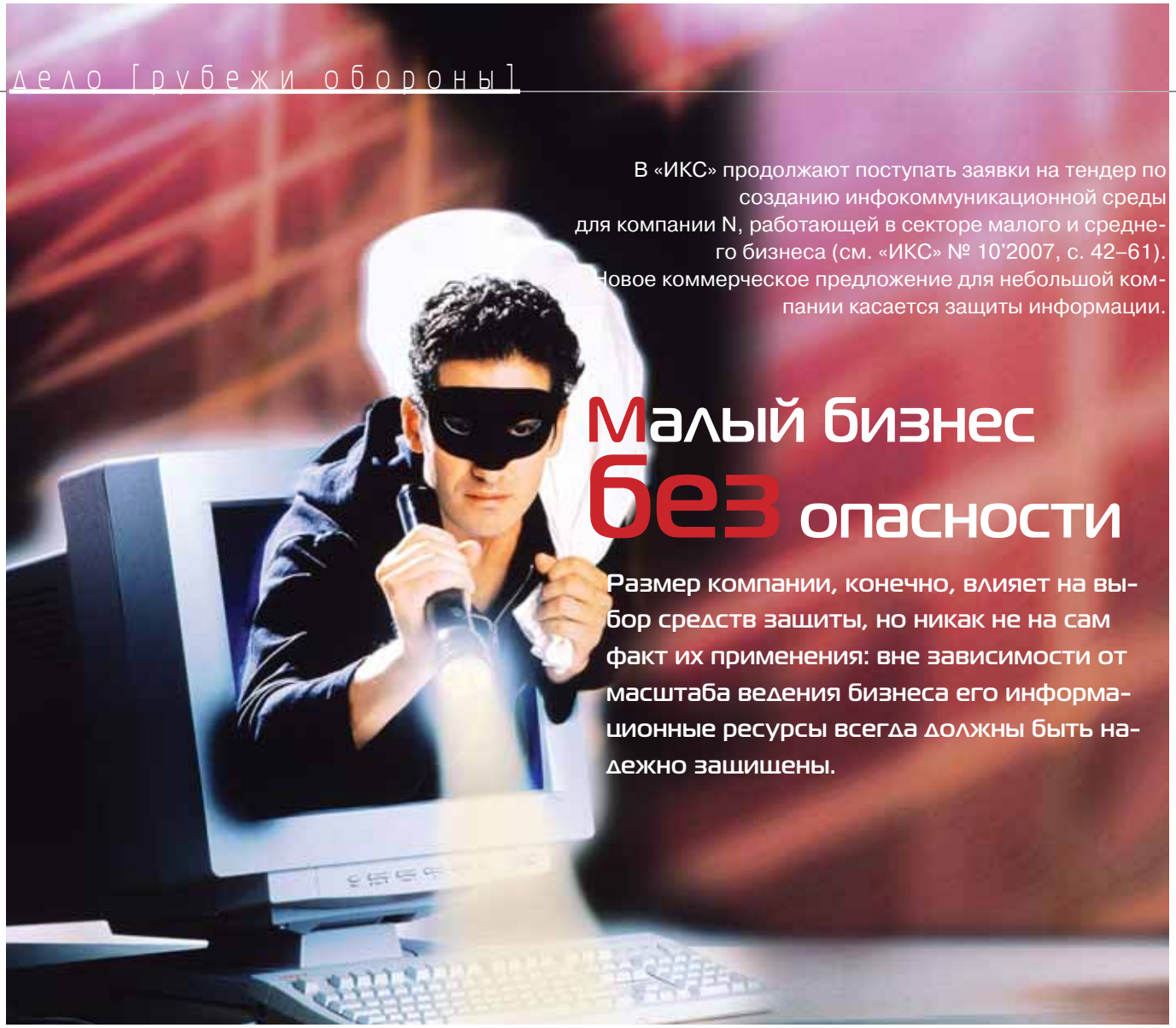

В «ИКС» продолжают поступать заявки на тендер по созданию инфокоммуникационной среды для компании N, работающей в секторе малого и среднего бизнеса (см. «ИКС» № 10'2007, с. 42–61). Новое коммерческое предложение для небольшой компании касается защиты информации.

Малый бизнес без опасности

Размер компании, конечно, влияет на выбор средств защиты, но никак не на сам факт их применения: вне зависимости от масштаба ведения бизнеса его информационные ресурсы всегда должны быть надежно защищены.

