УДК 004.056.57

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ БРАНДМАУЭРА KASPERSKY И NOD 32

Омельницкая Екатерина Викторовна, Баранов Анатолий Анатольевич
ГВУЗ «Национальный горный университет», nmu.org.ua, Omelnyckaya18katya@mail.ru

**Брандмауэр – это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую . Таким образом пропускает через себя весь сетевой трафик. Для каждого проходящего пакета брандмауэр принимает решение пропускать его или отбросить.**

***Ключевые слова*** **–** «Брандмауэр»**,** «ESET NOD32 Smart Security»**,** «Kaspersky Anti–Hacker»**,** «Kaspersky Antivirus Personal»**,** «Kaspersky Internet Security»

## ВСТУПЛЕНИЕ

Брандмауэр - это средство защиты, которое можно использовать для управления доступом между надежной сетью и менее надежной. Брандмауэр выполняет роль стражи между небезопасной глобальной сетью Internet и внутренними сетями. Брандмауэры, которые будут описаны в данной статье, также могут выполнять роль антивируса.

## ХАРАКТЕРИСТИКИ И ВОЗМОЖНОСТИ KASPERSKY INTERNET SECURITY, KASPERSKY ANTI-HACKER, KASPERSKY ANTIVIRUS PERSONAL И ESET NOD32 SMART SECURITY

Основными путями проникновения вирусов в компьютер являются съемные диски, а также компьютерные сети. Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Сейчас существует не малый выбор антивирусных систем, но для сравнения были выбраны два самых широко распространенных по результатам статистических исследований вида брандмауэров Kaspersky и NOD 32.

В антивирусной индустрии существуют два основных метода детектирования вредоносного ПО – сигнатурный и эвристический.

Сигнатурный метод эффективен против известных угроз, так как позволяет проверить потенциально опасный код на предмет его совпадения с существующим шаблоном вируса – сигнатурой, которая содержится в базе данных антивируса.

Эвристический метод защищает пользователя от новых угроз, которые еще не занесены в сигнатурную базу. Антивирус распознает вредоносную программу еще до того, как компания-разработчик получит образец кода, проанализирует его и выпустит новую сигнатуру.

Наиболее эффективную защиту могут гарантировать антивирусные решения, в которых сочетаются сигнатурный и эвристический методы. Именно такой подход реализован в решениях ESET NOD32. Разработчики ESET впервые в антивирусной индустрии стали использовать эвристические методы детектирования вредоносного ПО.

ESET NOD32 Smart Security разработан на основе передовой технологии ThreatSense. ThreatSense - это единый эвристический механизм, представляющий собой так называемую расширенную эвристику (Advanced Heuristics). В решениях ESET NOD32 эвристика – это технологическая платформа, на которой базируется работа всей системы. ThreatSense используется для выявления около 90% вирусов, одновременно применяются эмуляция, алгоритмический анализ, пассивная эвристика и сигнатурный метод.

Основными функциональными особенностями Esest NOD32 являются:

- эвристический анализ, позволяющий обнаруживать неизвестные угрозы;
- технология ThreatSense – анализ файлов для выявления вирусов, программ-шпионов (spyware), непрошенной рекламы (adware), phishing-атак и других угроз;
- проверка и удаление вирусов из заблокированных для записей файлов (к примеру, защищенные системой безопасности Windows библиотеки DLL);
- безопасность Wi-Fi;
- sysInspector -мощный инструмент для анализа работы операционной системы;
- самостоятельное обновление;
- сканирование при запуске;
- поверка протоколов HTTP, POP3 и SMTP и другие;
- возможность защитить настройки ESET NOD32 паролем;

При этом возможен ряд новых функций, а именно:

- система предотвращения вторжения на узел (HIPS);
- облачная технология ThreatSense;
- персональный файервол;
- пять режимов фильтрации;
- настройка и использование правил.

Интерфейс NOD32 организован максимально эргономично и эффективно. Основные пункты меню содержат подзаголовки, которые в свою очередь открывают справа от основного окна область работы с выбранным модулем или компонентом. Обновление

– одна из сильных сторон NOD32. Первоначально на выбор предложены целых 3 сервера с возможностью последующего добавления адресов. Также поддерживаются локальные обновления с сетевых ресурсов. Работа антивируса ESET NOD32 не отражается на производительности компьютера – сканирование и процессы обновления происходят практически незаметно для пользователя, не нагружая систему. Также у него высокая скорость работы.

Проведя некоторые исследования брандмауэра Kaspersky Internet Security, следует заметить, что можно вместо него использовать совместно Kaspersky Anti–Hacker и Kaspersky Antivirus Personal.

Отличие заключается в том, что Kaspersky Anti–Hacker является персональным файерволом. Программа предохраняет компьютер от заражения некоторыми типами вирусов и обеспечивает сохранность файлов от несанкционированного удаления или изменения. Он контролирует целостность приложений, и если его файлы изменяются, то пользователь будет проинформирован об этом. Все события, происходящие во время работы в сети, протоколируются в журнале работы.

Следует понимать, что Kaspersky Anti–Hacker является файерволом, который контролирует трафик между компьютером и серверами, а не антивирусом.

Основные функции Kaspersky Anti–Hacker:

- контроль сетевой активности всех приложений, установленных на компьютере;
- режим невидимости в сети, значительно затрудняет обнаружение компьютера в сети, и, следовательно, осложняет процесс подготовки и проведения атаки на него;
- определяет попытки сканирования портов, и блокирует тот хост, с которого производилось сканирование;
- позволяет просматривать список всех установленных соединений с сетью и при необходимости разрывать их.

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP/7/8 и другие версии данной операционной системы, от всех известных видов вирусов, включая потенциально опасное программное обеспечение. Также он не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию.

Однако, чтобы не тратить время на настройку двух защитных компонентов можно и даже нужно использовать Kaspersky Internet Security, который обеспечивает комплексную защиту от разнообразных угроз в сети, что было обеспечено путем включения нескольких добавочных модулей. На Kaspersky Internet Security дополнительно установлены файервол, защита от спама и фишинга, а также родительский контроль, работа с вирусами в почте, новый эвристический анализатор, обновленный и удобный интерфейс. Программа может блокировать вредоносные ссылки в популярных социальных сетях Facebook, ВКонтакте, Twitter; защита от эксплойтов; появился модуль "Антиспам", позволяющий усовершенствовать работу с вирусами; защита персональных данных.

## ВЫВОДЫ

Проведя анализ и изучив характеристики Kaspersky Internet Security и ESET NOD32 Smart Security, как вывод можно сказать, что производители данных брандмауэров постоянно усовершенствуют их и особое внимание уделяется сигнатурному и эвристическому анализам. Статистика показала, что у Kaspersky Internet Security оценка 2.25, а у ESET NOD32 Smart Security - 4,75 (чем меньше, тем лучше). Но выбор остается за пользователем.

## ПЕРЕЧЕНЬ ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Сравнительный анализ современных антивирусных программ (Электрон. ресурс) / Способ доступа: URL: http://www.coolreferat.com.– Загол. с экрана.

2. Нод 32 (Электрон. ресурс) / Способ доступа: URL: http://www.wm-bonus-ru.narod.ru/antivirusnoe_programnoe_obespechenie/nod32.htm. – Загол. с экрана.

3. Kaspersky (Электрон. ресурс) / Способ доступа: URL: http://www.kaspersky.ru/docs