DOI: 10.17117/na.2015.10.03.120

<http://ucom.ru/doc/na.2015.10.03.120.pdf>

Поступила (Received): 27.10.2015

**Кожанов М.Г., Амиров А.Ж.,
Томилова Н.И., Сагатбекова Д.Е.
Метод управления трафиком на межсетевых
узлах локальных вычислительных сетей**

**Kozhanov M.G., Tomilova N.I., Amirov A.Zh., Sagatbekova D.E.
The method of the traffic management on the
interconnect local computational networks nodes**

В статье рассмотрен метод интеллектуально-адаптивного управления трафиком на межсетевых узлах ЛВС с использованием предопределенной алгоритмизации и нечеткой логики, позволяющий предсказывать реакцию хостов на всевозможные виды воздействий при помощи распределенного анализа

Ключевые слова: защита информации, алгоритмизация, вычислительные сети

The article describes the method of intelligent adaptive the traffic management on the LAN interconnect sites using predefined algorithms and fuzzy logic, which allows to predict the reaction of the host to all kinds of influences using distributed analysis

Key words: data protection, algorithmization, computer networks

Кожанов Мурат Галиаскарович

Магистрант

Карагандинский государственный технический университет

г. Караганда, Бульвар-мира, 56

Kozhanov Murat Galiaskarovich

Master

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Томилова Надежда Ивановна

Кандидат технических наук, декан

Карагандинский государственный технический университет

г. Караганда, Бульвар-мира, 56

Tomilova Nadezhda Ivanovna

Candidate of Engineering Sciences, Dean

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Амиров Азамат Жанбулатович

Заведующий кафедрой

Карагандинский государственный технический университет

г. Караганда, Бульвар-мира, 56

Amirov Azamat Zhanbulatovich

Head of Department

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Сагатбекова Динара Ермековна

Магистрант

Карагандинский государственный технический университет

г. Караганда, Бульвар-мира, 56

Sagatbekova Dinara Ermekovna

Master

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Информационно-коммуникационные технологии оказывают значительное влияние на уровень экономической конкурентоспособности и государственной безопасности страны. Сетевые инфраструктуры муниципальных учреждений и частных фирм в предпочтительном большинстве организованы на технологии Ethernet и подключены к сети интернет Интернет, функционирующей на базе стека протоколов TCP/IP и широко распространенной по всему миру. Впрочем, данные технологии имеют ряд уязвимостей, обусловленных в первую очередь алгоритмами протоколов различного уровня взаимодействия на базе «жесткой» логики. Необходимость оптимизации загрузки каналов связи в корпоративных вычислительных сетях считается одной из приоритетных задач передовых IT-технологий [1]. Другим существенным аспектом считается защита процесса передачи данных. Уровень обеспечения информационной защищенности является следствием эффективности методов управления трафиком. Для достижения этих целей разрабатываются специализированные методы управления графиком вычислительных сетей. Так, вопросы управления трафиком корпоративных вычислительных сетей с точки зрения обеспечения надежного функционирования рассмотрены в работах В.М. Вишневого, С.Н. Вербицкого, В.В. Рыкова и другие. Однако данные исследования не принимают в расчет человеческий фактор, инсайдерские угрозы, имеющие место в реальных системах [2].

С 2009 г. основным трендом становления алгоритмов и методов управления трафиком локальных вычислительных сетей (ЛВС) являются исследования в сфере технологий обнаружения аномальной активности сетевого трафика по сигнатурным, поведенческим, комбинированным методикам с обеспечением информационной безопасности. Результаты, полученные в данном направлении, опубликованы в работах И.М. Ажмухамедова, Д.Ю. Гамаюнова и А.И. Качалина, Р.Н. Селина и др. Эти способы функционируют на базе жесткой логики с необходимостью в поддержке квалифицированными специалистами и не идентифицируют новые сетевые опасности.

Вопросы автономности сетевого трафика, а также модернизация инструментария накопления статистических данных для проверки и фильтрации сетевых пакетов по их содержимому представлены в работах Y.N. Cho, H. Zhao, Y. Tao и др. Данные методы не ориентированы на функционирование в реальных системах с криптографическими протоколами. Данные обстоятельства обуславливают потребность разработки новых методов интеллектуально-адаптивного управления трафиком вычислительных сетей, которые дадут возможность реструктуризировать загрузку каналов связи и увеличить уровень обеспечения информационной безопасности (ИБ) [3].

