© Smirnov A., Dreis Yu., Danilenko D. Simulating model NIPDS for intrusion detection and prevention in telecommunication systems and networks // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 29-35.

ИМИТАЦИОННАЯ МОДЕЛЬ NIPDS ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Алексей Смирнов[1], Юрий Дрейс[2], Дмитрий Даниленко[1]

[1]Кировоградский национальный технический университет, Украина
[2]Житомирский военный институт им. С.П.Королева Государственного университета телекоммуникаций, Украина

СМИРНОВ Алексей Анатольевич, д.т.н.

Год и место рождения: 1977 год, г. Кировоград, Украина.
Образование: Харьковский военный университет, 1999 год.
Должность: профессор кафедры программного обеспечения с 2013 года.
Научные интересы: защита информации, телекоммуникационные системы и сети.
Публикации: больше 200 научных трудов, среди которых монографии, учебные пособия с грифом МОН Украины, научные статьи и патенты на изобретения.
E-mail: assa_s@mail.ru

ДРЕЙС Юрий Александрович, к.т.н.

Год и место рождения: 1984 год, сгт. Красноармейск, Житомирская область, Украина.
Образование: Житомирский военный институт радиоэлектроники, 2007 год.
Должность: доцент кафедры безопасности информационных и коммуникационных систем с 2013 года.
Научные интересы: защита информации с ограниченным доступом.
Публикации: больше 40 научных трудов, среди которых учебное пособие, методички, научные статьи и авторские свидетельства на компьютерные программы.
E-mail: dr_yr_al@mail.ru

ДАНИЛЕНКО Дмитрий Алексеевич

Год и место рождения: 1988 год, г. Коростень, Житомирская область, Украина.
Образование: Кировоградский национальный технический университет, 2009 год.
Должность: аспирант кафедры программного обеспечения с 2013 года.
Научные интересы: защита информации, телекоммуникационные системы и сети.
Публикации: 8 научных статей.
E-mail: dmitriy.danilenko@kiroe.com.ua

Аннотация. *В статье предложена имитационная модель NIDPS (Network-based Intrusion Detection and Prevention System) для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях. NIDPS использует пакет Wireshark для реализации процедур захвата и фильтрации трафика, процедуры статистической обработки данных сетевого трафика, проверки гипотез, обработки полученных результатов и принятия решения о наличии вредоносной сетевой активности, что позволяет адаптивно реагировать на текущую ситуацию, при необходимости блокировать подозрительный трафик и рассылать предупреждения соседним узлам сети, на рабочую станцию сетевого администратора, сервер протоколирования атак и т.д. Разработанная модель может быть интерпретирована как сенсорная и аналитическая часть элементарной сетевой системы обнаружения вторжений на основе статистического анализа.*

Ключевые слова: *защита информации, телекоммуникационные системы и сети, система обнаружения и предотвращения вторжений, имитационная модель.*

Введение

Для обеспечения безопасности современных телекоммуникационных сетей применяются т.н. системы обнаружения (Intrusion Detection System – IDS) и предотвращения (Intrusion Prevention System – IPS) вторжений (СОПВ) [1-6]. В основе их функционирования лежит сбор, анализ и обработка информации о событиях, связанных с безопасностью

защищаемой телекоммуникационной сети, накопление полученных данных, мониторинг сетевой активности отдельных служб и сервисов, принятие решения о состоянии защищаемой системы с выявлением и возможным протии-водействием несанкционированному использованию инфокоммуникационных ресурсов [2].

Важным направлением в совершенствовании СОПВ является исследование аномалий (Anomaly-Based Intrusion Detection and Prevention Systems – AB IDPS) телекоммуникационных систем, в основу которого может быть положен статистический анализ сетевого трафика [2]. При таком подходе СОПВ определяет «нормальную» сетевую активность отдельных служб и информационных сервисов телекоммуникационной системы, после чего весь трафик, не подпадающий под определение «нормального» помечается как «аномальный».

