УДК 004.056

И.В. Котенко, А.В. Шоров

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ ИНФРАСТРУКТУРНЫХ АТАК НА ОСНОВЕ ПОДХОДА “НЕРВНАЯ СИСТЕМА СЕТИ”

Котенко И.В., Шоров А.В. **Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “нервная система сети”.**

Аннотация. Статья посвящена анализу механизма защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода “нервная система сети”. В работе предлагается использование имитационного моделирования на уровне сетевых пакетов для исследования механизма защиты “нервная система сети”. Описывается архитектура системы защиты, реализующей данный механизм защиты, и алгоритмы его работы, представляются результаты экспериментов. На основе полученных экспериментальных данных проводится анализ эффективности предлагаемого механизма защиты.

Ключевые слова: имитационное моделирование, инфраструктурные атаки, биоинспирированные подходы, DDoS-атаки, сетевые черви.

Kotenko I.V., Shorov A.V. **Simulation of protection mechanisms against infrastructure attacks based on the “nervous network system” approach.**

Abstract. The paper considers an analysis of a protection mechanism against infrastructure attacks based on the bio-inspired approach “nervous network system”. We propose to use a network packet-level simulation to investigate the protection mechanism “nervous network system”. The paper presents the structure of the protection mechanism, the algorithms of its functioning, and the results of the experiments. Basing on the experimental data, we analyze the effectiveness of the proposed protection mechanism.

Keywords: security modeling and simulation, infrastructure attacks, bio-inspired approaches, DDoS, computer worms, network attacks and defense.

1. Введение. В последнее время наблюдается тенденция к увеличению количества и мощности компьютерных атак на инфраструктуру вычислительных сетей. Мощность распределенных атак типа “отказ в обслуживании” (DDoS-атак) значительно возросла и преодолела барьер в 100 Гб/с. Также постоянно появляется информация о различных вирусных эпидемиях, провоцируемых сетевыми червями, которые при распространении генерируют большие объемы трафика, вследствие чего перегружают каналы связи. Не менее опасны и другие типы инфраструктурных атак на компьютерные сети, такие как атаки на DNS-серверы и атаки на маршрутизаторы.

Все это говорит о необходимости исследований в области защиты компьютерных сетей от инфраструктурных атак. Одним из перспективных подходов к защите компьютерных сетей от

инфраструктурных атак представляется подход “нервная система сети”, являющийся примером биоинспирированного подхода [6-8]. Подход “нервная система сети” воплощает метафору нервной системы человека. Концепция данного подхода была предложена Ю. Ченом и Х. Ченом [10]. Система защиты, основанная на данном подходе, базируется на распределенном механизме сбора и обработки информации, который координирует действия основных устройств компьютерной сети, идентифицирует атаки и принимает контрмеры. Подобный подход, называемый “электронной нервной системой”, описывал в своих книгах Б. Гейтс, где он предлагался в качестве механизма внутренних коммуникаций и координации работы предприятия. Механизм защиты компьютерных сетей, похожий на “нервную систему сети”, рассматривали в своих работах Ф. Дресслер [13] и К. Анагностакис [9].

Для проектирования и реализации новых систем защиты, таких как “нервная система сети”, необходимо иметь средства для их исследования, адаптации, разработки и тестирования. Исследование инфраструктурных атак и механизмов защиты от них на реальных сетях достаточно сложный и труднореализуемый процесс. Для выполнения инфраструктурных атак требуется огромное количество вычислительных узлов, объединенных в сеть. При этом сами инфраструктурные атаки очень опасны, так как в случае их выполнения вычислительная сеть может выходить из строя из-за перегрузок, что может приводить к выходу эксперимента из-под контроля и даже распространению атак вне экспериментальных машин. В таком случае невозможно соблюсти такие важные условия научного эксперимента как контролируемость и повторяемость.

Таким образом, применение методов имитационного моделирования для исследования инфраструктурных атак и механизмов защиты от них представляется наиболее предпочтительным решением. Имитационное моделирование предоставляет гибкий механизм моделирования сложных динамических систем, что позволяет оперировать различными наборами параметров и сценариев, затрачивая намного меньше усилий, чем в реальных сетях.

В статье предлагается использование методов имитационного моделирования на уровне сетевых пакетов для исследования механизма защиты “нервная система сети”. Дается описание структуры механизма защиты, алгоритмов его работы, представляются результаты экспериментов.

2. Использование биоинспирированных подходов для защиты компьютерных сетей. Защищенные компьютерные системы должны иметь возможность взаимодействовать между собой, быстро реагировать на опасность и самовосстанавливаться в случае повреждений.

Одним из методов позволяющих быстро реагировать на угрозы является автоматизация. Большинство современных атак проводится в автоматическом режиме, поэтому необходимо обеспечивать процесс реагировании на атаку до того момента, когда она нанесет критические повреждения целевой системе.

Для разработки автоматических механизмов реагирования на атаку можно использовать модель работы системы защиты человека. Например, на верхнем уровне человека защищает кожа, которая обладает такими свойствами как [20]: физическая защита от проникновений; механизм обнаружения и раннего оповещения об опасности (осязание); противобактериальная и противогрибковая защита.

На точках входа в организм, таких как рот, глаза, нос, уши также существуют механизмы, противодействующие проникновению различных угроз: в качестве фильтров и ловушек выступает слизь и мастоциты; системами обнаружения и раннего оповещения являются обоняние, вкус, антипатогенными свойствами обладает слюна и слезы.