Метод управления трафиком на межсетевых узлах локальных вычислительных сетей. В имеющихся системах применяется «жесткая» логика поведения, не проводящая сравнительного анализа и поиска рационального решения, что и позволяет хакерам идентифицировать продукт защиты атакуемого объекта и внедриться через уже известные уязвимости. Для решения этих трудностей разработаны методы интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей с использованием

измененной генетической алгоритмизации и нечеткой логики, позволяющий прогнозировать реакцию хостов на всевозможные виды сетевых действий при помощи распределенного анализа на модельных объектах. Отличия от имеющихся способов заключаются в обеспечении минимизации загрузки канала связи выбором подходящей стратегии управления трафиком при разных типах сетевой активности, а также автоматической идентификацией новейших сетевых угроз и выработкой подходящего решения по их устранению.

При помощи модельных объектов возможно моделирование реакции системы, затем по обратной связи исправление исходной выборки (современных разработок) и идентичной подстройкой фильтра с использованием нечеткой логики выбирать из правильных решений – более оптимальные, что даст возможность уменьшить загрузку как сервера, так и сетевого канала связи [4].

Использование средств защиты от атак типа DoS и DDoS для повышения устойчивости бизнес-систем. Пример подобных средств – система Cisco Guard, способная отражать атаки типа "отказ в обслуживании" (DoS), обнаруженные специализированными средствами обнаружения вторжений, в качестве которых могут выступать Cisco Anomaly Traffic Detector, Cisco IDS/IPS 42xx, Arbor Peakflow и т. д. Подобные средства защиты отводят "загрязненный" атакой трафик и отделяют вредоносные пакеты от пакетов с полезными данными. Эта технология позволяет важным ресурсам сохранить работоспособность в ситуациях, когда классические средства обеспечения безопасности просто блокировали бы трафик.

"Кластеризация" классических средств обеспечения ИБ (межсетевых экранов, средств IDS/IPS, VPN-концентраторов) предназначена для повышения производительности систем защиты до уровня канальных скоростей. Кроме того, использование "кластерных" решений позволяет повышать скорость переключения трафика на резервные устройства и балансировать нагрузку. Как пример можно привести интеграционное решение компании "Микротест", обеспечивающее шифрование по ГОСТу каналов до 3 Гбит/с с использованием средств коммутации контента Cisco и VPN-шлюзов S-terra CSP [5].

Комплексный подход к ИБ всей цепочки средств автоматизации бизнес-процесса. Сочетание традиционных средств обеспечения безопасности на уровне сети с технологиями персонификации защиты рабочих станций и серверов уменьшит число атак и, следовательно, позволит обойтись менее производительными и более дешевыми межсетевыми экранами и IPS, контролирующими наиболее критичные сегменты. Примером таких технологий могут служить Cisco Security Agent (CSA), ISS RealSecure Server/Desktop Protection и Network Admission Control. Вышеупомянутые средства обеспечивают защиту от червей, вирусов и генерируемого ими вредоносного трафика, в частности, DDoS. Как пример: CSA будет блокировать работу почтовых клиентов, пытающихся установить ПО. Network Admission Control (NAC) обеспечивает проверку состояния ОС, средств защиты и антивирусного ПО на ПК каждого пользователя. Если состояние средств защиты на ПК не соответствует политике безопасности, то доступ к сети и информационным ресурсам может быть огра-

ничен или полностью запрещен, а возможные атаки со стороны данного хоста предотвращены; снижается также нагрузка на сетевые IPS.

Список используемых источников:

1. Вишневский В.М., Ляхов А.И., Терещенко Б.Н. Моделирование беспроводных сетей с децентрализованным управлением // Автоматика и телемеханика. 1999. № 6. С. 88-99.
2. Ивницкий В.А. О стационарных вероятностях состояний замкнутой звездообразной сети массового обслуживания при зависимости вероятностей перехода от ее состояния // Автоматика и вычислительная техника. 1994. № 6. С. 29-37.
3. Вербицкий С.Н., Рыков В.В. Численное исследование оптимальных политик управления скоростью обслуживания // Автоматика и телемеханика. 1998. № 11. С. 59-70.
4. Ажмухамедов И.М. Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. №2. С. 68-72.
5. Селин Р.Н. Алгоритм распознавания сетевых атак с мониторингом подозрительной активности и ретроспективным анализом // Известия высших учебных заведений. Северо-Кавказский регион.

© 2015, Кожанов М.Г., Амиров А.Ж., Томилова Н.И., Сагатбекова Д.Е.

Метод управления трафиком на межсетевых узлах локальных вычислительных сетей

© 2015, Kozhanov M.G., Tomilova N.I., Amirov A.Zh., Sagatbekova D.E.

The method of the traffic management on the interconnect local computational networks nodes