Функционирование статистических методов в СОПВ организовано следующим образом:

1. Производится первичный мониторинг сетевой активности телекоммуникационной системы. На основе результатов наблюдений за активностью сетевых служб и информационных сервисов в течении некоторого периода времени оцениваются показатели, характеризующие штатное функционирование телекоммуникационной системы, при этом выявляется т.н. «нормальный» сетевой трафик;

2. Вырабатываются статистические правила (критерии), по которым принимается решение о переходе телекоммуникационной системы в неустановленный (нештатный) режим функционирования. Правило принятия решений может базироваться на статистической проверке гипотезы об однородности наблюдаемого и выявленного ранее «нормального» сетевых трафиков. Разница между «нормальным» и «аномальным» событием определяется пороговой величиной (в случае проверки гипотез – критической областью);

3. Производится анализ сетевого трафика с поиском аномалии в установившейся картине «нормального» сетевого трафика. Всем пакетам дается оценка «аномальности» (включающая в себя степень отклонения отдельных показателей для специфического события) и если эта оценка выше определенного предела (лежит в критической области), СОПВ генерирует сигнал тревоги либо блокирует соответствующий процесс.

Главным преимуществом статистических методов в СОПВ является возможность изучать (мониторить) сетевой трафик и отличать «нормальную» сетевую активность от «аномальной». Кроме того, существует возможность самообучения, самонастраивания, т.е. первичный мониторинг сетевой активности телекоммуникационной системы может производится периодически (при отсутствии вторжений) с корректировкой пороговых величин и самих критериев принятия решений о переходе системы в неустановленный («аномальный») режим функционирования. Все это в совокупности делает статистическую СОПВ гораздо гибче сигнатурной, дает ей возможность без известных сигнатур вторжений обнаруживать и предотвращать новые, еще неизвестные атаки и сетевые вирусы.

Таким образом, ***целью*** данной работы есть построение СОПВ со статистическими методами обнаружения вторжений, что предполагает разработку надежных инструментов мониторинга сетевой активности, позволяющих с высокой точностью и достоверностью детектировать «нормальный» сетевой трафик и выявлять «аномальные» события. В работе разработана имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях, а также проводится статистический анализ сетевого трафика различных служб и информационных сервисов современных телекоммуникационных систем и сетей.

Основная часть исследования

Для проведения экспериментальных исследований статистических свойств сетевого трафика и обоснования практических рекомендаций по построению сетевых систем обнаружения вторжений (СОВ) и систем предотвращения вторжений (СПВ) разработана имитационная модель NIDPS (Network-based Intrusion Detection and Prevention System) для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях. Структурная схема имитационной модели приведена на рис. 1.

Разработанная имитационная модель содержит:

– блок генерации сетевого трафика, который предназначен для имитации потока данных в телекоммуникационной системе, как на подготовительном, так и на основном этапе функционирования NIDPS. В первом случае блок генерации сетевого трафика формирует шаблонные данные, во втором случае – имитирует работу отдельных служб и сервисов ТКС;

– имитаторы захвата и фильтрации сетевого трафика – имитируют соответствующие процедуры сетевого анализатора, т.е. производят первичную обработку сгенерированных блоком генерации данных. Имитаторы (1) обрабатывают поток шаблонных данных, имитаторы (2) – потоки данных отдельных служб и сервисов ТКС;

– блок статистической обработки предназначен для анализа отфильтрованных данных и формировании на его основе статистических портретов. Блок (1) обрабатывает шаблонные данные, блок (2) – потоки данных отдельных служб и сервисов ТКС;

– блок хранения данных сберегает статистические портреты шаблонных данных;

– блок проверки статистических гипотез предназначен для обработки статистических портретов шаблонных данных и потоков данных отдельных служб и сервисов ТКС. В результате обработки принимается или отвергается гипотеза об однородности обрабатываемых данных по каждой службе или сервису ТКС;

