УДК 681.3

Л. М. Груздева, К. Г. Абрамов, Ю. М. Монахов

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ С АДАПТИВНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Проанализированы результаты экспериментальных исследований производительности корпоративной сети передачи данных в условиях функционирования системы защиты информации, оперативно изменяющей настройки своих параметров под действием информационных атак.

Ключевые слова: *сеть передачи данных, производительность, система защиты информации, информационные атаки.*

Введение. Эффективная эксплуатация корпоративных сетей передачи данных (КСПД) в условиях воздействия информационных атак, их проектирование и модернизация невозможны без оценки показателей качества функционирования, одним из которых является производительность сети.

Анализ работ, посвященных изучению КСПД, и опыт практических исследований позволяют констатировать резкое снижение производительности в условиях воздействия информационных атак. Современные системы защиты (СЗИ) в известной степени решают данную проблему за счет частичного блокирования вредоносного трафика (ВТ), но обеспечение высокой вероятности обнаружения и задержки, связанные с противодействием, ведут к значительному расходованию ресурсов сетей, что в конечном итоге сопровождается снижением их производительности.

Экспериментально было выявлено, что отключение ряда средств противодействия (СП) не вызывает значительного снижения показателя защищенности КСПД, в то время как уменьшается средняя задержка обмена информацией.

В настоящей статье представлены результаты экспериментальных исследований характеристик производительности сети, функционирующей в условиях воздействия информационных атак, и адаптивной СЗИ, реализуемой на основе алгоритмов раннего и достоверного обнаружения информационных атак [1] и оперативного инициирования СП только в наиболее уязвимых узлах КСПД [2].

Экспериментальная установка. Схема сети представлена на рис. 1. Сеть состоит из двух сегментов, объединенных коммутатором: пять компьютеров моделируют подсеть, на которую непосредственно были организованы атаки, остальные три компьютера были задействованы для служебных нужд и как компоненты консоли распределенной сетевой системы обнаружения вторжений D-NIDS (Distributed Network IDS). Основные характеристики используемого оборудования представлены ниже.

1. Рабочая станция — Intel Core2 Duo CPU E8400 3 Гц, 2 ГБ RAM DDR2, HDD 256 ГБ.
2. Виртуальная рабочая станция — Virtualbox 3, PCnet-Fast3, 128 МБ RAM.
3. Сетевое оборудование — Intel Express 330T Hub, Compex PS2208B, кабель UTP-5.

Исследуемая сеть строилась на базе концентраторов (все компьютеры образуют единый домен коллизий, благодаря чему передающиеся по сети пакеты определяются сенсорами IDS). Для увеличения количества узлов сети были использованы инструменты виртуализации: на каждом компьютере были развернуты по три виртуальные машины, работающие под управлением MS WindowsXP. В качестве платформы для виртуализации

выбрана Sun VirtualBox3. Конфигурации программного обеспечения (ПО) всех виртуальных рабочих станций и сенсоров IDS одинаковы.

В качестве сенсоров созданной D-NIDS выбран Snort IPRoute2. Сведения о выявленных атаках хранятся сервером баз данных, на этом же компьютере установлено ПО для синхронизации времени всех узлов сети. В качестве СУБД использован MySQL-сервер версии 5.0.

