УДК 004.7

Е.А. Басыня, Г.А. Французова, А.В. Гунько

Самоорганизующаяся система управления трафиком вычислительной сети

Предлагается один из возможных подходов к формированию самоорганизующейся системы управления трафиком вычислительной сети, основанной на оригинальных методах противодействия сетевым угрозам и обеспечения конфиденциальности информационных потоков корпоративной сети. Метод противодействия сетевым угрозам представлен в виде этапов, выполнение которых позволяет идентифицировать злоумышленника и защитить информационный ресурс. Метод обеспечения конфиденциальности информационных потоков корпоративной сети предполагает формирование распределенной многоуровневой системы шифрования с обеспечением безопасности информационных процессов и процедуры их электронной автоматизации. Реализация самоорганизующейся системы управления трафиком вычислительной сети на основе представленных методов предполагает использование определенных инструментариев и включает в себя три основных блока: прогнозирования и фальсификации серверных решений, корпоративных серверов. Представлены результаты экспериментов по идентификации систем защиты и уязвимостей (посредством механизмов сканирования и зондирования), дешифровке внутренних информационных потоков локальной вычислительной сети предприятия, устойчивости к распределенным сетевым атакам (в том числе и на отказ в обслуживании) в сравнительном анализе с существующими решениями. Предложенные методы обеспечения информационной безопасности показали высокую эффективность и стабильность.

Ключевые слова: самоорганизующаяся система управления трафиком вычислительной сети, прогнозирование, фальсифицирование, генетическая алгоритмизация, нечеткая логика, сканирование, зондирование, межсетевой экран, распределенные сетевые атаки.

Необходимость защиты информационных процессов и процедуры их электронной автоматизации является одной из приоритетных задач современных IT-технологий. Сегодня крупные преступления совершаются, в том числе, с использованием глобальной сети Интернет. Практически все государственные структуры и частные организации имеют доступ в эту сеть, защищая свои информационные потоки межсетевыми экранами, криптографическими средствами и антивирусным программным обеспечением, функционирующими на основе «жесткой» логики. Однако при определенных временных затратах и вычислительных мощностях любая информационная система может быть взломана или выведена из состояния доступности [3]. Задействовав механизмы сканирования, зондирования и дешифрования, злоумышленник может идентифицировать продукт защиты атакуемого объекта, а так же получить перечень уязвимостей объекта с информацией по их использованию. Уязвимость стека протоколов TCP/IP и запрограммированная «жесткая» логика различных аппаратно-программных средств управления и защиты трафика обусловливают необходимость сопровождения сектора информационно-коммуникационных технологий предприятия квалифицированными техническими специалистами. Еще одним фактором в вопросе обеспечения информационной безопасности является потенциальная возможность нахождения злоумышленника из числа доверенных пользователей корпоративной сети, в том числе из штата IT-специалистов. Исследованиями в области методов обнаружения аномальной активности сетевого трафика и обеспечения информационной сетевой безопасности занимаются российские и зарубежные ученые Р.Н. Селин, R. Lippmann, R. Kwitt, A. Ghosh, В.А. Артамонов, Д.Ю. Гамаюнов, И.М. Ажмухамедов и др. [1, 4, 6, 7]. Но при введении криптографических протоколов, либо элементарного дробления пакетов для сокрытия их типа (как, например, организовано в Tor-сетях) данные методы не дают однозначного результата – обнаружения аномальной активности сетевого трафика. Вследствие чего вытекает актуальность разработки методов противодействия сетевым угрозам и обеспечения информационной безопасности трафика предприятия.

Целью данной работы является разработка методов, которые будут составлять основу самоорганизующейся системы управления трафиком вычислительной сети (ССУ) [8].

Ключевой задачей является разработка методов противодействия сетевым угрозам и обеспечение конфиденциальности информационных потоков распределенных вычислительных сетей корпоративного уровня.

Научная новизна данной работы заключается в разработке методов и самоорганизующегося аппарата управления трафиком вычислительной сети, обладающим свойствами динамической адаптации, оптимизации, автономности, отказоустойчивости высшего класса и обеспечивающим высокий уровень информационной безопасности с пресечением возможности прогнозирования стратегии реагирования. Суть предлагаемого подхода описывается в данной работе.

I. Метод противодействия сетевым угрозам. При разработке ССУ предлагается использовать следующий метод противодействия сетевым угрозам, использующий аппарат генетической алгоритмизации и нечеткой логики, предполагающий последовательное выполнение следующих операций:

1. Первоначальное сканирование топологии и конфигурации сети.

2. Конфигурирование базовых правил системы управления трафиком с учетом текущей политики безопасности.