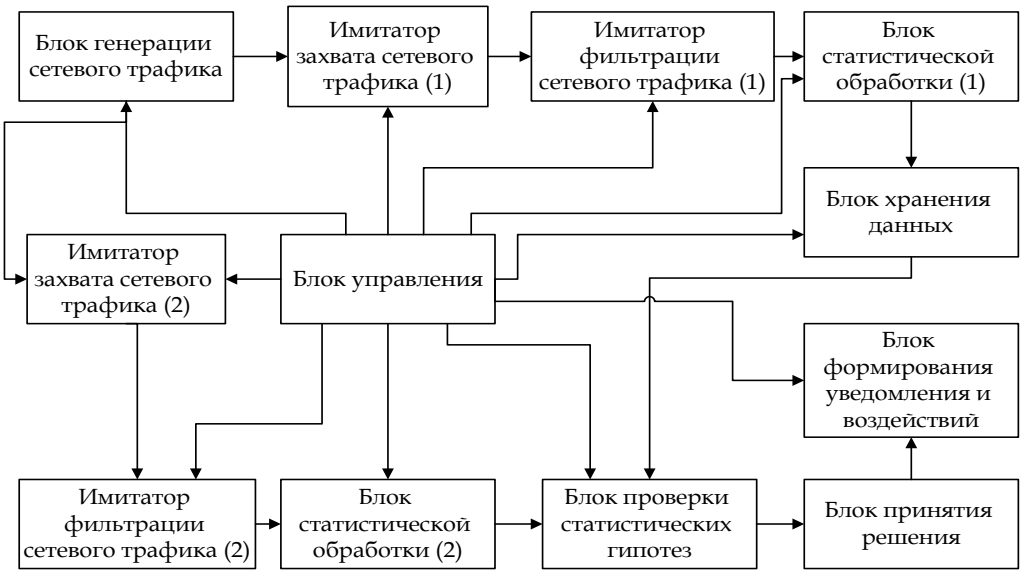

Рис. 1 Структурная схема имитационной модели NIDPS

– блок принятия решения на основании результатов проверки статистических гипотез обобщает и принимает решение о наличии или отсутствии вредоносного сетевого трафика и соответствующего вторжения;

– на основании принятого решения (в блоке принятия решения) в блоке формировании уведомления и воздействий осуществляется формирование управляющих воздействий (в случае обнаружения вторжения) и формируется уведомление для системного администратора (офицера безопасности) о текущем состоянии системы;

– блок управления осуществляет согласование работы остальных блоков имитационной модели NIDPS и управление основными вычислительными операциями.

В качестве блока генерации сетевого трафика может выступать отдельный узел компьютерной сети, при этом на вход соответствующего модуля подается весь трафик, который проходит через данный сегмент сети. Имитаторы захвата и фильтрации выполняют в этом случае анализ протокола передачи данных, фиксируют время и получают дополнительные параметры. Все пакеты агрегируется по заданному интервалу времени (например, 1 секунда), таким образом, формируется временной ряд: количество пакетов, полученных либо переданных за единицу времени. Этот ряд передается на следующий блок имитационной модели NIDPS.

Таким образом, разработанная имитационная модель может адаптивно реагировать на текущую ситуацию и при необходимости (в зависимости от параметров настройки) блокировать подозрительный трафик и рассылать преду-преждения соседним узлам сети (один из видов управляющих воздействий), на рабочую станцию сетевого администратора, сервер протоколирования атак и т.д.

Разработанная имитационная модель NIDPS может быть интерпретирована как сенсорная и аналитическая часть элементарной сетевой системы обнаружения вторжений на основе статистического анализа. Широко известны системы обнаружения вторжений, которые развивают подобную концепцию (статистический анализ) и успешно выполняют свои задачи (Например, IDES, NIDES, Snort и др) [3]. Однако разработанную имитационную модель можно использовать и в другом, более простом и узком контексте: как компонент антивирусной системы, либо как отдельный модуль системы, формирующий предупреждение о сетевой опасности (вторжении) прямо на рабочую станцию конечного пользователя, т.е. как СОВ отдельных станций (HIPS).

Наиболее сложный в техническом исполнении элемент предлагаемой имитационной модели NIDPS является захват и фильтрация трафика. Для реализации данной функции использован специальный пакет Wireshark [3]. Одной из возможных опций этого пакета является настройка параметров перехвата, они включают в себя возможность фильтрации. Для каждого сервиса подбирается специальный фильтр с настройками захвата трафика для протоколов HTTP с использованием Wireshark (рис. 2). По выбранному фильтру и опциям пакет Wireshark осуществляется захват информационного трафика, что приведено (рис. 3) на примере его функционирования.