Внутренняя система защиты обычно разделяется на два уровня: локальный, работающий непосредственно на определенном участке, и общий, охватывающий все тело человека и распространяющийся с помощью кровяной, лимфатической системы, а также с помощью нервной системы.

В работе Ф.Дресслера [13] за основу механизма защиты компьютерных сетей взята аналогия с живыми клетками. Локальная передача данных осуществляется от клетки к клетке, сигнал попадает на рецептор клетки и приводит к ответной реакции, которая влияет на соседние клетки. По аналогии с данной метафорой в компьютерной сети имеется монитор, сканирующий трафик. Он отправляет собранные данные системе обнаружения вторжений, которая после получения и обработки этих данных вносит новые правила в межсетевые экраны.

К.Анагностакис и др. [9] предлагают кооперативный механизм защиты от вирусов COVERAGE (Cooperative virus response algorithm), основанный на иммунологии. В этой работе была предпринята попытка реализовать такие свойства и механизмы

иммунных систем живых организмов, как адаптивность, децентрализованная архитектура, механизмы коммуникации. Авторы работы также попытались оптимизировать стоимость сканирования и фильтрации пакетов для детектирования вирусов.

В работе С.Форест и С.Хофмейера [14] представлен подход, основанный на концепции иммуннокомпьютинга и использовании алгоритма отрицательного отбора. Компонент, реализующий этот подход, работает по аналогии с антителами, которые уничтожают все чужеродные объекты в теле человека. При построении модели пространства объектов и (или) событий разделяются на две части: “свои” и “чужие”. Для того чтобы система могла точно определить, где свой и где чужой, в работе предлагается использовать детекторы, которые реагируют только на “чужие” элементы.

Более детально в работе был исследован подход, предложенный Ю.Ченом и Х.Ченом, и названный “нервная система сети”. Механизм защиты, основанный на данном подходе, базируется на распределенном механизме сбора и обработки информации, который координирует действия основных устройств компьютерной сети, идентифицирует атаки и принимает контрмеры. [10].

3. Представление метафоры “нервная система сети”. За основу предлагаемого подхода к защите компьютерных сетей, называемого “нервная система сети” [10], была взята нервная система человека. Нервная система пронизывает все тело человека и служит системой сбора, передачи, обработки информации, а также вырабатывает ответную реакцию на различные раздражители. Структура данной системы повторяет структуру нервной системы человека. Механизм работы нервной системы сети - распределенный, т.е. нет единого центра, который координирует действия всей сети.

Система защиты включает в себя два основных компонента - сервер “нервной системы сети” и узел “нервной системы сети”. Сервер устанавливается в различных подсетях и реализует большую часть процессов обработки и анализа информации, а также координацию действий близлежащих сетевых устройств. Узлы служат для сбора, первоначальной обработки и передачи информации о состоянии сети серверам и могут работать на основе маршрутизаторов. Серверы, находящиеся в разных подсетях, обмениваются обрабатываемой информацией о состоянии своих подсетей (рис. 1).

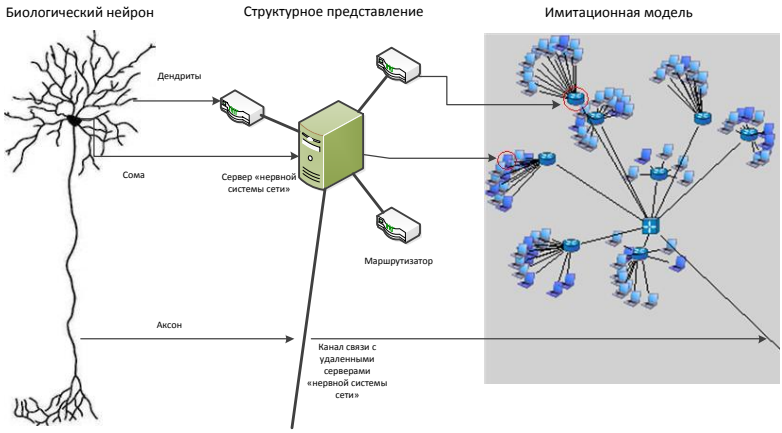

Рис. 1. Представление биологического нейрона
в модели компьютерной сети.

Таким образом, на основе метафоры нервной системы сети предлагается адаптивная сетевая инфраструктура, обеспечивающая получение информации, ее передачу на специальный сервер и принятие решений исходя из сложившейся ситуации.

Для обеспечения безопасности системы в [10] предлагается протокол IFSec (infrastructure security protocol), являющийся новым протоколом безопасности сетевой инфраструктуры. Этот протокол работает на сетевом уровне (уровень 3) и определяет формат и механизм шифрования, которые поддерживают безопасный обмен информацией между доменами, а также между маршрутизаторами и сервером в домене. IFSec строится как надстройка IP и работает прозрачно, чтобы транспортировать протоколы более высокого уровня.

Протокол IFSec предоставляет три уровня коммуникации. Самый низкий уровень дает возможность маршрутизаторам в одном домене обмениваться информацией для контроля состояния сети. Второй уровень - коммуникация между маршрутизаторами и сервером, расположенными в одном домене. На самом высоком уровне сервер обменивается информацией с другими серверами, расположенными в других доменах.