3. Развертывание блоков прогнозирования и фальсифицирования:

3.1. Установка, конфигурирование изолированных виртуальных серверов.

3.2. Анализ установленных экземпляров (см. п. 3.1), для межсетевого экрана (на рис. 1 обозначен буквой *A*) подготавливаются конфигурационные файлы имитации информационных систем.

4. Установка для сторонних соединений ССУ модели реагирования, выбранной блоком генетической алгоритмизации [5] из выборки п. 3.2 на определенный интервал времени (итерации по истечении).

5. Произведение системой динамического сигнатурного анализа трафика с идентификацией попыток сканирования, зондирования и взлома. В случае обнаружения подозрительной сетевой активности – производится оценка степени угрозы, реагирование:

5.1. В случае низкой степени угрозы – подключение блока генетической алгоритмизации, состоящей из трех категорий рулеток (объектов, групп и классов объектов). Имитация выбранного алгоритмом серверного решения из п. 3.2.

5.2. В случае высокой степени угрозы – реагирование блока нечеткой логики с фальсификацией серверного решения: переренаправление соединения на изолированную серверную модель определенного типа, отслеживание дальнейших действий злоумышленника. Одновременное самообучение ССУ с генерацией новых сигнатур. Аналогичный метод применяется для имитации состояния «зависания» с целью выявления вредоносных узлов.

6. Трассировка и идентификация хостов-злоумышленников и дальнейшее их внесение в черный список с временной блокировкой.

7. Систематическая самореорганизация системы с предварительной проверкой решений на ее моделях.

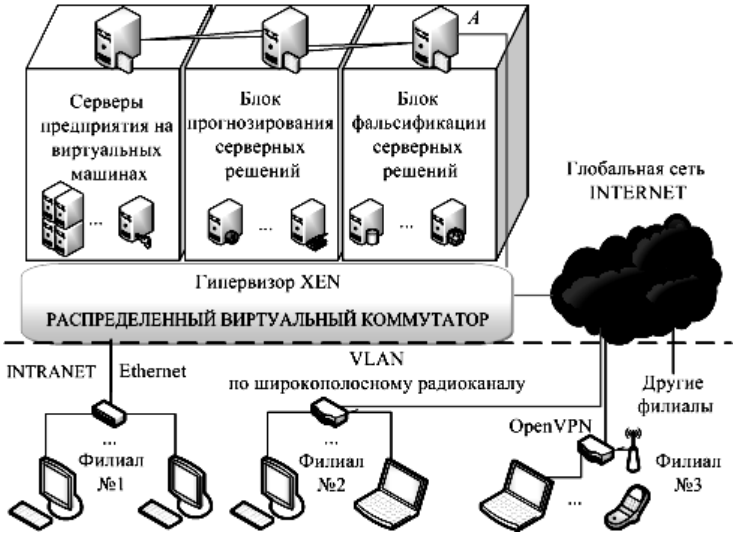

Рис. 1. Общая схема функционирования ССУ в корпоративной распределенной сети

Каждый уровень включает содействующие методы и детализированные алгоритмы действий.

Как представлено на рис. 1, ССУ состоит из трех блоков: прогнозирования, фальсификации серверных решений и корпоративных серверов предприятия на виртуальных машинах. Соответственно взаимодействуют три межсетевых экрана, главный обозначен буквой *A*.

Спроектированная таким образом ССУ способна автономно видоизменять существующие и создавать новые алгоритмы, исходя из накопленного опыта и изолированных тестирований на собственных моделях.

II. Метод обеспечения конфиденциальности информационных потоков корпоративной сети. Злоумышленник из числа доверенных пользователей, в том числе и со стороны провайдера, может попытаться перехватить потоки информации посредством снифферов (сканированием и зондированием в режиме сетевого интерфейса – неразборчивый захват).

Для минимизации данной возможности авторами предлагается метод обеспечения конфиденциальности информационных потоков корпоративной сети, в основу которого заложена распределенная самоорганизующаяся система шифрования. Данная идея появилась при изучении «луковой маршрутизации» tor-сетей [10], созданных для анонимизации в сети Интернет. При этом программная основа и принцип шифрования реализованным, более безопасным способом.

Метод включает в себя выполнение следующих этапов:

1. В пространстве блока виртуальных серверов (см. рис. 1) устанавливается и конфигурируется доверенный удостоверяющий центр сертификации корпоративной сети (ЦС).

