информации: шифруют открытый текст одним из криптографических методов, внедряют зашифрованный текст в звуковые файлы, распыляя биты внутри одного или нескольких контейнеров.

3. Рассмотренный метод сокрытия информации может быть использован для формирования «водяных знаков» (защиты авторских прав).

Литература

1. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации. Самара: Изд. ПГУТИ, 2010. – 330 с.
2. Bender W., Gruhl D. u.a. Techniques for data hiding // IBM Systems Journal. №35(3&4), 1996. – P.313-336.
3. Алдошин И.А., Вологдин Э.И. и др. Электроакустика и звуковое вещание. М.: Горячая линия – Телеком, Радио и связь, 2007. – 872 с.
4. Аленин А.А., Алексеев А.П. Пространственное распределение информации в звуковых файлах // Тезисы XVI РНТК ПГУТИ, 2009. – С. 171-172.

HIDDEN DATA TRANSMISSION A SOUND FILE TO WAV FORMAT

Alekseev A.P., Alenin A.A.

There is an acute problem of protecting confidential information and copyrights. Development of new methods of information protection is performed using techniques de-veloped in cryptography and steganography. Cryptographic methods of information security based on a modification (transformation) of the protected message. Steganography allows you to hide the fact of the transfer message. In article results of experimental researches and the program for introduction of the information in sound files are described.

Keywords: *information, steganography, secrecy, signal, level, waveform, container, silence, distortion, evaluation.*

Алексеев Александр Петрович, к.т.н., доцент Кафедры «Информатика и вычислительная техника» Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 228-00-59. E-mail: apa2008@rambler.ru

Аленин Артем Алефтинович, старший преподаватель Димитровградского института технологий, управления и дизайна (филиал Ульяновского государственного технического университета). Тел. (8-842) 355-74-43; 357-25-94. E-mail: styleal@mail.ru

УДК 004.056

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Ажмухамедов И.М., Марьенков А.Н.

Предложена схема повышения безопасности компьютерных систем и сетей на основе анализа сетевого трафика. К преимуществам данной схемы относятся скорость реагирования на угрозы, минимальное использование вычислительных ресурсов системы, отсутствие необходимости разборки пакетов и, как следствие, независимость от сигнатур вредоносных программ.

Ключевые слова: безопасность, трафик, сеть, самоподобие, сетевые аномалии, сетевые атаки, IP-пакеты, циклический анализ, метод Хольта, компьютерные системы, моделирование, прогнозирование.

Введение

В последнее время сложилась устойчивая тенденция увеличения количества атак на компьютерные сети из Internet. Механизмы атак и способы взлома постоянно совершенствуются. Все это делает разработку и внедрение новых методов и средств защиты информации в компьютерных сетях весьма актуальным.

Одним из методов борьбы с атаками через Интернет может служить отслеживание аномального поведения сетевого трафика, поскольку резкое увеличение количества передаваемой или принимаемой извне информации обычно является признаком начала атаки на сетевой ресурс.

Анализ трафика в силу ряда особенностей эксплуатации компьютерных сетей является новой и еще не до конца проработанной в методическом плане задачей.

В этом направлении в настоящее время существует несколько разработок.

Так, например, в [1] при разработке статистического анализатора была выбрана модель, основанная на среднем значении и среднеквадратичном отклонении параметров сетевого трафика. Данный метод основан на сравнении локальных (текущих) характеристик потока пакетов с усредненными за некоторый промежуток времени (глобальными характеристиками).

В качестве статистических характеристик используются выборочное среднее значение, выборочная дисперсия и критерий согласия хи-квадрат.

Если локальные характеристики значительно отличаются от глобальных, то делается вывод об аномальном поведении потока пакетов, которое вполне вероятно может привести к сбоям в работе оборудования, ПО или нарушениям политики безопасности.

В работе [2] рассмотрен подход, который опирается на минимальную информацию о трафике и не учитывает статистику поступления заявок на обслуживание, длину очереди и прочие показатели, характерные для систем массового обслуживания.

В рамках указанного подхода в первую очередь целесообразен анализ среднечасовых и среднесуточных показателей трафика. Эти показатели, с одной стороны, довольно полно отражают состояние работы сети, а с другой – более устойчивы, чем исходные данные, съем которых обычно осуществляется с частотой один раз в несколько минут.

На основе данных, приведенных в [3-5], было выявлено, что задача анализа сетевого трафика обладает следующими специфическими особенностями:

- отсутствует общепризнанная модель сетевого трафика;
- информативность трафика зависит от загруженности каналов: в слабозагруженных каналах информативность падает из-за неустойчивого поведения трафика, в сильнозагруженных – из-за их максимальной загруженности;
- проявляется свойство «самоподобия» трафика вычислительной сети;
- при анализе резких всплесков сетевого трафика необходимо учитывать сезонные колебания, а также другие нарушения стационарности.

На основе анализа этих особенностей был разработан алгоритм управления сетевым трафиком, схема которого приведена на рис. 1.

Весь исходящий и входящий поток информации перехватывается блоком «Сетевой монитор». Данный блок, выполняя функции снифера, производит захват данных на втором уровне коммуникационной модели обмена OSI.

В перехваченных кадрах осуществляется поиск заголовков IP-пакетов, из которых извлекается вся необходимая для дальнейшей работы информация. Полученные таким образом данные сохраняются в «Базе данных сетевой статистики» вместе с датой и временем прихода кадра. На основе накопленной статистики проводится моделирование поведения сети и прогнозирование объема сетевого трафика.