Таким образом, протокол IFSec работает в трех различных слоях. Слой 1 служит для коммуникации между одиночными узлами. Слой 2 реализует взаимодействие между узлами и их

сервером. Слой 3 объединяет серверы в разных доменах. Кроме того, серверы общаются с общей сетью через протоколы IPSec.

Интернет-провайдеры часто используют разные политики безопасности, кроме того, они не хотят, чтобы конкуренты знали, каково состояние их сетей, доступные пределы пропускной способности, даже если провайдеры работают по соглашению о совместной защите от DDoS-атак. Слой 3 в протоколе IFSec решает проблему приватности на уровне политики.

Это достаточно простая и доступная для реализации схема управления доверием. Используя эту схему, IFSec может позволить провайдерам объединять усилия для защиты от DDoS-атак. С помощью доверительного обмена информацией провайдеры могут определить, какую приватную информацию разрешается открыть для доступа другим системам.

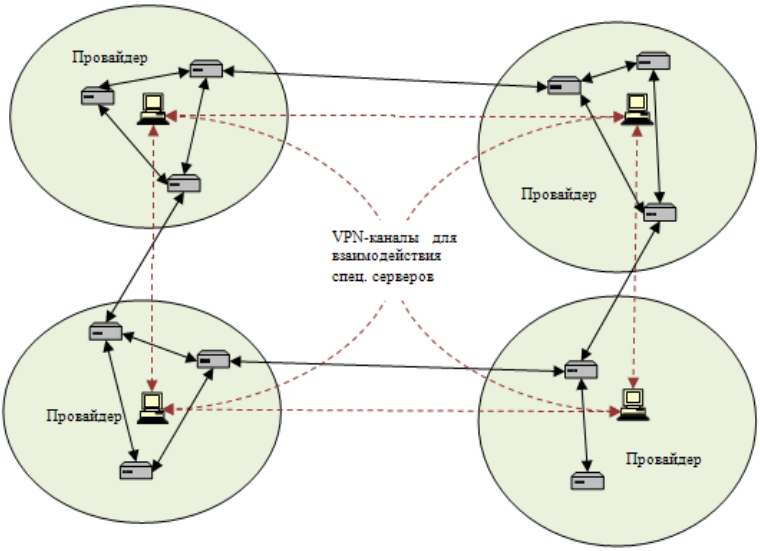

Рис. 2. Обобщенная архитектура компьютерной сети, построенной на основе подхода “нервная система сети”.

Архитектура системы, основанной на данном подходе, представляется следующим образом. Домены сети, которые подключены к нервной системе сети, формируют оверлейную сеть и взаимодействуют между собой через каналы VPN, установленные

между специализированными серверами безопасности (рис. 2). Маршрутизаторы, расположенные в разных точках сети, взаимодействуют не только друг с другом, но и со специализированным сервером безопасности в своем домене.

Функциональные возможности данной архитектуры могут быть представлены на двух уровнях:

(1) локальная обработка поступившей информации на отдельных устройствах;

(2) обработка информации в масштабе распределенной кооперации провайдеров.

Конкретный процесс по обеспечению защиты осуществляется локально, т.е. в каждом отдельном узле. Крупномасштабная кооперация выполняется для реализации защищенного обмена информацией как внутри домена (от маршрутизатора к маршрутизатору, от маршрутизатора к серверу), так и между доменами (от сервера к серверу). В этом случае информация автоматически распределяется по различным узлам сети (рис. 3). Своевременное получение информации позволяет более эффективно реагировать на различные внешние угрозы.

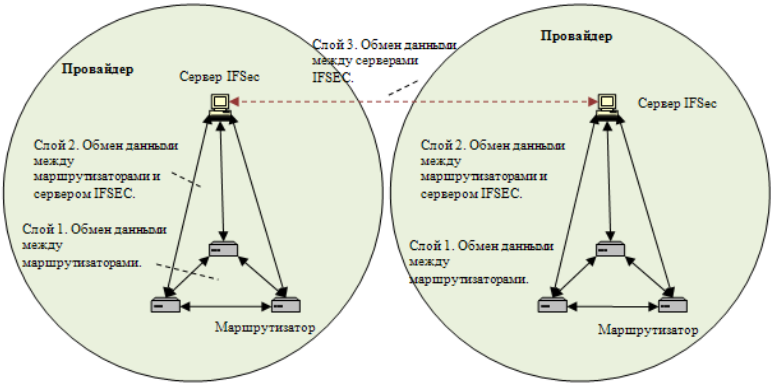

Рис. 3. Слои (уровни) обмена данными с помощью протокола IFSEC.

Каждый узел состоит из функциональных блоков со стандартным интерфейсом передачи данных, что обеспечивает большую гибкость при динамическом обновлении и обслуживании узлов.

Идея этой модели возникла из аналогии с нервной системой живых существ. Кооперация распределенных узлов происходит

подобно реакции человеческой нервной системы. Одиночные узлы работают не только как исполнители, но также и как сенсоры. Помимо общей защиты, которая осуществляется ими самостоятельно, они также предоставляют результаты анализа данных другим узлам и серверам безопасности. Серверы безопасности тоже выполняют две роли. Прежде всего, они функционируют как координаторы, направляя управляющие сигналы к узлам в своих управляющих доменах. Также они работают как дистрибьюторы, получая полезную информацию от узлов в своих доменах и обмениваясь ею с другими серверами безопасности, распределяя полученную от них информацию собственным узлам.

