Каналы утечки информации

Владимир Безмалый

Охарактеризовать состояние информации что дома, что на работе, можно одним словом: «Воруют».

Представив в предыдущей статье угрозы для домашних пользователей, присмотримся повнимательнее к каналам утечки информации с домашних, а также с рабочих компьютеров в организациях, где к защите данных относятся еще не слишком серьезно.

Согласно международному исследованию, проведенному сотрудниками «Лаборатории Касперского» совместно с агентством B2B International в 22 странах мира, включая РФ, за последний год 96% небольших отечественных компаний хотя бы раз сталкивались с информационными угрозами, опережая по этому показателю соответствующие предприятия из США и Европы, где он не превышает 91%.

Чаще всего российские малые и средние предприятия страдают от спама (74%) и вредоносных программ (71%) — вирусов, червей и шпионского ПО. Со взломом компьютеров сталкиваются четверть представителей СМБ-сектора, со случаями корпоративного шпионажа — 12%.

Подобные инциденты в России закончились потерей данных в 40% случаев, в США и Европе — в 23% случаев. Из этого несложно сделать вывод о том, что текущий уровень обеспечения информационной безопасности в России в данном сегменте рынка значительно ниже, чем на таких же предприятиях в Европе и США.

По данным «Лаборатории Касперского», ежедневно регистрируется до 125 тыс. новых угроз, а год назад их было 70 000.

Казалось бы, такое огромное количество угроз должно заставить задуматься, однако результаты опроса показали, что IT-стратегия не является приоритетом для компаний малого и среднего бизнеса. Большинство компаний поставили ее на пятое место.

Сейчас наиболее распространены следующие меры информационной безопасности:

- антивирусная защита — 70%;
- регулярная установка обновлений — 62%;
- политика и механизмы аварийного восстановления системы — 46%;
- лишь одна компания из 100 не имеет антивирусной защиты.

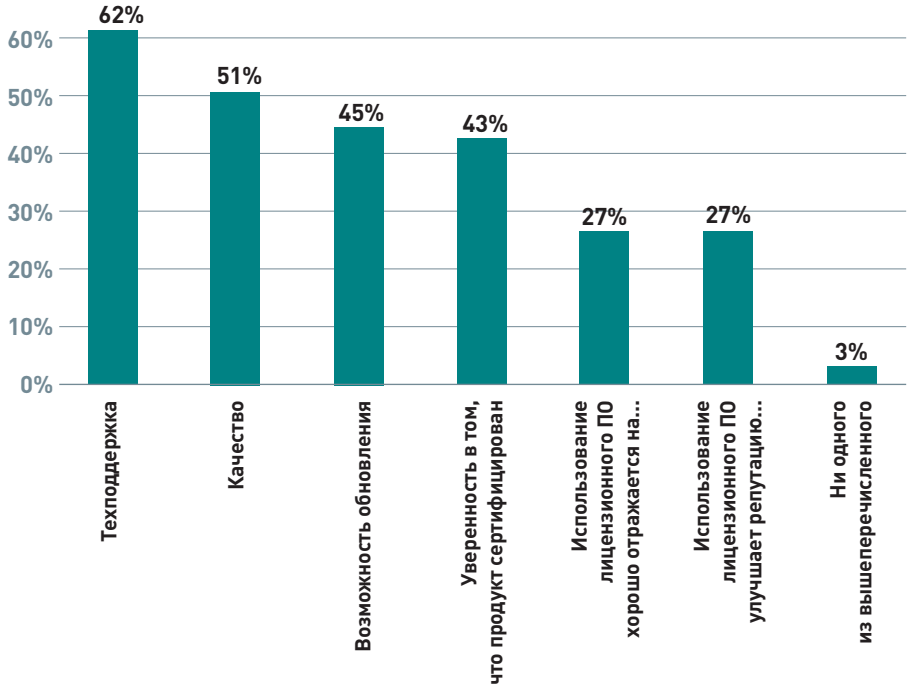
Обсуждая информационную безопасность, следует учесть и типичную для России ситуацию с использованием нелицензионного ПО.