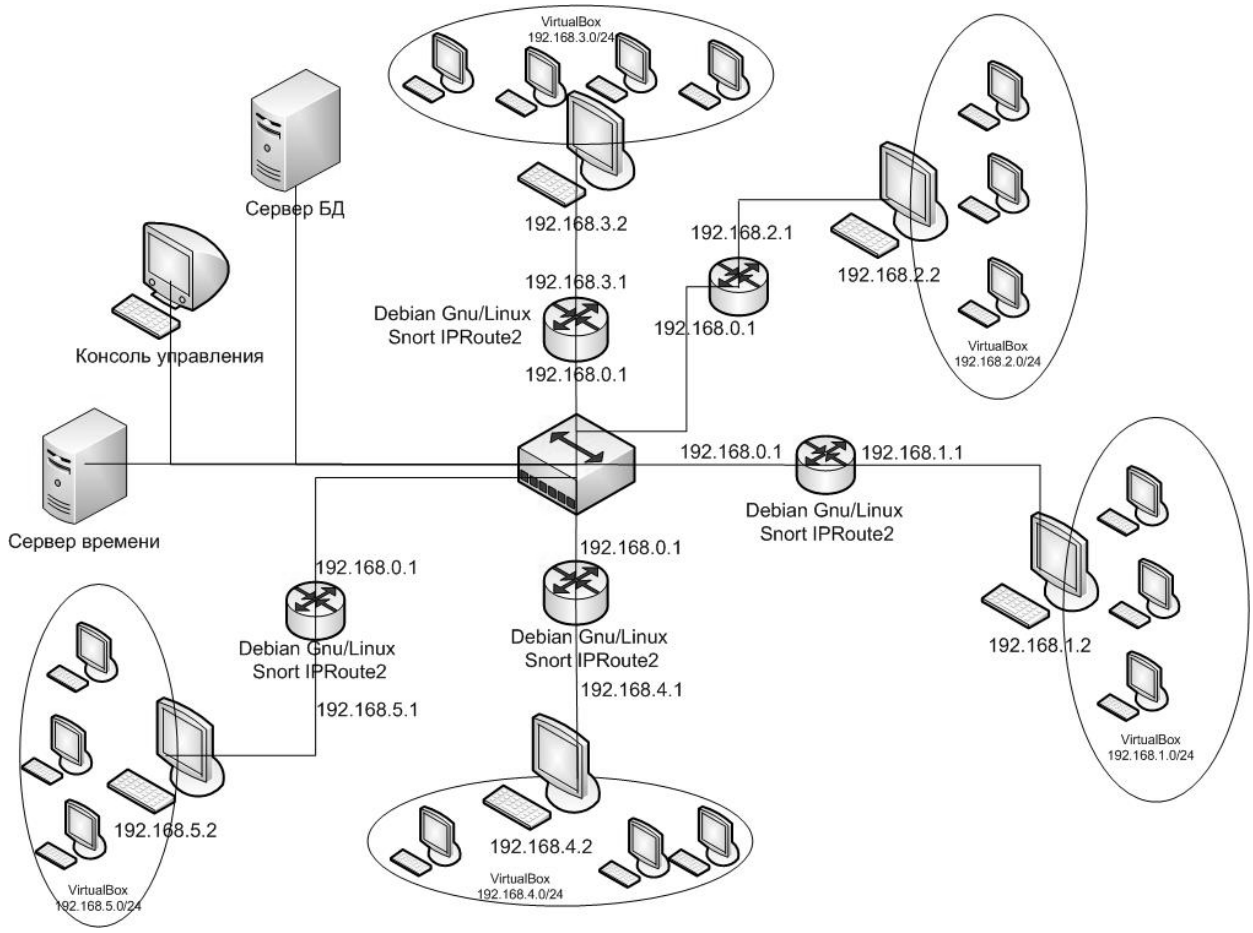

Рис. 1

Результаты и анализ экспериментальных исследований. В статье [3] рассмотрены результаты экспериментов по исследованию характеристик производительности КСПД, характеризующейся передачей больших объемов трафика в условиях воздействия угроз ИБ. Рассмотрим эксперимент по оптимизации СЗИ в сети. График изменения производительности в сети в условиях воздействия ВТ и динамического построения адаптивной СЗИ представлен на рис. 2.

Вредоносный трафик в системы стал поступать с 10-й секунды. Производительность сети с этого момента стала падать. В отсутствие СЗИ (кривая *1*) среднее время задержки пакета t_3 возросло до 0,33 с (производительность упала приблизительно в 6 раз за 40 с). В условиях типовой СЗИ (кривая *2*, в каждом узле типовой комплект) среднее время задержки возросло до 0,28 с, и после того как СЗИ блокировала ВТ (приблизительно на 50 с) оно уменьшилось до 0,18 с (производительность по сравнению с исходным вариантом снизилась примерно в 3 раза, что может обеспечить нормальное функционирование корпоративной сети).

Наилучший вариант, приводящий к снижению производительности всего лишь в 2 раза (кривая *3*), обеспечивается следующими механизмами: за счет использования алгоритма „критическая область угроз“ [1] снижается время обнаружения ВТ (примерно на 20 %), с помощью алгоритма расстановки СЗИ в узлах сети [2] в максимальный режим включается лишь

часть узлов СЗИ. В данном эксперименте вместо пяти СЗИ, функционирующих в максимальном варианте защиты, процедура подключила только три.