2. Через групповые политики или «вручную» на рабочих станциях разворачивается клиентская часть;

3. Посредством нечеткой логики ЦС конфигурирует протокол взаимодействия с хостами в рамках данной корпоративной сети, составляет список доверенных узлов, синхронизирует его с клиентской частью;

4. Обмен данными происходит в следующей последовательности:

4.1. Узел по блоку генетической алгоритмизации [5] выбирает N-количество доверенных узлов.

4.2. Убеждается, что данные хосты еще являются доверенными в рамках данной корпорации (согласование по закрытому протоколу с ЦС).

4.3. На каждый сеанс связи узел-отправитель обменивается с хостами [1; N] новой парой ключей.

4.4. Начиная с ключа N до 1-го узел-отправитель шифрует пакеты, инкрементируя содержимое таким образом, чтобы каждый участник взаимодействия мог дешифровать лишь свою часть и просмотреть информацию о следующем адресе пересылки.

4.5. Система фрагментирует пакеты и в допустимых рамках изменяет флаги дейтаграмм (для сокрытия типа содержимого и усложнения анализа).

4.6. Происходит путешествие пакета с пошаговом дешифрованием, и лишь последний узел декапсулирует пакет окончательно и по зашифрованному каналу (например, https поверх vpn) передает информацию и прогоняет ответ по той же цепочке).

5. Блок нечеткой логики производит систематический анализ сетевого трафика на автомодельность. Далее, в зависимости от результатов, генерирует фальшивый p2p трафик, усложняющий дешифровку трафика злоумышленным хостом.

При использовании данного метода попытки дешифровки информационных потоков и деанонимизации источника являются нерентабельной задачей (временные издержки и стоимость привлеченных технических и других средств значительно превышают выгоду от дешифрованного потока информации одного случайного источника за малый период времени).

III. Инструментарий ССУ. Реализация самоорганизующейся при выполнении п. 5 разд. 2 системы управления трафиком вычислительной сети [9] на основе предложенного подхода предполагает использование определенного инструментария. В качестве такого средства может выступать ОС CentOS 6.x с пакетным фильтром iptables на базе Netfilter с POM (Patch-o-matic, сценариями, выполняющими наложение заплат на ядро ОС) и трассировщиком соединений, СУБД PostgreSQL, а блоки прогнозирования и реагирования реализованы на гипервизоре XEN.

ССУ состоит из трех блоков: прогнозирования, фальсификации серверных решений и корпоративных серверов на виртуальных машинах. Взаимодействуют три межсетевых экрана, главный из которых обозначен буквой А на рис. 1.

Аппарат нечеткой логики и генетической алгоритмизации функционирует во всех 3 составляющих, их преимущество в данном случае – работа без большой начальной выборки и способность выходить на глобальный экстремум решения, минуя локальные, сохраняя достаточную пропускную способность канала [2].

При данной реализации разработанная система [9] имеет возможность самообучаться и менять свою конфигурацию, обеспечивая высокий уровень информационной безопасности с отсутствием

возможности прогнозирования стратегии реагирования как с локальной сети предприятия, так и «извне». Тем самым человеческий фактор сводится к минимуму.

Результаты экспериментов. Один из вариантов самоорганизующейся системы управления трафиком вычислительной сети на основе предложенного подхода был реализован и проведен анализ эффективности его работы. С этой целью было проведено более 100 итераций сканирования ССУ (с установленным параметром реагирования блока фальсификации до 20% на обнаруженные процессы сканирования) посредством программ XSpider, LanGuard, ShadowSecurityScanner, X-Scan с параллельным использованием в каждой итерации средств зондирования GcodePRO, ZondGuard (результаты представлены на рис. 2).

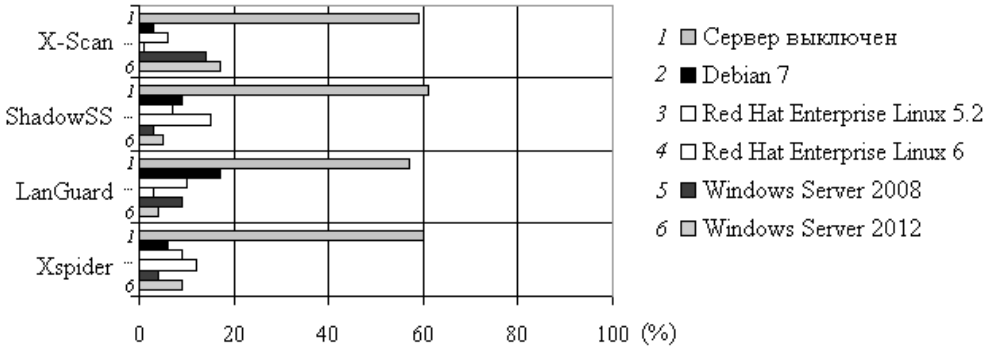

Рис. 2. Диаграмма идентификации операционных систем сервера сканерами и зондерами

В ходе эксперимента ССУ выдержала порог фальсификации серверных решений в 20% (имитируя Windows Server 2012, 2008, Red Hat Enterprise 6, 5.2, Debian 7), в остальных 80% злоумышленного сканирования информационная система представлялась выключенной.

