АНАЛИЗ ЭФФЕКТИВНОСТИ ФИЛЬТРАЦИИ НЕБЛАГОПРИЯТНОГО СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ КОМПЛЕКСНЫХ СИСТЕМ

канд. техн. наук, доц. С.Ю. Гавриленко, студ. А.А. Горносталь, Национальный технический университет "Харьковский политехнический институт", г. Харьков

Угроза сетевой безопасности является самой серьёзной информационной проблей. При этом существует очень мало средств, которые бы полностью брали на себя функцию фильтрации трафика [1].

Наиболее эффективным является совмещение различных методов анализа получаемых сетевых пакетов [2]. Одним из преуспевающих проектов современности в области фильтрации нежелательного Интернет-трафика на пути к конечному пользователю является The Advanced Threat Defense Platform. Основным преимуществом данного программно-аппаратного комплекса является особый комплексный подход к оценке получаемых данных [3]. Специальное устройство анализирует сетевые запросы и трафик следующим образом:

1. Полученные пакеты помещаются в специальные коллекторы с виртуальной рабочей средой.
2. Трафик всесторонне изучается (проводится проверка источника информации, анализируется количество получателей, поведение данных в рабочей среде и возможные последствия их использования и т.д.).
3. Результаты тестирования сохраняются в базе.
4. Система пытается устранить вредоносный код из трафика или восстановить повреждённые файлы на основе имеющейся информации.
5. Принимается решение по поводу дальнейшего пропуска пакетов.

Таким образом, конечный получатель данных полностью защищён от нежелательного (вредоносного) трафика [4]. При этом проверка проходит не за счёт ресурсов компьютера, а за счёт ресурсов подключаемого к маршрутизатору устройства, которое играет роль потоковых ворот, используя для защиты сетей как имеющуюся базу, так и методы моделирования виртуальных программных сред.

Список литературы: **1.** Актуальность обеспечения информационной безопасности в системах облачных вычислений, анализ источников угроз [Электронный ресурс] – Режим доступа: http://www.tusur.ru/filearchive/reports-magazine/2012-25-2/078.pdf. **2**. Top Threats to Cloud Computing V1.0 / Cloud Security Alliance, March 2010 [Электронный ресурс] – Режим доступа: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. **3.** Large enterprise with cloud infrastructure mitigates APT risk while containing costs [Электронный ресурс] – Режим доступа: http://go.cyphort.com/rs/181-NTN-682/images/CYPHORT_CS_LgCloudEnterprise.pdf. **4.** Advanced Malware Attacks Need An Advanced Response [Электронный ресурс] – Режим доступа: http://go.cyphort.com/rs/181-NTN-682/images/CYPHORT_DataSheet.pdf.