Алексей КОМАРОВ,
менеджер по работе с заказчиками компании Aladdin

Компьютерные сети и системы сегмента SMB (small & medium business) имеют свои особенности, которые необходимо учесть при выборе средства защиты. Например, небольшие компании редко приобретают дорогостоящие системы обнаружения вторжения или мониторинга действий пользователей в режиме реального времени. Понятно, что стоимость системы не должна превышать стоимость данных, для защиты которых она применяется. Однако при проектировании системы информационной безопасности (ИБ) нужно помнить и о тех средствах защиты, которые могут понадобиться в перспективе.

Анализ рисков и угроз

Для абсолютного большинства SMB-компаний важной составляющей их коммерческой тайны является информация о клиентах. Как показывает практика, именно эти данные нуждаются в максимально надежной защите, поскольку кража сведений о заказчиках (а такие ситуации, к сожалению, нередки) наносит серьезный ущерб бизнесу.

Для связи между удаленными офисами и складами обычно используются открытые каналы передачи данных (Интернет). Информация о заказах, поступивших оплатах и другая внутрикорпоративная переписка в большей или меньшей степени носит конфиденциальный характер и требует соответствующей защиты.

Разнесенная географическая структура и наличие в компании мобильных сотрудников предполагают широкое использование ноутбуков. Три четверти случаев утечки или потери конфиденциальных данных связаны с человеческим фактором – умышленными или ошибочными действиями сотрудников компании. При этом 50% приходится на ошибку и еще 25% – на умышленные действия. По данным IT Policy Compliance Group, за прошедший год в 20% компаний зафиксировано более двух десятков подобных прецедентов.

Речь идет, как правило, об уничтожении или краже финансовой, клиентской информации или данных о сотрудниках.

Если компания имеет сеть филиалов и в перспективе планирует связать их единой сетью, то очевидно, что все используемые платформы и решения должны быть совместимы. Обслуживание ИТ-парка, доверенное аутсорсеру, подвергает информационные ресурсы дополнительному риску неавторизованного доступа посторонних лиц. В небольшой компании имеется ИТ-бюджет, но выделенной статьи расходов на ИБ, скорее всего, нет. Годовой оборот позволяет рассчитывать на разовое выделение бюджета в размере не более 0,5–1% от него. Стоимость ежегодного обслуживания желательно свести к минимуму.

Основными рисками для компаний SMB является утечка конфиденциальной информации по причине:

- несанкционированного доступа злоумышленников к компьютерам организации – при получении физического доступа к серверам, при краже или утрате мобильных компьютеров и носителей информации;
- работы в открытых каналах связи – при использовании электронной почты, при удаленном доступе к информационным ресурсам;
- неавторизованного доступа пользователей – при передаче друг другу паролей, при использовании недостаточно стойких паролей и их подборе злоумышленником.

Итак, риски велики, наиболее вероятные угрозы ясны, притом что ИБ-бюджет у таких компаний, как правило, ограничен.

Минимизация угроз

Персонализированный доступ к данным и шифрование почты. В основе любой современной комплексной системы обеспечения ИБ лежит разделение прав доступа. До последнего времени самым доступным способом аутентификации пользователей были пароли. Привычка пользователей использовать простые пароли и прямо противоположное требование политики ИБ либо значительно ослабляют уровень защищенности, либо усложняют работу пользователей и заметно снижают производительность труда, в том числе из-за частых проблем, связанных с забытыми/заблокированными паролями.

Отличная альтернатива паролям – смарт-карты и USB-ключи (токены). Чтобы пройти процедуру аутентификации, пользователь должен подключить к компьютеру токен и ввести правильный пин-код от него. Аппаратное ограничение количества неправильных попыток ввода пин-кода существенно повышает уровень безопасности.

Пропажу токена легко обнаружить. Кроме того, сам факт персонифицированного доступа дисциплинирует пользователей: передача своего токена коллеге психологически воспринимается им как более тяжкое нарушение, чем, например, сообщение по телефону пароля.

Использование аппаратных средств аутентификации выгоднее и с финансовой точки зрения. Стоимость такого решения обычно не превышает 1400–1450 руб. на одного пользователя (например, PRO/32 кбайт стоит 1390 руб.). Для аутентификации пользователей при входе в домен/ОС Windows по цифровым сертификатам X.509, хранящимся на токенах, достаточно использовать штатные средства самой ОС Windows – кроме самих токенов ничего дополнительно приобретать не нужно.