Далее, при проведении 153 распределенных сетевых атак с различными модификациями типов вторжений от 760 зараженных узлов (на рис. 3 временной интервал от 0 до 50 с), рассматриваемые средства защиты (ССУ, Kerio Control 8, Outpost Network Security 3.2, Traffic Inspector 2 – функционирующие на идентичной аппаратной платформе) дали результат, показанный на рис. 3.

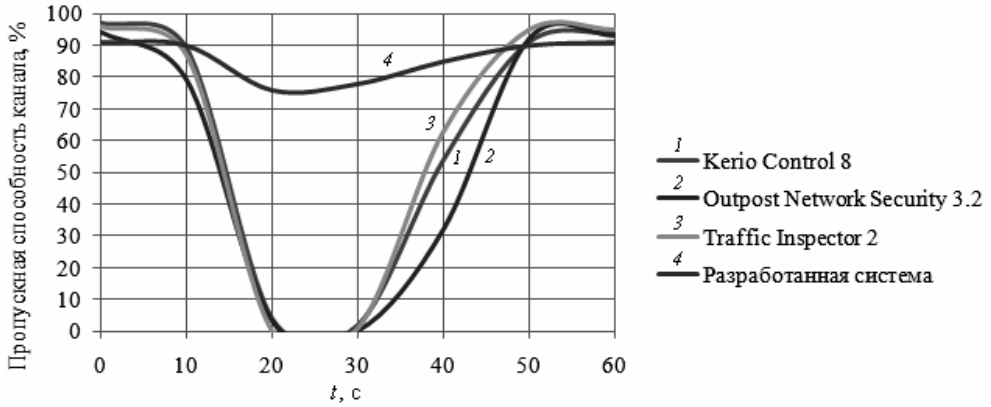

Рис. 3. Диаграмма пропускной способности канала связи при распределенных сетевых атаках

Как видно из рис. 3, разработанная ССУ сохраняет режим минимальной загрузки канала, не «проседает» в режим недоступности. Данные результаты обусловлены работой метода противодействия сетевым угрозам с фальсификацией серверных решений, выставлением «ловушек» и идентификацией круга зараженных машин.

Параллельно в течение года проводился эксперимент по расшифровке конфиденциальных данных сети ССУ путем внедрения снифферов (CommView, IRIS, LanExplorer, Net Analyzer) в каналы связи различных филиалов, а также средствами дешифровки трафика канального уровня (unMilitaryZ, BDUpro и иными специализированными средствами) на вычислительных кластерах из 15 серверов DELL PowerEdge™ R720 12th Generation DX290 (Dual Intel® Xeon® E5-2620 Hexa Core incl. Hyper-Threading Technology128 GB DDR3 ECC RAM optional max. 384 GB, RAID Controller Dell PERC H710 8 Port SAS/SATA 6Gbit/s, Redundant Platinum Certified Hot Plug). Программное обеспе-

чение для распараллеливания вычислений разворачивалось на различных хостах с различными операционными системами на базе гипервизоров (ESXi) и паравиртуализаторов (XEN). Попытки дешифровки данных, в рамках описанного временного интервала, оказались безуспешными.

В идентичных условиях взаимодействия двух хостов разработанная система не уступает i2p-технологии, выигрывая функционально в сфере корпоративных вычислительных сетей.

Заключение. Разработанные методы противодействия сетевым угрозам и обеспечения информационной безопасности корпоративных потоков, лежащие в основе самоорганизующейся системы управления трафиком, зарекомендовали себя надежным автономным и отказоустойчивым средством защиты сектора ИКТ, исключающим возможность даже прогнозировать стратегию реагирования и дешифровки информации в рентабельные сроки. Минусом системы является требование к значительным вычислительным мощностям, так как остальным средствам защиты было бы достаточно CPU Intel Pentium IV 4 GHz (или аналогичные), RAM 1 Gb, HDD 30 Gb. Учитывая, что развитие микроэлектроники стремительно набирает обороты, требование обеспечения заявленных вычислительных мощностей не является весомым недостатком.

Литература

1. Ажмухамедов И.М. Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. – 2010. – № 2. – С. 68–72.