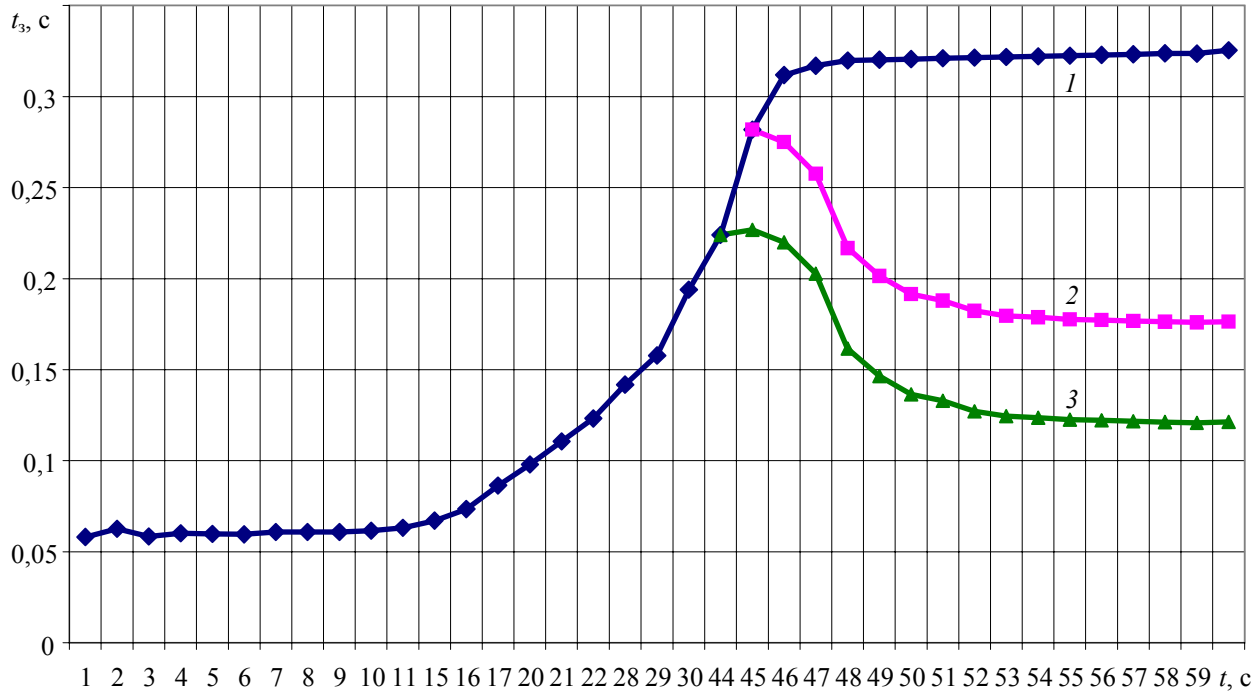

Рис. 2

Выводы. Раннее обнаружение информационных атак (результаты экспериментов показали снижение времени обнаружения на 20—25 % по сравнению с традиционными логическими схемами обнаружения угроз ИБ) позволяет оперативно использовать средства противодействия угрозам ИБ в наиболее уязвимых узлах КСПД. В результате производительность КСПД в условиях воздействия угроз ИБ остается на требуемом уровне (снижение не более чем в 2 раза), что обеспечивает нормальное функционирование корпоративной сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Груздева Л. М., Монахов М. Ю.* Алгоритм раннего обнаружения атак на информационные ресурсы АСУП // Автоматизация в промышленности. 2008. № 3. С. 12—14.

2. *Груздева Л. М., Монахов М. Ю.* Алгоритм оптимизации функционирования распределенной системы защиты // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. техн. и естеств. науки „Системный анализ. Теория и практика“. 2008. Т. 14, № 2. С. 80—82.

3. *Груздева Л. М., Монахов Ю. М., Монахов М. Ю.* Экспериментальное исследование производительности корпоративной телекоммуникационной сети // Проектирование и технология электронных средств. 2009. № 4. С. 21—24.

Сведения об авторах

Людмила Михайловна Груздева — канд. техн. наук; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: glm@vlsu.ru

Константин Германович Абрамов — аспирант; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: abramovk@vlsu.ru

Юрий Михайлович Монахов — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: unclefck@gmail.com

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.