В этом случае при наличии домена Windows автоматически появляется возможность использовать токены и для обмена зашифрованными почтовыми сообщениями, ЭЦП почтовых сообщений и офисных документов, построения защищенных VPN-соединений, удаленных RDP-подключений и т.д.

В отдельных случаях для ускорения процесса внедрения можно использовать продукты класса Windows Logon, которые сохраняют логины и пароли в памяти токена. В данном случае стандартный компонент операционной системы – Gina (запрашивающий при входе в ОС логин и пароль пользователя) от Microsoft подменяется Windows Logon, который после подключения токена и ввода правильного пин-кода от него считывает из его закрытой области памяти логин и пароль пользователя и «пробрасывает» их операционной системе. Такое решение менее надежно, но значительно проще во внедрении, поскольку не требует наличия сервера.

Три четверти случаев утечки или потери конфиденциальных данных связаны с человеческим фактором – умышленными (25%) или ошибочными (50%) действиями сотрудников

Затраты на оснащение четырех серверов компании продуктами Secret Disk Server NG составят 180 тыс. руб.

Безопасность повышается за счет возможности введения более стойких (длинных и сложных) паролей.

Вариант с Windows Logon можно использовать даже тогда, когда в сети организации нет домена, а также для отдельных рабочих станций, не входящих в его состав. Стоимость Windows Logon составляет 2065 руб. и не зависит от числа пользователей.

Защита баз данных и корпоративных информационных ресурсов. Современные программно-аппаратные комплексы для защиты от несанкционированного доступа к конфиденциальной информации, обрабатываемой и хранящейся на серверах организации, такие как Secret Disk Server NG, позволяют защитить жесткий диск, зашифровав его с помощью устойчивого к взлому криптографического алгоритма, и поддерживают программные и аппаратные RAID-массивы любого уровня, а также внешние носители.

Для того чтобы разрешить пользователям работу с защищенным диском/разделом диска, администратор безопасности подсоединяет к своей рабочей станции персональное средство строгой аутентификации – токен (в виде USB-ключа или смарт-карты) и вводит пин-код. После этого защищенный диск становится доступным пользователям в соответствии с их правами доступа, установленными средствами ОС. Такие продукты защищают информацию от злоумышленника, который сумел получить физический доступ к жесткому диску. Запрет сетевого доступа к данным, хранящимся и обрабатывающимся на серверах приложений, например файлам баз данных SQL-серверов, почтовым хранилищам и др., позволяет исключить риск несанкционированного копирования данных пользователями, имеющими административные полномочия в системе (защита от инсайдеров).

Выполняемое шифрование прозрачно. Это означает, что данные на диске постоянно зашифрованы, а их расшифровка происходит на лету, при обраще-

Коммерческое предложение для SMB-компании

Продукт или услуга	Особенности	Цена, руб.	Количество, шт.	Стоимость, руб.
USB-ключи для аутентификации пользователей				
Электронный ключ eToken PRO/32K	Электронный USB-ключ. Память: 32 кбайт. Алгоритмы: RSA/1024, DES, 3DES, SHA-1	1 390	75	104 250
Для аутентификации пользователей при входе в операционную систему (в том числе и вне домена)				
eToken Windows Logon. Комплект документации и ПО	Media Kit. Ключ не входит. Лицензия не входит. Упаковка: DVD-коробка	590	1	590
eToken Windows Logon. Лицензия на использование	Лицензия корпоративная (одна на организацию). Количество пользователей продукта равно числу eToken, приобретенных вместе с продуктом	1 475	1	1 475
Руководство по внедрению строгой двухфакторной аутентификации пользователей в домене на базе Windows Server и реализации ЭЦП и шифрования почты в MS Outlook				
eToken для Microsoft Windows 2000/XP/2003. Комплект документации и ПО	Media Kit. Ключ не входит. Лицензия не входит. Упаковка: DVD-коробка	590	1	590
eToken для Microsoft Windows 2000/XP/2003. Лицензия на использование	Лицензия корпоративная (одна на организацию). Количество пользователей продукта равно числу eToken, приобретенных вместе с продуктом	1 475	1	1 475
Для защиты информации, хранящейся на персональных компьютерах				
Secret Disk, версия 4.0. Лицензия на использование	Лицензия на использование для владельцев USB-ключей eToken PRO/OTP/FLASH	2 500	21	52 500
Secret Disk-MK, версия 4.0	Комплект документации и ПО	590	1	590
Для защиты информации, хранящейся хранящейся на двух файл-серверах (50 и 25 пользователей)				
SDSNG3.x-FS-50-L	Лицензия на использование Secret Disk Server NG для файл-сервера на 50 одновременных подключений	52 990	1	52 990
SDSNG3.x-FS-25-L	Лицензия на использование Secret Disk Server NG для файл-сервера на 25 одновременных подключений	37 990	1	37 990
eToken PRO/32K	Электронный ключ eToken PRO/32K. Используется для хранения серверной лицензии	1 390	2	2 780
SDSNG3.x-Admin-L	Лицензия администратора Secret Disk Server NG, записывается в eToken PRO/32K	1 900	2	3 800
SDSNG3.x-MK	Secret Disk Server NG версия 3.x. Комплект документации и ПО	1 480	1	1 480
ACS-ALRM-COM White	Устройство "Красная кнопка" для подачи сигнала "тревога"	440	2	880
	Итого			**261 390**