Таким образом, разработанная имитационная модель использует пакет Wireshark для реализации процедур захвата и фильтрации трафика, процедуры статистической обработки данных сетевого трафика, проверка гипотез, обработка полученных результатов и принятие решения о наличии вредоносной сетевой активности реализованы в отдельном программном модуле, листинг кода программы приведен в приложении.

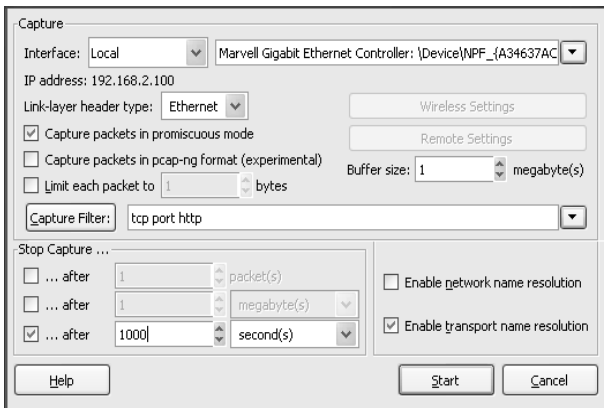

Рис. 2 Пример настроек фильтра захвата HTTP трафика

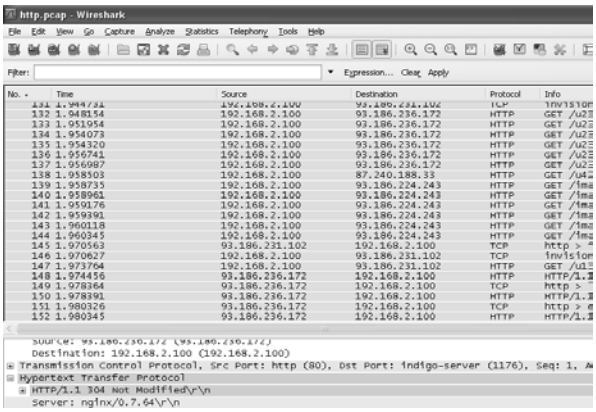

Рис. 3 Пример захвата информационного трафика

Разработанная программная реализация позволяет осуществлять статистический анализ данных сетевого трафика и проводить соответствующие экспериментальные исследования. Ниже приводятся полученные статистические портреты и результаты проведенных экспериментальных исследований.

Результаты экспериментальных исследований статистических свойств сетевого трафика

Для проведения экспериментальных исследований свойств сетевого трафика были использованы эмпирические данные, полученные в результате работы программного анализатора (снифера) Wireshark. Выбор этого программного сетевого анализатора связан с возможностью перехвата трафика сетевого интерфейса в режиме реального времени.

В ходе практических замеров с использованием снифера Wireshark оценивался объем данных, передаваемых через компьютерную сеть за определённый период времени. Замеры трафика, т.е. объема информации, передаваемого в единицу времени, проводились как по числу пакетов, так и по числу бит данных. При этом эмпирические данные были получены и обобщены не менее чем по 100 000 временным отсчетам.

В качестве исходных данных при проведении экспериментальных исследований были использованы различные телекоммуникационные службы и информационные сервисы, а именно [3-6]:

– FTP (File Transfer Protocol – протокол передачи файлов) – стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга;

– HTTP (HyperText Transfer Protocol – «протокол передачи гипертекста») – протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов в формате HTML). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом;

– электронная почта (email, e-mail, от англ. electronic mail) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети;

– Skype – бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую связь и видеосвязь через Интернет между компьютерами (IP-телефония), опционально используя технологии пиринговых сетей, а также платные услуги для звонков на мобильные и стационарные телефоны;

– YouTube – сервис, предоставляющий услуги видеохостинга, т.е. доступа к сайтам, позволяющим загружать и просматривать видео в браузере, например, через специальный проигрыватель. При этом большинство подобных сервисов не предоставляют видео, следуя таким образом принципу «User-generated content». Видеохостинг стал наиболее популярен в связи с распространением широкополосного доступа в Интернет и развитием (удешевлением) носителей больших объемов информации (жёстких дисков).

