ИБ и системы менеджмента ИБ – 3,29%.

Как и ожидалось, наибольшее количество баллов набрал ответ «Хороший системный администратор», который по результатам опроса является «основой» ИТ-безопасности в компании. Приятно, когда так доверяют человеку твоей профессии. Но современная ситуация требует внедрения самых различных инструментов, гибкого подхода в каждом конкретном случае, умения взглянуть на свою сеть глазами хакера и быстро реагировать на изменение ситуации. Помня, что информация – это все, руководство организации, возложив на одного человека такую задачу, должно всячески ему помогать и контролировать.

Вполне логично выглядит и второе место в опросе, которое выбрали 13,15% ответивших, – «Управление доступом, распределение ролей и ответственности». Каждый должен заниматься своей работой, за которую взялся, и иметь доступ только к «своей» части информации. Это база для построения системы безопасности в любой организации.

Среди рисков вирусы занимают первое место. Остановить заразу может только хороший антивирус плюс блокировка интернет-ресурсов (веб, ICQ) и фильтрация трафика. Кроме этого, следует прикрыть сетевые порты брандмауэром. Эти мероприятия относятся к обязательным и выполняются в первую очередь.

По результатам опроса соответствующие пункты составляют основу безопасности и заняли третье и четвертое места.

Лицензионный софт отметили 8,45% опрошенных. С точки зрения ИБ наличие лицензии означает спокойствие. Если нагрянут проверяющие органы, эта поддержка поможет быстро решить возникшую проблему, но, главное, дает возможность своевременного обновления ОС и программ.

А вот за необходимость контроля в первую очередь сменных устройств проголосовали 7,04%. Как показывает статистика, вирусы, распространяющиеся через сменные носители, никуда не делись и до сих пор присутствуют в ТОП10. Бесконтрольность в этом вопросе может стоить занесенного в систему троянца, а значит, и до утечки данных недалеко. Кроме этого, сменные носители могут быть использованы для кражи конфиденциальных данных, что нельзя допустить ни в коем случае.

На седьмом и восьмом местах – мероприятия подготовительного и образовательного порядка. Ведь безопасность начинается с момента приема человека на работу, его инструктажа, обучения и понимания возможной ответственности.

Привлекать специалистов по ИБ, которые могут провести полноценный аудит и оценить риски, очевидно, у нас еще не очень любят, или просто пока этого не требует бизнес. Видимо, поэтому аудит и анализ рисков, а также наличие службы ИБ заняли последние места. Хотя в западной компании без такой проверки бизнес не может считаться доверенным (читайте статью Константина Кондакова).

Сергей Яремчук, технический редактор журнала, автор концепции приложения «Безопасность»