Источник: компания Aladdin

нии локальных приложений или сетевых пользователей к этому диску.

Кроме того, в Secret Disk Server NG предусмотрена возможность подачи сигнала тревоги (специальной кнопкой, радиобрелоком или комбинацией клавиш), по которому происходит отключение зашифрованного диска или даже уничтожение специального защищенного хранилища с информацией о зашифрованных дисках и зарегистрированных администраторах безопасности. В последнем случае получить доступ к данным будет невозможно, даже предъявив токен и введя правильный пин-код. Для восстановления доступа к информации придется использовать заранее созданный файл резервной копии защищенного хранилища (размещенный, например, на носителе, хранящемся в надежном сейфе).

Затраты на оснащение четырех серверов продуктами Secret Disk Server NG составят ориентировочно 180 тыс. руб.

Защита данных, хранимых на ноутбуках сотрудников. Современный ноутбук хранит большое количество конфиденциальной информации. При этом большинство программ и приложений по умолчанию хранят данные на системном диске. Там же находятся временные файлы, журналы работы, файл подкачки и др.

На рынке представлен широкий ассортимент решений, обеспечивающих надежное шифрование данных, находящихся на несистемных разделах жестких дисков или в специальных файловых контейнерах. Большинство из них предлагают только парольную аутентификацию пользователей.

Продукт компании Aladdin – Secret Disk 4 позволяет зашифровать все разделы жесткого диска, включая системный. Таким образом, даже загрузка операционной системы будет невозможна без подключения USB-токена и ввода правильного пин-кода от него. Кража ноутбука, защищенного Secret Disk 4, фактически равносильна краже компьютера, лишенного жесткого диска.

Лицензия на продукт стоит 2300–2800 руб. (в зависимости от количества рабочих мест).

Итоги и рекомендации

Коммерческое предложение для небольшой компании (75 пользователей, 2 файловых сервера, 21 мобильный компьютер) представлено в таблице.

Предлагаемый набор продуктов позволит существенно повысить информационную безопасность компании. Для доступа к информационным ресурсам все сотрудники должны будут использовать строгую двухфакторную аутентификацию с помощью USB-ключей. Важные почтовые сообщения, отправляемые из одного офиса в другой, можно будет надежно зашифровать. Базы данных на серверах организации будут защищены от посторонних в случае их кражи. Все мобильные пользователи получат гарантию сохранности конфиденциальности данных на своих ноутбуках.

Финансовые затраты составят около 3500 руб. на одно рабочее место. Дополнительной абонентской платы за сопровождение продуктов не взимается. Предлагаемое решение легко масштабируется, позволяя не только проводить поэтапное внедрение, но и легко адаптировать его под дальнейшие нужды компании, например при расширении штата.

Важным преимуществом является также максимально полное задействование уже имеющегося в компании ПО – штатных возможностей ОС Microsoft Windows.

В качестве дальнейших рекомендаций по повышению уровня защищенности информационных ресурсов компании можно предложить:

- разработку корпоративной политики ИБ с четким разделением ролей пользователей и внесением соответствующих разделов в должностные инструкции сотрудников;
- внедрение полнофункциональной системы управления жизненным циклом токенов – Token Management System, позволяющей автоматизировать типовые задачи по предоставлению пользователям прав доступа к тем или иным информационным ресурсам с помощью аппаратных токенов на основе выработанной политики информационной безопасности;
- установку системы комплексного обеспечения проактивной безопасности информации в корпоративной сети на уровне интернет-шлюзов и почтовых серверов – eSafe. ИКС

Кража ноутбука, защищенного Secret Disk 4, равносильна краже компьютера, лишенного жесткого диска