Примеры полученных гистограмм сетевого трафика при загрузке данных с сервиса YouTube (720p) приведены на рис. 4 (трафик представлен в виде числа пакетов, переданных в единицу времени) и на рис. 5 (трафик представлен в виде числа бит данных, переданных в единицу времени). На рис. 6 и рис. 7 приведены соответствующие примеры полученных гистограмм сетевого трафика при загрузке данных с сервиса YouTube (360p). Рисунки 8 и 9 соответствуют гистограммам сетевого трафика, полученного при использовании сервиса Skype в случае передачи только звуковых сообщений (voice). На рис. 10 и 11 приведены примеры гистограмм трафика Skype при передачи видеосигналов.

Примеры гистограмм трафика, полученного при использовании услуг электронной почты (E-mail), приведены на рис. 12 и 13. Рисунки 14 и 15 иллюстрируют гистограммы трафика HTTP, а на рис. 16, 17 приведены соответствующие гистограммы трафика FTP.

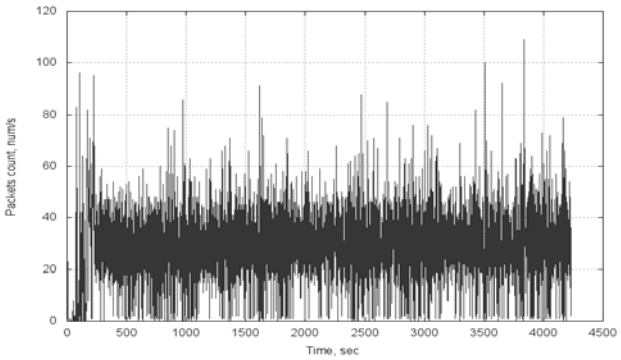

Рис. 4 Фрагмент полученной гистограммы сетевого трафика при загрузке данных с сервиса YouTube (720p, пакет/с)

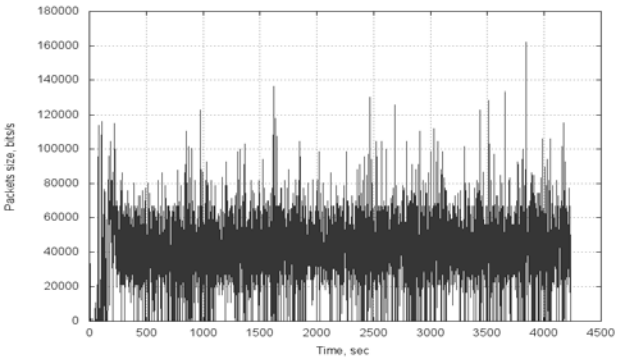

Рис. 5 Фрагмент полученной гистограммы сетевого трафика при загрузке данных с сервиса YouTube (720p, бит/с)

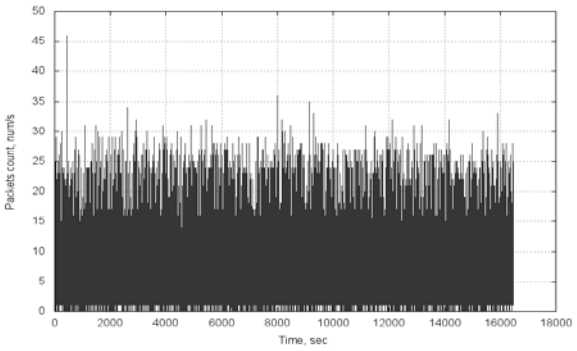

Рис. 6 Фрагмент полученной гистограммы сетевого трафика при загрузке данных с сервиса YouTube (360p, пакет/с)

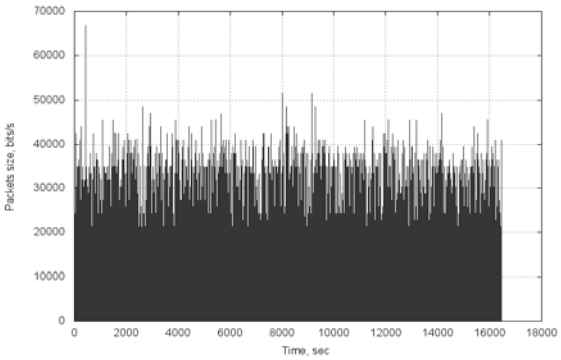

Рис. 7 Фрагмент полученной гистограммы сетевого трафика при загрузке данных с сервиса YouTube (360p, бит/с)