Метафора “нервной системы сети” реализует основные свойства структуры нервной системы, определяющие механизм обмена информацией, обнаружения и реакции на атаку. Существуют системы, использующие похожие принципы построения и функционирования, например концепцию автономного компьютинга [1].

4. Архитектура системы защиты “нервная система сети”. Для начала представим общую архитектуру “нервной системы сети” (рис. 4).

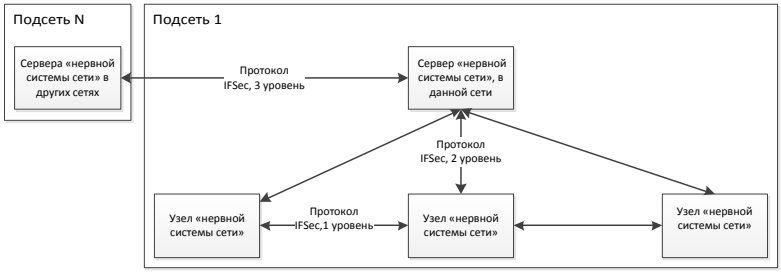

Рис. 4. Общая архитектура “нервной системы сети”.

В подсети 1 компьютерной сети имеется сервер “нервной системы сети”. Он связан с серверами “нервной системы” в других подсетях. К каждому серверу подключены узлы “нервной системы сети”, находящиеся в одной подсети с главным сервером. Кроме того, каждый из узлов имеет связи с другими узлами “нервной системы” в данной подсети. Взаимодействие между всеми узлами и серверами в сети обеспечивается с помощью различных уровней протокола IFSec.

На основе предложенной архитектуры отобразим компонентную структуру “нервной системы сети”. В частности раскроем компоненты сервера и узла “нервной системы сети”.

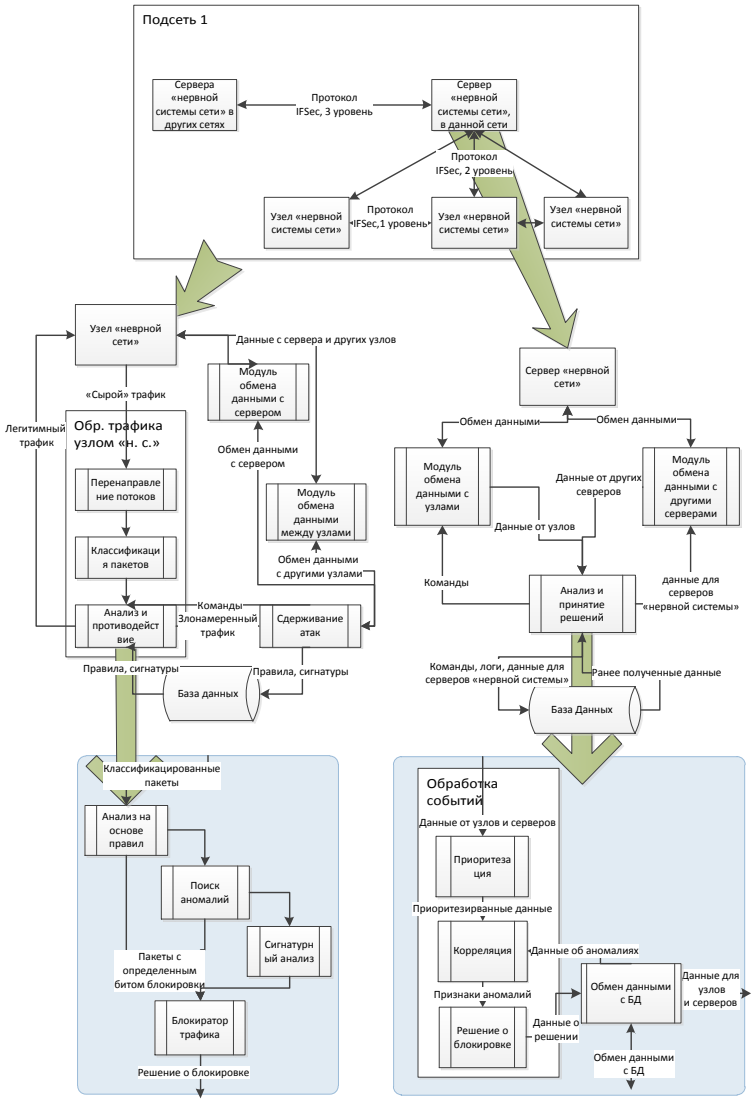

Рис. 5. Структурное представление «нервной системы сети».

На рис. 5 показана архитектура сервера “нервной системы сети”. Сервер “нервной сети” содержит следующие модули: блок обмена данными с узлами; блок обмена данными между серверами; блок принятия решений и определения ответной реакции; база данных.

Сервер “нервной системы сети” имеет модули обмена данными с подчиненными ему узлами, а также с серверами, находящимися в других подсетях. Модули обмена данными соединены с компонентом, отвечающим за анализ данных и принятие решений. С помощью него они получают команды и данные для отправки на узлы и другие сервера “нервной системы” и доставляют ему информацию о событиях, происходящих в сети. К модулю анализа и принятия решений подключена база данных, которая служит хранилищем данных, полученных из внешних источников, и поставляет ранее сохраненную информацию.

Компонент, отвечающий за анализ полученной информации и принятие решений, представлен на рис. 6.

Рис. 6. Архитектура сервера “нервной системы сети”.