2. Басыня Е.А. Интелектуально-адаптивные методы обеспечения информационной сетевой безопасности / Е.А. Басыня, А.В. Гунько // Автоматика и программная инженерия. – Новосибирск: Изд-во НГТУ, 2013. – Вып. 3. – С. 95–97.

3. Басыня Е.А. О перспективах развития криптографии / Е.А. Басыня, Г.А. Французова, А.В. Гунько // Перспективное развитие науки, техники и технологий: матер. III-й Междунар. науч.-практ. конф.: в 3 т. – Курск: Изд-во ЮЗГУ, 2013. – Т. 1. – С. 199–200.

4. Гамаюнов Д.Ю. Обнаружение компьютерных атак как задача распознавания образов / Д.Ю. Гамаюнов, А.И. Качалин // Матер. Пятого Всерос. симпозиума по прикладной и промышленной математике. – Кисловодск: Изд-во «ТВП», 2004. – С. 91–95.

5. Гунько А.В. Стохастические методы обеспечения информационной сетевой безопасности / А.В. Гунько, Е.А. Басыня // Актуальные проблемы электронного приборостроения: матер. XI Междунар. конф. – Новосибирск: Изд-во НГТУ, 2011. – Т. 7. – С. 47–49.

6. Марьенков А.Н. Повышение защищенности информационных систем на основе анализа аномалий сетевого трафика // Сб. науч. ст. 12-й Всерос. науч.-практ. конф. молодых ученых, студентов и аспирантов. – Ярославль: Изд-во «Еще не поздно!», 2011. – С. 68–69.

7. Селин Р.Н. Алгоритм распознавания сетевых атак с мониторингом подозрительной активности и ретроспективным анализом // Изв. вузов. Северо-Кавказский регион. Технические науки. Прил. № 1. – Ростов/н/Д. Изд-во ЮФУ, 2006. – С. 15–20.

8. Французова Г.А. Обеспечение информационной безопасности внутренних информационных потоков корпоративной сети / Г.А. Французова, А.В. Гунько, Е.А. Басыня // Наука. Технологии. Инновации: матер. Всерос. науч. конф. молодых ученых, Новосибирск, 21–24 нояб. 2013 г.: в 10 ч. – Новосибирск : Изд-во НГТУ, 2013. – Ч. 2. – С. 41–43.

9. Французова Г.А. Разработка и исследование самоорганизующейся системы управления трафиком вычислительной сети / Г.А. Французова, А.В. Гунько, Е.А. Басыня // Наука. Технологии. Инновации: матер. Всерос. науч. конф. молодых ученых, Новосибирск, 21–24 нояб. 2013 г.: в 10 ч. – Новосибирск : Изд-во НГТУ, 2013. – Ч. 2. – С. 3–7.

10. Tor: The second-generation onion router [Электронный ресурс]. – Режим доступа: https://svn.torproject.org/svn/projects/design-paper/tor-design.html, свободный (дата обращения: 01.02.2014).

Басыня Евгений Александрович
Аспирант каф. автоматики НГТУ
Тел.: (383) 346-11-19
Эл. почта: basinya@mail.ru

Французова Галина Александровна
Д-р техн. наук, профессор каф. автоматики
Новосибирского государственного технического университета (НГТУ)
Тел.: (383) 346-11-19
Эл. почта: frants@ac.cs.nstu.ru.

Гунько Андрей Васильевич
Канд. техн. наук, доцент каф. автоматики НГТУ
Тел.: (383) 346-11-19
Эл. почта: gun@ait.cs.nstu.ru.

Basinya E.A., Frantsuzova G.A., Gunko A.V.
Self-organizing control system of computer network traffic

This paper proposes one possible way to implement self-organizing area network traffic control system based on the original network threat protection method and method of providing privacy for corporate network information flows. Network threat protection method is a set of actions aimed to identify the attacker and provide protection of information resources. Method of providing privacy for corporate network information flows involves the formation of a distributed multi-level encryption, information processes security providing and procedures of their electronic automation. Implementation of self-organizing traffic control system computer network on the basis of these methods involves the use of certain tools and includes three main blocks: the server solution prediction and falsification blocks and corporate servers. This paper presents the experimental results and comparative analysis with existing solutions of the protection system and vulnerabilities identification (by scanning and probing), local area network internal information flows deciphering, distributed network attack resistance (including denial of service). Proposed methods of information security showed high efficiency and stability.
Keywords: self-organizing control system of computer network traffic, prediction, falsification of server solutions, genetic algorithmization, fuzzy logic, scanning, probing, firewall, distributed network attacks.