Треть небольших российских компаний считают, что преимущества коммерческих антивирусов по сравнению с бесплатным ПО не оправдывают затраты на них. Чуть меньше респондентов (23%) по той же причине допускают применение нелицензионного ПО. Более того, свыше четверти специалистов отметили, что вынуждены использовать бесплатные или нелицензионные версии антивирусных продуктов из-за жестких бюджетных ограничений в компании. В регионах России эта проблема стоит особенно остро: о вынужденном переходе на бесплатные и нелицензионные антивирусы заявили 32% региональных компаний. В Москве этот показатель чуть ниже — 23% организаций.

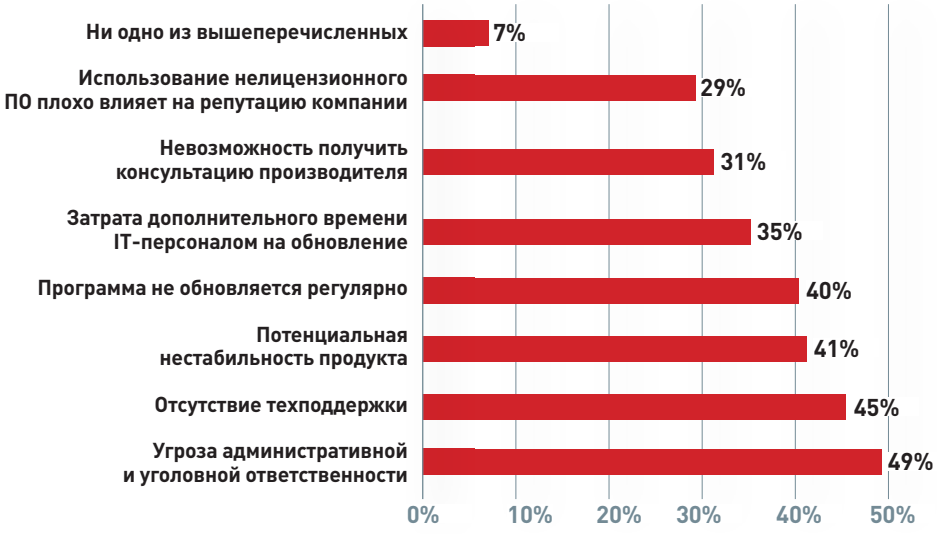
Большую тревогу у российских представителей СМБ-компаний вызывает

Типы внешних угроз, с которыми сталкиваются компании малого и среднего бизнеса

Преимущества лицензионного защитного ПО с точки зрения российских малых и средних компаний



Недостатки нелицензионного защищенного ПО с точки зрения российских малых и средних компаний



использование социальных сетей. Почти половина опрошенных назвала их главным источником угроз. На втором месте прочно обосновались сменные носители.

Так, 60% малых и средних компаний в России запрещают своим сотрудникам доступ к социальным сетям, 69% — к онлайн-играм, а 52% — к P2P-сетям для обмена файлами (например, BitTorrent, eDonkey).

Так почему же наблюдается такой разброс в цифрах по Европе и США и по России в целом?

Прежде всего потому, что у нас к сектору малых предприятий традиционно относятся те, на которых работают от одного до десяти ПК. Как правило, обеспечением информационной безопасности там занимается системный администратор, к тому же зачастую являющийся приходящим раз в неделю работником. Естественно, в таком случае говорить о качественном обеспечении требований ИБ просто не приходится. На это нет ни времени, ни денег, ни желания. Кроме того, руководство фирмы обычно просто не задумывается об этом. Чаще всего можно услышать: «Да что у нас воровать? Вот украдут, тогда и думать будем, а пока на насущные проблемы денег нет!»

С одной стороны, такой подход, безусловно, имеет место, а с другой — вполне понятно, почему думают именно так. Для того чтобы задумываться о проблеме информационной безопасности, нужно быть уверенным в том, что твой бизнес просуществует еще хотя бы лет пять. Думаю, что у большинства владельцев малых предприятий такой уверенности просто нет. Тут бы как-то с налоговой (пожарной, санитарной) службами договориться, а вы об информационной безопасности. И пока бизнес строится таким образом, у информационной безопасности будет один из самых низких приоритетов! ■