Данные, полученные от модулей обмена информацией с узлами и серверами “нервной системы сети”, попадают в модуль приоритезации, где в соответствии с установленными политиками классифицируются события и определяется, насколько важна та или иная информация, на основе чего принимается решение об очередности выполнения действий в следующих блоках.

Затем данные попадают в модуль корреляции, который, в соответствии с приоритетом, выбирает события и запрашивает похожие события из базы данных (БД) с помощью компонента “обмен данными с базой данных”. После чего происходит сопоставление набора событий, и определяется уровень угрозы. Затем в блоке “решение о блокировке” на основе политик и порогов определяется реакция на текущую ситуацию в сети. В случае необходимости данные отправляются серверам и узлам “нервной системы сети”. Информация о принятом решении и текущем уровне угрозы записываются в базу данных.

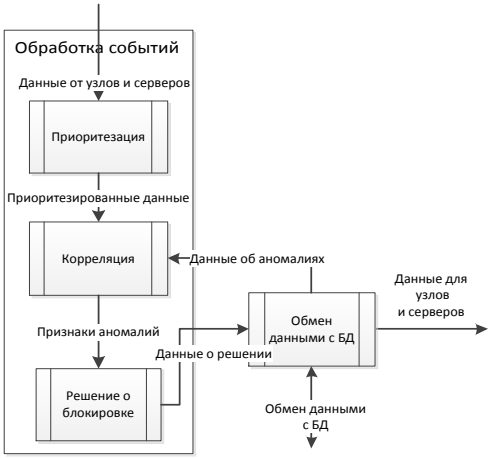

Рис. 7. Модуль анализа и принятия решений сервера “нервной системы сети”.

Рассмотрим более подробно блок анализа и принятия решений (рис. 7). В состав этого блока входят: модуль приоритезации полученных данных; модуль корреляции данных; модуль обмена данными с другими серверами “нервной системы сети” и узлами локальной “нервной системы сети”; модуль обмена информацией с базой данных сервера; модуль принятия решений.

Опишем алгоритм работы модуля приоритезации. Если получаемые данные содержат подозрительные IP-адреса, они получают наивысший приоритет обработки; данные о прохождении подозрительных пакетов получают более низкий приоритет; данные из неизвестных источников отбрасываются.

После приоритезации выполняется обработка полученных данных модулем корреляции. Если модуль не занят, он ищет данные с наивысшим приоритетом и производит поиск в БД сервера информации об адресах, с которых предположительно выполняются атаки на легитимные узлы. Если подозрительный адрес уже был замечен в подобных действиях, уровень угрозы со стороны данного адреса повышается. В случае если задач с высшим приоритетом нет, выполняется задача выявления источника атаки.

Рассмотрим работу основных алгоритмов, отвечающих за определение источников выполнения атак.

Раскроем функцию получения данных от узлов, подчиненных серверу "нервной системы сети". Для этого опишем алгоритм на основе подхода "множество изменяемых деревьев" (CAT - change aggregation trees) [11]. Для получения локального дерева сервер собирает данные об обнаруженных аномалиях от подключенных к нему узлов. Сначала алгоритм проверяет, есть ли узлы, расположенные на более низком уровне. Если таких узлов нет, узел, отправивший данные об атаке, становится корневым, и выполняется поиск узлов более высокого уровня, обнаруживших атаку. Если они найдены, они присоединяются к локальному дереву в качестве ветвей. Если же узел более низкого уровня найден, узел, инициировавший отправку данных, присоединяется к нему в качестве ветви.

Рассмотрим работу механизма при получении данных от удаленных серверов "нервной системы сети". В случае получения данных от удаленного сервера выполняется построение глобального дерева атак. Алгоритм построения глобального дерева атак следующий. При получении локальных деревьев от других узлов сервер проверяет, есть ли у него свое локальное дерево. Если локальное дерево имеется, проверяется, является ли подсеть, в которой расположен сервер, целью атаки, предполагая, что адрес назначения вредоносных пакетов находится в данной подсети. Если подсеть является целью атаки, сервер пытается объединить свое локальное дерево с деревьями сетей, с которыми данная подсеть граничит и образует так называемый первый радиус. После чего сервер пытается присоединить к полученному дереву подсети,

которые граничат с первым радиусом и т.д. Если количество узлов, обнаруживших атаку, больше, чем определенное пороговое значение, детектируется атака. Если подсеть, в которой находится сервер, не является целью атаки, проверяется в какую сеть уходит вредоносный трафик, после чего локальное дерево отправляется серверу, находящемуся в данной подсети.

Далее выполняется функция блокировки трафика. В данном модуле проверяется, превысил ли подозрительный IP-адрес пороговое значение, если превысил, то принимается решение о блокировке адреса атакующего, которое отправляется всем подчиненным узлам, а также удаленным серверам “нервной системы сети”.

Представим узел “нервной сети” в следующем виде: модуль сбора информации с сенсоров; модуль обмена данными с сервером “нервной системы сети”; модуль обмена данными между узлами “нервной системы сети”; модуль, реализующий обработку трафика.