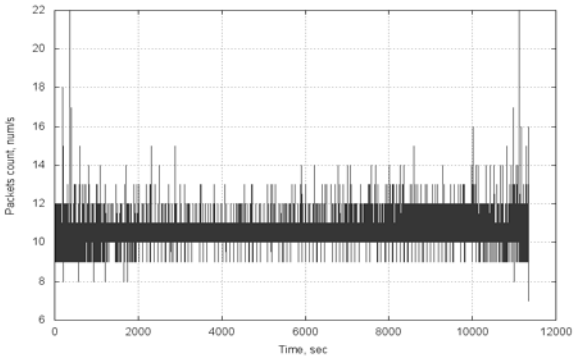

Рис. 8 Фрагмент полученной гистограммы сетевого трафика при обмене данными с использованием Skype (voice, пакет/с)

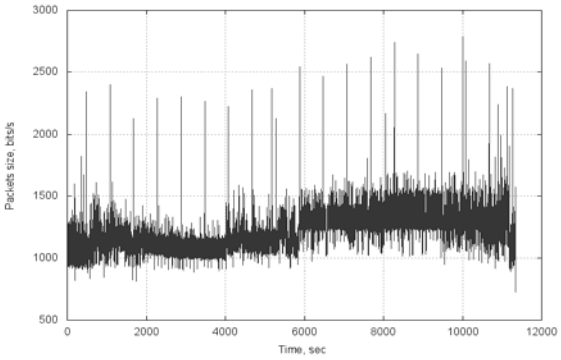

Рис. 9 Фрагмент полученной гистограммы сетевого трафика при обмене данными с использованием Skype (voice, бит/с)

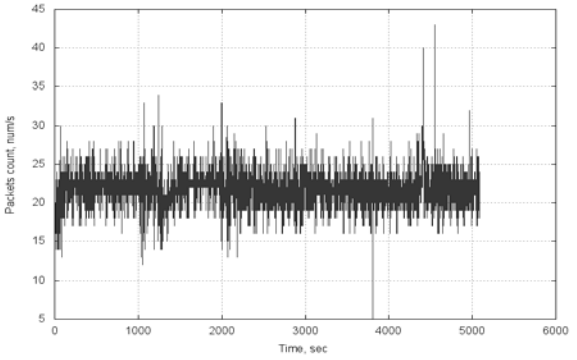

Рис. 10 Фрагмент полученной гистограммы сетевого трафика при обмене данными с использованием Skype (video, пакет/с)

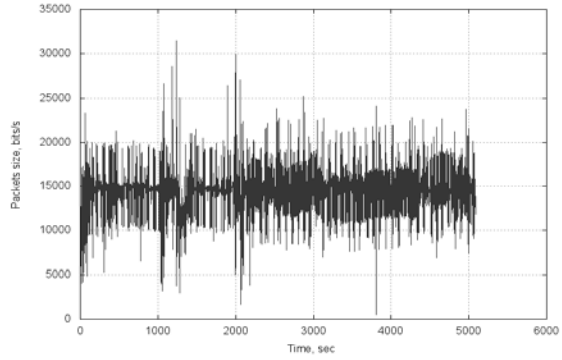

Рис. 11 Фрагмент полученной гистограммы сетевого трафика при обмене данными с использованием Skype (video, бит/с)

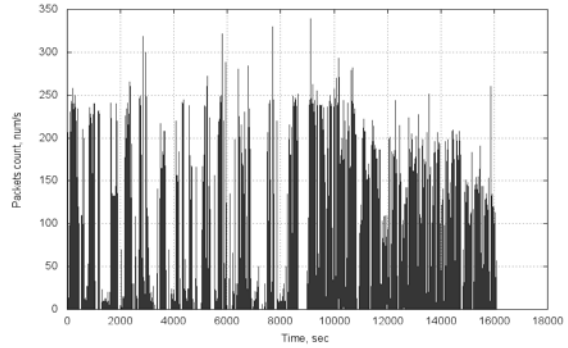

Рис. 12 Фрагмент полученной гистограммы сетевого трафика при передаче электронной почты (пакет/с)

