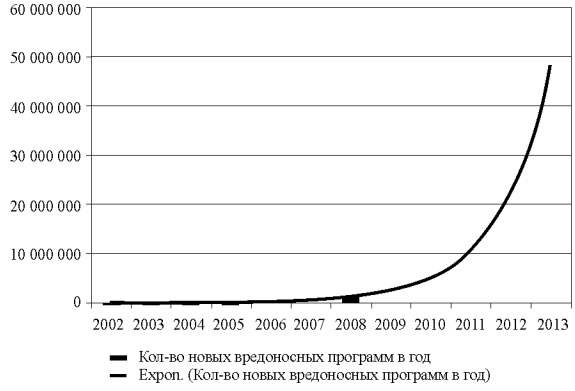
О. М. Никонова (Москва, ЦЭМИ РАН)**. Инновационные технологии компьютерной безопасности в образовательных учреждениях.**

Интеграция компьютерных технологий в современный процесс образования заставляет администрацию и преподавателей учебных заведений заботиться об антивирусной защите информации, хранящейся на ПК компьютерных классов и аудиторий.

Киберпреступность давно стала одним из самых успешных видов бизнеса и количество всевозможных вредоносных программ увеличивается. Старые антивирусные технологии теряют эффективность, нужны инновации.

Вредоносное ПО и борьба с последствиями его деятельности в течение уже нескольких лет являются одной из самых серьезных проблем для всех, кто работает за компьютером. Каждый студент, преподаватель образовательного учреждения ежедневно сталкивается в сети с различными вредоносными и нежелательными программами, которых становится все больше и больше. Целью злоумышленников может быть кража финансовых данных, паролей к различным интернет-сервисам и другой персональной информации; вымогательство, или банальное использование вычислительных ресурсов пользователя компьютера в криминальных целях.

Любой антивирусный эксперт знает, что количество регистрируемых в его лаборатории вредоносных программ растет в геометрической прогрессии. Говоря проще, их количество каждый год увеличивается в разы. Если ничего не менять, то со старыми реактивными (сигнатурными) и старыми проактивными технологиями (расширенные сигнатуры, эвристика, поведенческий анализ и т. п.) антивирусы с каждым годом будут пропускать все больше и больше, и в какой-то момент использовать их станет вовсе бессмысленно. Ниже представлен график прогноза увеличения количества вредоносных программ до 2013 года [3]



Из графика видно, если никаких глобальных изменений не произойдет, то в 2013 году будет выпущено порядка 50 млн. новых вредоносных программ, т. е. 136 тыс. ежедневно. Возникает извечный вопрос: «Что же делать?»В той или иной степени все ведущие мировые вендоры сейчас работают над инновационными технологиями, внедренными в новые антивирусные программы, предлагаемые к реализации в 2011 году. Среди них можно отметить такие компании как: Symantec, Trend Micro, «Лаборатория Касперского», McAfee и Panda Security [4].

Необходим профессиональный подход к защите информации в образовательных учреждениях.

1. Комплексный подход к безопасности конечных точек: от антивируса, контроля приложений и съемных носителей до интеллектуального патч-менеджмента, управления ИТ-рисками и проверки на соответствие политикам и стандартам безопасности.

2. Обеспечение всестороннего централизованного мониторинга деятельности студентов, включая: E-mail, чаты, мгновенные сообщения, посещаемые веб-сайты, он-

лайновые поисковые запросы, нажимаемые клавиши и используемые программы. Механизмы предупреждения злоупотреблений и расследования инцидентов.

3. Локализация на защищаемом компьютере возможности запуска программ с механизмом контроля доступа к ресурсам (разграничения прав доступа к файловым объектам), при условии выполнения требований к полноте и к корректности реализации разграничительной политики доступа. Под полнотой реализации разграничительной политики доступа в данном случае понимается возможность разграничить доступ "на выполнение" для всех компьютерных ресурсов, с которых возможен запуск программы. Под корректностью реализации разграничительной политики доступа в данном случае понимается предотвращение любой возможности модификации разрешенных к запуску исполняемых файлов, а также предотвращение любой возможности запуска под их именем (под «видом» санкционированных) других (несанкционированных для выполнения) исполняемых файлов.

4. Сегментирование образовательной сети с отделением значимых информационных ресурсов от кампусного студенческого сетевого пространства.

Разумеется, при разработке проекта реализации перечисленных направлений необходимо во всех аспектах учитывать соотношение ценности защищаемой информации с ценой внедрения комплексных мер.

СПИСОК ЛИТЕРАТУРЫ

1. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. Учебное пособие для высших учебных заведений. М.: 2010, 544 с.
2. *Шаньгин В. Ф.* Информационная безопасность компьютерных систем и сетей. Учебное пособие для высших учебных заведений. М.:2009, 416 с.
3. Информационно-аналитический центр. http://www.anti-malware. ru/antivirus_trends.
4. Антивирус Навигатор http://www.antivirus-navigator.com/