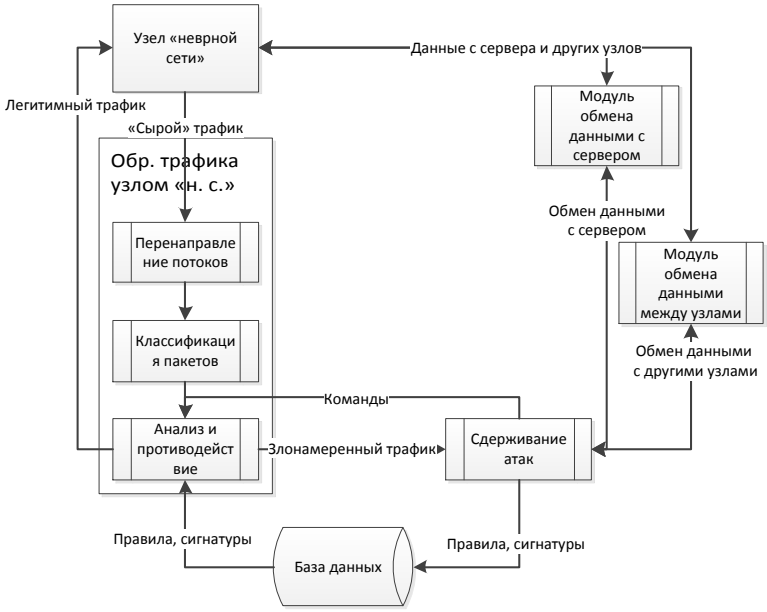

Рис. 8. Архитектура узла “нервной системы сети”.

Модуль обработки трафика, в свою очередь, состоит из блока перенаправления потоков, выполняющего разделение трафика на потоки согласно адресу отправителя и адресу получателя; блока классификации пакетов, определяющего протокол и тип пакетов (запрос на соединение, пакет с данными и т.п.); блока анализа и противодействия. Блок анализа и противодействия содержит модуль анализа трафика на основе правил, модуль анализа с помощью модуля обнаружения аномалий, модуль сигнатурного анализа и модуль блокировки трафика.

На рис. 8. изображена архитектура узла “нервной системы сети”. Узел, на первом этапе обработки, с помощью блока перенаправления потоков распределяет потоки исходя из IP-адреса отправителя. Далее используя блок классификации пакетов, он определяет типы пакетов, отправляемых источником. После этого производит анализ трафика, полученного после обработки. К модулю анализа и противодействия подключена база данных, из которой он получает информацию, на основе которой производится анализ трафика. Если узел обнаружил, что трафик вредоносный, он передает информацию об этом модулю сдерживания атак с данными о вредоносном трафике. Легитимный трафик возвращается в сеть. Модуль сдерживания атак с помощью компонентов обмена данными пересылает эту информацию серверу и узлам, а также получает информацию от них и обновляет базу данных правил и сигнатур.

Архитектура модуля анализа и противодействия представлена на рис. 9. Пакеты из модуля классификации попадают в компонент “анализ на основе правил”, где на базе правил фильтрации принимается решение о блокировке трафика. Далее трафик проходит модули поиска аномалий и сигнатурного анализа. Если какой-либо модуль принял решение о блокировке трафика, пакет, не проходя через последующие фильтры, попадает на модуль блокировки, который в случае положительного решения удаляет пакет и передает информацию о нем в модуль сдерживания атак. В случае если пакет легитимный, он возвращается в сеть.

Если узел обнаруживает вредоносные потоки трафика, он отправляет сообщение об этом серверу “нервной сети”, с которым он связан. Сообщение содержит следующие поля: идентификатор маршрутизатора, идентификатор вредоносного потока (например, IP-адрес получателя и IP-адрес отправителя), идентификатор маршрутизатора, от которого получен пакет, идентификатор маршрутизатора, которому передается пакет, количество

маршрутизаторов на верхнем уровне, количество маршрутизаторов на нижнем уровне, состояние маршрутизатора.

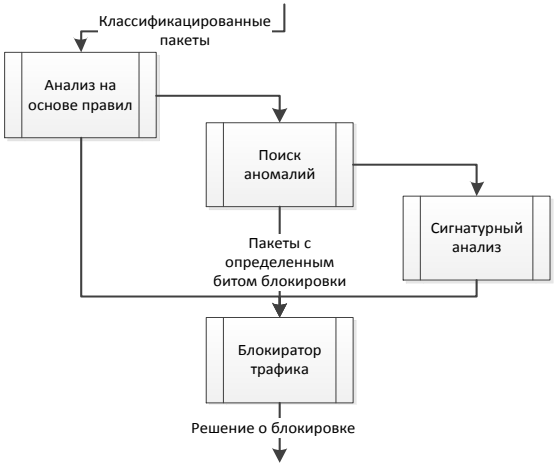

Рис. 9. Архитектура модуля анализа и противодействия.

Серверы “нервной системы сети” постоянно анализируют информацию, поступающую от подключенных к ним узлов и других серверов, вследствие чего принимаются решения об ограничении работы тех или иных пользователей вычислительной сети.

5. Стенд для имитационного моделирования механизма защиты “нервная система сети”. Для оценки качества работы механизма защиты “нервная система сети” использовался стенд имитационного моделирования на уровне сетевых пакетов, сформированный на основе системы моделирования, описанной в [2–3, 16–17].

С помощью системы имитационного моделирования были реализованы модели распространения сетевых червей (в т.ч. модель уязвимого узла), распределенной атаки типа “отказ в обслуживании”, модели механизмов защиты на основе подходов FC [12], VT [22], HCF [15], SIM [19], SAVE [18], SYN detection [21], модель распределенного механизма защиты на основе подхода “нервная система сети”.