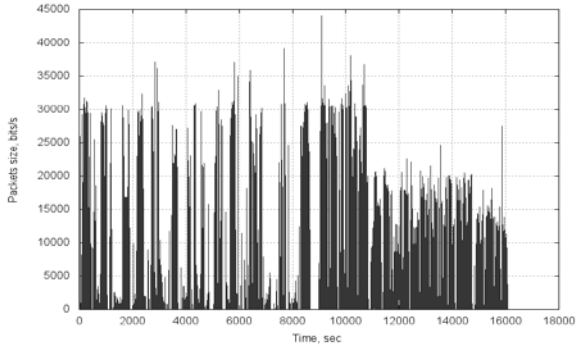

Рис. 13 Фрагмент полученной гистограммы сетевого трафика при передаче электронной почты (бит/с)

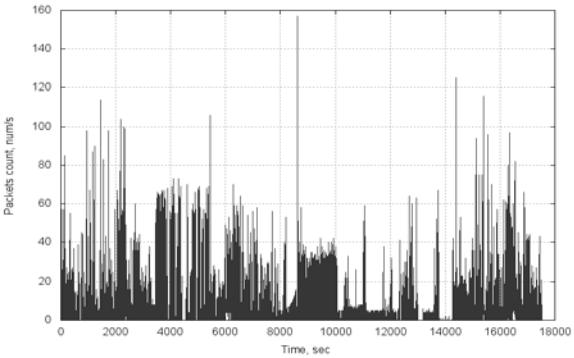

Рис. 14 Фрагмент полученной гистограммы сетевого трафика при передаче данных с использованием протоколов HTTP (пакет/с)

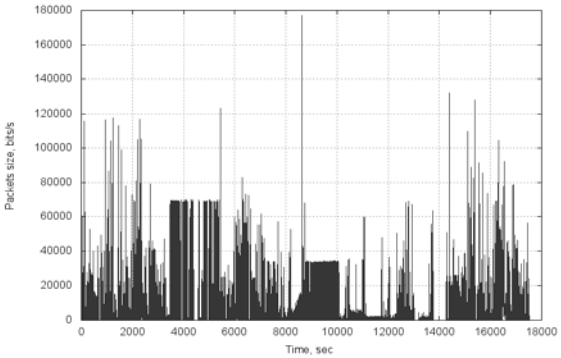

Рис. 15 Фрагмент полученной гистограммы сетевого трафика при передаче данных с использованием протоколов HTTP (бит/с)

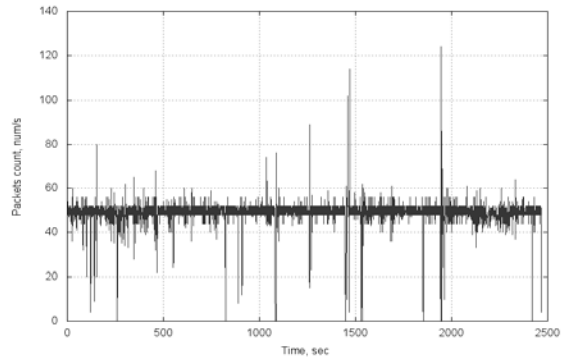

Рис. 16 Фрагмент полученной гистограммы сетевого трафика при передаче данных с использованием протоколов FTP (пакет/с)

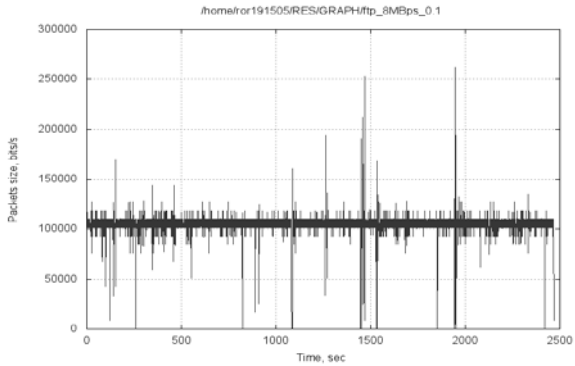

Рис. 17 Фрагмент полученной гистограммы сетевого трафика при передаче данных с использованием протоколов FTP (бит/с)

