ОБЗОР СОВРЕМЕННЫХ АНТИВИРУСОВ

Якунин С. А.
Шевченко В.А.– руководитель
ХНАДУ

Компьютерный вирус был назван по аналогии с биологическими за исходный механизм распространения. Человеческий вирус внедряется в клетку, после чего начинает размножаться. Так и компьютерный: попав в программу, вирус действует аналогичным образом. Основная цель вируса – его распространение, нарушение работы программно-аппаратных комплексов удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей.

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Изначально вирусы распространялись на дискетах и другихносителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

Для того, чтобы защитить свой компьютер, нужно использовать антивирусы.

Антивирус – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Эффективными программами-антивирусами являются ESET NOD32 и Malwarebytes.

ESET NOD32 – это комплексное антивирусное решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программычерви, spyware, adware, фишинг-атаки. В ESET NOD32

используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ. ThreatSense является собственной запатентованной технологией компании и основана на эвристическом анализе потенциальных угроз. Как утверждают сами разработчики, она работает на опережение планов вирусописателей. Приложение осуществляет запуск подозрительного файла в изолированной виртуальной среде и отслеживает его поведение и структуру кода. Если характер действий рассматриваемого объекта несет фатальный характер, антивирус немедленно реагирует, блокируя его, затем уведомляет пользователя и отправляет данные анализа разработчикам.

Плюсы: в сравнении с конкурентами, приложение от ESET существенно меньше нагружает систему, при этом, скорость сканирования показывает отличные результаты

Минусы:

1. Глубина сканирования. Специалисты отмечают возможную недостаточность глубины сканирования каталогов с объемной структурой, в результате, некоторые вредоносные объекты могут быть не обнаружены. Для домашнего использования этот недостаток не критичен, так как воссоздать такие условия, когда сканер не сможет проверить все файлы достаточно сложно, к тому же велика вероятность того, что этот недостаток будет устранен разработчиками в будущих релизах.

2. Ложные срабатывания. Некоторые пользователи замечают ложные срабатывания на файлы, не являющиеся вредоносными. Это происходит достаточно редко и не столь критично, хоть и может вызвать панику у неопытных пользователей.

Malwarebytesпозволяет обнаруживать, помещать в карантин и удалять трояны и черви. Программа доступна в бесплатном варианте с неполным функционалом, но также можно купить полную версию программы.

Бесплатная версия имеет функции быстрого сканирования и полного сканирования всех дисков. В платной версии доступно мгновенное сканированиеоперативной памяти и объектов автозапуска, добавлен защитный модуль, который находится в оперативной памяти и сканирует объекты непосредственно при обращении к ним.

Плюсы: сканер данного антивируса отлично находит некоторые вирусы и другие совершенно ненужные нам с вами трояны-черви, которых не могут найти распространенные и считающиеся надежными антивирусные программы. Так же, если его активировать, то есть приобрести Pro версию, будет работать защитный модуль, который в режиме реального времени сканирует все процессы и программы. И в защитном модуле есть хорошая функция – он автоматически распознает попытки соединения трояна с удаленным компьютером хозяина трояна и прерывает это соединение

Минусы: Malwarebytes Anti-Malware не умеет лечить вирусы, он их находит, после сканирования предложит удалить в карантин или оставить на месте. Если оставить, значит, проблема не решена, а если удалить, то могут пострадать нужные программы. Так же он не сканирует архивы. Если в архиве есть вирус, он не найдет, но если разархивировать файлы, которые заражены, он их находит и удаляет

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками.

Литература

1. ru.wikipedia.org
2. hidemy.name/ru/obzor-sovremennyh-antivirusov
3. www.comss.ru