Для проведения экспериментов использовалась сеть, состоящая из 3652 узлов, 10 из которых являлись серверными

узлами, в состав которых входили: один DNS-сервер, три веб-сервера и шесть почтовых серверов. 1119 узлов (около 30% от общего количества) имели уязвимости, необходимые для успешного осуществления распространения сетевых червей, эти же узлы выполняли DDoS-атаку.

Эксперименты по исследованию моделей защиты от инфраструктурных атак включают моделирование базовых механизмов защиты FC, VT, HCF, SIM, SAVE, SYN detection и механизма защиты “нервная система сети”, работающего в кооперации с базовыми механизмами защиты.

В случае проведения экспериментов только с базовыми механизмами защиты они устанавливаются на 100% маршрутизаторов. При использовании подхода “нервная система сети” базовые механизмы защиты подключаются к серверам “нервной системы сети”. В случае исследования механизма защиты на основе подхода “нервная система сети” используются те же самые параметры компьютерной сети и механизмов атаки, что и при проведении экспериментов по исследованию базовых механизмов защиты. Это позволяет сравнивать эффективность работы механизма защиты “нервная система сети” с базовыми механизмами защиты.

6. Эксперименты. На первом этапе выполнения экспериментов моделировались механизмы защиты от распространения сетевых червей. Для моделирования распространения сетевых червей было принято допущение, что в компьютерной сети часть узлов имеет уязвимости, которые может эксплуатировать моделируемый червь. Сетевой червь работал по протоколу TCP, в качестве алгоритма сканирования применялось случайное сканирование по известному диапазону адресов.

Для противодействия распространению сетевых червей в качестве базовых механизмов защиты использовались подходы FC и VT. При включении механизма защиты на основе “нервная система сети” базовые компоненты защиты координировались со стороны сервера “нервной системы сети”, к которому они подключены.

На рис. 10 демонстрируется количество зараженных хостов при работе механизма защиты FC, установленного на 100% маршрутизаторов (FC-100%), механизма защиты VT (VT-100%) и механизма защиты на основе подхода “нервная система сети” в кооперации с механизмом защиты FC (HCC-100%), а также при

распространении сетевых червей без использования механизмов защиты.

Видно, что в случае координации механизма защиты FC на основе “нервной системы сети” количество зараженных хостов снижается почти на 20% относительно механизма защиты FC и примерно на 10% относительно VT.

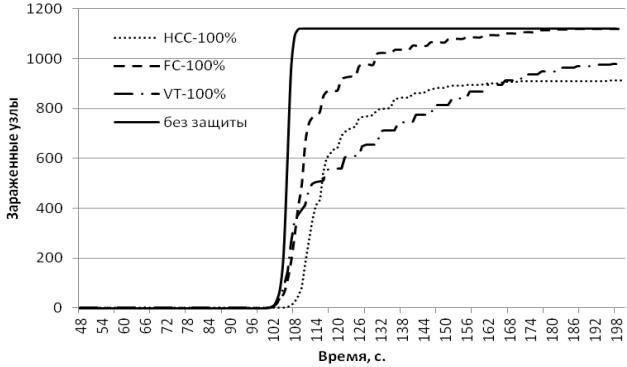

Рис. 10. Зависимости количества зараженных хостов от модельного времени при использовании механизмов защиты FC-100%, VT-100%, НСС-100% и без защиты.

Далее выполнялись эксперименты по защите от атак DDoS. В экспериментах по моделированию DDoS-атак выполнялись атаки SYN Flooding и Ping Flooding, причем в половине экспериментов использовалась подмена IP-адреса отправителя. В качестве механизмов защиты от DDoS-атак использовались подходы SAVE, Hop-Count Filtering и SIM. В случае работы механизма защиты “нервная система сети” управление базовыми механизмами защиты выполняется серверами “нервной системы”.

На рис. 11 изображен объем трафика, поступающего на атакуемый узел во время выполнения DDoS-атаки без подмены IP-адреса отправителя в зависимости от модельного времени. В первом случае для защиты от DDoS-атаки используются защитные механизмы SAVE. Так как атака выполняется без подмены IP-адреса, механизм защиты SAVE не может детектировать вредоносные потоки. Во втором случае механизмы защиты SAVE и SIM подключаются к механизму “нервная система сети”.

С помощью механизма защиты SIM, который установлен на атакуемом сервере, определяются IP-адреса возможных источников атаки. “Нервная система сети” передает эти IP-адреса механизму защиты SAVE, расположенному на маршрутизаторах, где он блокирует вредоносный трафик непосредственно у источников DDoS-атаки.

При самостоятельной работе базовые механизмы защиты применяют собственные алгоритмы обнаружения и блокировки атак. В случае включения их в “нервную систему сети” базовые механизмы защиты используют собственные механизмы обнаружения, но информацию об обнаруженных атаках передают серверу “нервной системы сети”, к которому они подключены, и, в случае отсутствия правил, сигнатур или политик соответствующих обнаруженной угрозе, ожидают команд от сервера “нервной системы сети”.

