Официальное мнение

Вячеслав Медведев,
ведущий аналитик отдела развития,
«Доктор Веб»,
www.drweb.com

PC Magazine/RE: Не пришло ли время, когда защита должна обеспечиваться интегрированными «в железо» средствами?

В. М.: Подобные попытки были и неоднократно. Помню попытку вывести на рынок систему с TRM-модулями. Рынок идею не принял, чему было много разных причин. Повлияла, конечно, и возросшая цена, но в большей степени данную инициативу убило нежелание пользователей ограничивать свои действия. Не стоит забывать и об антимонопольных органах. Наличие встроенной системы всегда негативно влияет на конкуренцию (если только встроенная система не убога по умолчанию). Достаточно вспомнить многолетние суды против Microsoft по поводу наличия в Windows встроенного браузера.

PC Magazine/RE: А может быть стоит создать «национальную защищенную ОС»?

В. М.: Идея с точки зрения безопасности не так и плоха. Хотим мы того или нет, но противостояние с мировыми центрами разработки ПО — сложившийся факт. Как гласит известная мудрость — для ведения войны нужно три вещи: деньги, деньги и еще раз деньги. При этом разработка самой ОС — не самая трудоемкая задача, этим занимаются многие студенты в качестве своих проектов. Создать ядро ОС можно за ограниченный срок. Но пользователям нужны не ОС, а базы данных, почтовые клиенты, пакеты для дизайнерских работ. Нетрудно подсчитать, сколько программ использует тот или иной специалист и его окружение. И это не говоря об играх, сетевых сервисах и т. д. Можно ли заново написать все активно используемое ПО, идеально его спроектировав, в приемлемые сроки? Да и написать ПО — это полдела. В той же Европе большие территории заявляли о переходе на Linux — и сразу сталкивались с огромными проблемами. Как минимум требуется глобальная система переобучения и техническая поддержка в масштабах всей страны.

Думаю, что начинать нужно с малого. Например, с почтовых систем (серверов и клиентов) и замкнутой сети для критически важных систем и госорганов. Нужна не новая ОС — нужна новая парадигма безопасности, национальная система информирования об угрозах и реагирования на них, методики построения систем защиты в условиях, когда любое ПО (в том числе и средства защиты) ненадежно, и его можно обойти.

PC Magazine/RE: Наиболее актуальные, на ваш взгляд, отличия продуктов «Доктор Веб», предлагаемых на 2015 г.?

В. М.: Развитие средств обнаружения и лечения. Будут, естественно, и новые продукты. Но текущая проблема информационной безопасности — рост количества организованных преступных групп, наладивших потоковый выпуск вредоносных программ, не обнаруживаемых в момент проникновения. Старые критерии оценки средств безопасности ушли в прошлое. Важно то, что под капотом. Каков бы ни был дизайн, если нет «движка» — машина поедет в лучшем случае под горку. Будет развитие поведенческого анализатора, системы поиска пока не попавших на анализ вредоносных программ, сетевого экрана.

PC Magazine/RE: Как будут развиваться продукты «Доктор Веб»?

В. М.: Мы будем поддерживать все выходящие ОС и корпоративные продукты — все, что используется клиентами, должно быть защищено. Будут развиваться средства администрирования, решения для провайдеров услуг.