Выводы

Методы статистического анализа сетевого трафика используются в качестве основной вычислительной компоненты современных сетевых СОВ и СПВ для мониторинга сетевой активности и детектирования вредоносного сетевого трафика. В ходе проведения исследований разработана имитационная модель NIDPS (Network-based Intrusion Detection and Prevention System) для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях. Разработанная имитационная модель позволяет адаптивно реагировать на текущую ситуацию и при необходимости (в зависимости от параметров настройки) блокировать подозрительный трафик и рассылать предупреждения соседним узлам сети, на рабочую станцию сетевого администратора, сервер протоколирования атак и т.д.

При моделировании сетевых СОВ и СПВ в ТКС наиболее сложный в техническом исполнении элемент захвата и фильтрации трафика реализован с использованием специального пакета Wireshark. Разработана также программная реализация, которая позволяет осуществлять статистический анализ данных сетевого трафика и проводить соответствующие экспериментальные исследования. При проведении экспериментальных исследований свойств сетевого трафика были использованы эмпирические оценки объемов данных, передаваемых через компьютерную сеть за

определённый период времени. В качестве исходных данных при проведении экспериментальных исследований использованы различные телекоммуникационные службы и информационные сервисы, а именно: протоколы FTP и HTTP, электронная почта, Skype, YouTube.

Литература

[1] Карпук Н.М. Статистический анализ сетевого трафика. Электронная библиотека Белорусского государственного университета. — 2008. — С. 116-119.

[2] NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). — Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg. — 127 p. (February 2007).

[3] Brian Caswell, Jay Beale, Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. — Syngress Media, U.S. 2006.

[4] Ушаков Д.В. Развитие принципов функционирования систем обнаружения сетевых вторжений на основе модели защищенной распределенной системы: дис. канд. техн. наук: 05.13.19. — Москва, 2005. — 175 с.

[5] Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. — М., 2008. — Т. II: Средства защиты в сетях. — 558 с.

[6] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2010. — 944 с.

УДК 004.056.57 (045)

Смірнов О.А., Дрейс Ю.О., Даниленко Д.О. Імітаційна модель NIPDS для виявлення та запобігання вторгнень в телекомунікаційних системах і мережах

Анотація. *У статті запропонована імітаційна модель NIDPS (Network-based Intrusion Detection and Prevention System) для виявлення і запобігання вторгнень в телекомунікаційних системах і мережах. NIDPS використовує пакет Wireshark для реалізації процедур захоплення і фільтрації трафіку, процедури статистичної обробки даних мережевого трафіку, перевірки гіпотез, обробки отриманих результатів та прийняття рішення про наявність шкідливої мережевої активності, що дозволяє адаптивно реагувати на поточну ситуацію, при необхідності блокувати підозрілий трафік і розсилати попередження сусіднім вузлам мережі, на робочу станцію адміністратора, сервер протоколювання атак і т.д. Розроблена модель може бути інтерпретована як сенсорна і аналітична частина елементарної мережевої системи виявлення вторгнень на основі статистичного аналізу.*

Ключові слова: *захист інформації, телекомунікаційні системи та мережі, система виявлення і запобігання вторгнень, імітаційна модель.*

Smirnov A., Dreis Yu., Danilenko D. Simulating model NIPDS for intrusion detection and prevention in telecommunication systems and networks

Abstract. *The paper proposes a simulation model NIDPS (Network-based Intrusion Detection and Prevention System) for intrusion detection and prevention in telecommunication systems and networks. NIDPS package uses Wireshark to capture and implement procedures to filter traffic, the procedures of statistical data processing network traffic, testing hypotheses, processing the results and the decision of a malicious network activity that allows adaptively respond to the current situation, if necessary, to block suspicious traffic and send warning neighboring nodes in the network, the workstation network administrator logging server attacks, etc. The developed model can be interpreted as sensory and analytical part of the elementary network intrusion detection system based on statistical analysis.*

Key words: *protection of information, telecommunication systems and networks, system intrusion detection and prevention, imitating model.*

Отримано *25 лютого 2014 року*, затверджено редколегією *19 березня 2014 року*