Для этой цели применяются метод циклического анализа и метод Хольта. Эти методы позволяют надежно описать загрузку компьютерной сети и выдают приемлемый результат уже при небольшом объеме исходных данных.

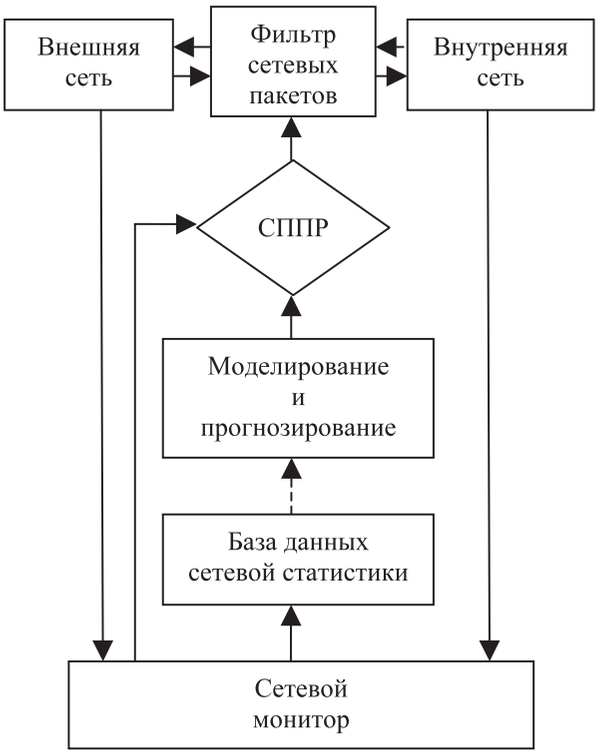

Рис.1. Схема управления сетевым трафиком.

Выводы

Программа, основанная на данном алгоритме, может применяться в сочетании с традиционными, более сфокусированными на сигнатурном анализе, антивирусными пакетами. Она самостоятельно собирает статистику, анализирует собранную информацию и реагирует на внештатные ситуации, генерируя предупреждения о возможном начале атаки или вирусной эпидемии и давая техническому персоналу возможность принять

меры по минимизации ущерба от вредоносного трафика.

Литература

1. Кучер А.В. «Интеллектуальная система поддержки принятия решения на основе нечеткой логики для диагностики состояния сети передачи данных». Краснодар: Изд. КГТУ, 2007.
2. Васенин В.А., Макаров А.А. Проблемы и методики анализа трафика телекоммуникационных компьютерных сетей // Тез. докл. МНТК. Новосибирск, 1997. – С.173.
3. Петров В.В., Платов В.В. Исследование самоподобной структуры телетрафика беспроводной сети // Радиотехнические тетради. №30, 2004. – С. 58-62.
4. Треногин Н.Г., Соколов Д.Е. Фрактальные свойства сетевого трафика в клиент-серверной информационной системе // Вестник НИИ СУВПТ/ Новосибирск, Изд. Сиб-ГУТИ, 2003 – С. 163-172.
5. Стешенко В.В. Исследование интернет-трафика пользователей корпоративной вычислительной сети Астраханского государственного технического университета // Вестник АсГТУ. Астрахань, 2008. – С. 130-132.

INCREASE IN THE SAFETY OF COMPUTER SYSTEMS AND NETWORKS ON THE BASIS OF THE ANALYSIS OF NET TRAFFIC

Azhmukhamedov I.M., Marjenkov A.N.

Annotation is proposed the schematic of an increase in the safety of computer systems and networks on the basis of the analysis of net traffic. To the advantages of this diagram they relate speed of response to the threats, the minimum use of computational of service lives of system, the absence of the need for the dismantling of packets and, as a result, independence from the signatures of harmful programs.

Keywords: *security, traffic, network, self-similarity, network anomalies, network attacks, IP packets, cyclical analysis, method of Holt, computer systems, modeling, forecasting.*

Ажмухамедов Искандар Маратович, к.т.н., доцент Кафедры «Информационная безопасность» Астраханского государственного технического университета (АсГТУ); E-mail: aim_agtu@mail.ru

Марьенков Александр Николаевич, аспирант АсГТУ; E-mail: _amar_@mail.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 334.764.47

ТРАНСФОРМАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ В МЕЖРЕГИОНАЛЬНЫХ КОМПАНИЯХ СВЯЗИ

Навойчик Л.М.

В статье дана оценка эффективности реорганизации межрегиональных операторов связи с позиций оптимизации бизнес-процессов компаний. Рассмотрены основные приоритеты их развития, предложены механизмы совершенствования процессов управления в условиях резкого роста конкурентоспособности рынка услуг связи.

Ключевые слова: реорганизация, процессы управления, рынок услуг связи.

Кардинальные изменения в жизни общества, связанные с его информатизацией, влекут за собой глобальную трансформацию корпоративной структуры как основной формы осуществления деятельности в современном обществе. Россия также не осталась в стороне от этих общемировых процессов. В отечественной телекоммуникационной отрасли происходят кардинальные перемены, вызванные стабилизацией экономической ситуации в стране, ростом качества услуг и развитием новых технологий в области связи, повышением интереса потенциальных инвесторов к телекоммуникационной индустрии. Внутренняя интеграция систем управления и бизнесов самой динамично развивающейся отрасли позволит существенно повы-