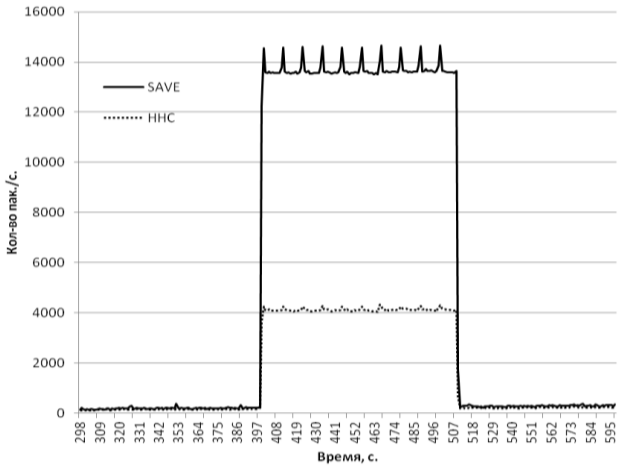

Рис. 11. Зависимости объема трафика, поступающего на атакуемый узел при работе механизма защиты SAVE и механизмов защиты SAVE и SIM под управлением “нервной системы сети” в случае выполнения DDoS-атаки без подмены IP-адреса отправителя, от модельного времени.

7. Оценка результатов. Проведем оценку качества работы механизма защиты “нервная система сети” относительно базовых и кооперативных механизмов защиты как с помощью традиционных метрик качества классификации трафика: ошибки первого (FP) и

второго рода (FN), так и с помощью дополнительных метрик, таких как полнота, точность, аккуратность, ошибка и F-мера.

Полнота (recall, r) определяется как отношение количества правильно классифицированных пакетов вредоносного трафика к общему количеству пакетов: r=TP/(TP+FN).

Точность (precision, p) вычисляется как отношение правильно классифицированных вредоносных пакетов к общему количеству пакетов, классифицированных как вредоносные: p=TP/(TP+FP).

Аккуратность (accuracy, a) рассчитывается как отношение правильно принятых системой решений к общему числу решений: a=(TP+TN)/(TP+FP+FN+TN).

Ошибка (error, e) вычисляется как отношение количества неправильно принятых системой решений к общему числу решений: e=(FP+FN)/(TP+FP+FN+TN).

F-мера (F-measure) часто используется как единая метрика, объединяющая метрики полноты и точности. *F-мера* для данной категории вычисляется по формуле:

$$F_i = \frac{2 p_i r_i}{p_i + r_i}.$$

Данные метрики используются также для оценки качества работы механизма защиты “нервная система сети” по сравнению с другими механизмами защиты.

Кроме того, применяются и другие метрики, характеризующие эффективность работы механизмов защиты. Так при сравнении механизмов защиты от сетевых червей оценивается количество зараженных узлов ($N_{зар}$), а в случае проведения DDoS-атак - объем вредоносного трафика, поступающего на атакуемый узел ($V_{вр.тр.}$).

Значения метрик, характеризующих работу базовых механизмов защиты и механизма “нервная система сети” при распространении сетевых червей, приводятся в табл. 1. В данном случае “нервная система сети” использует в качестве детектора базовый механизм защиты FC.

Таблица 1. **Сравнение механизмов защиты FC, VT и НИС**

	FP	FN	*r*	*p*	*a*	*e*	F-мера	$N_{зар}$, %
FC	0.31	0.18	0.52	0.78	0.21	0.21	0.59	99
VT	0.01	0.57	0.43	0.98	0.66	0.33	0.60	93
НСС	0.22	0.22	0.77	0.90	0.71	0.28	0.83	81

Табл. 1 показывает, что под управлением “нервной системы сети” механизм защиты FC показывает несколько лучшую

эффективность работы по сравнению с другими, учитывая значения F-меры и количество зараженных узлов.

Метрики, характеризующие эффективность работы механизмов защиты при выполнении DDoS-атак, представлены в табл. 2.

Таблица 2. **Сравнение механизмов защиты SAVE, SIM и HHC**

	FP	FN	r	p	a	e	F-мера	$V_{вр.тр.}$, %
DDoS-атака с подменой адреса отправителя пакета								
SAVE	0.04	0.01	0.99	0.97	0.98	0.02	0.98	1
SIM	0.09	0.01	0.99	0.98	0.97	0.03	0.98	99
HCC	0.04	0.01	0.99	0.97	0.98	0.02	0.98	1
DDoS-атака без подмены адреса отправителя пакета								
SAVE	0.03	0.99	0.01	0.01	0.01	0.99	0.01	99
SIM	0.07	0.29	0.70	0.93	0.68	0.32	0.80	99
HCC	0.07	0.30	0.69	0.93	0.68	0.33	0.80	30

Так как “нервная система сети” применяет механизмы кооперации для защиты компьютерной сети от инфраструктурных атак, необходимо провести сравнение эффективности ее работы с другими кооперативными механизмами защиты. Для сравнения были выбраны механизмы кооперативной защиты COSSACK, DefCOM и механизмы, базирующиеся на многоагентном подходе, описанные в работах [4, 5, 16]. Сравнение механизма защиты “нервная система сети” с кооперативными механизмами защиты производилось на основе данных о количестве вредоносного трафика, поступающего на атакуемый узел. Сравнивалась работа механизмов защиты при выполнении DDoS-атак, так как представленные кооперативные механизмы не предназначены для защиты от других типов инфраструктурных атак. На основе полученных данных о вредоносном трафике, поступающем на атакуемый объект, и трафике, получаемом после активации механизмов защиты, были получены метрики, показывающие, на сколько процентов снизилась нагрузка на атакуемый объект. Полученные данные представлены в табл. 3.

Таблица 3. **Процент фильтруемого вредоносного трафика кооперативными механизмами защиты**

COSSACK	DefCOM	Кооп. мех. [4,5,16]	HCC
21.5%	42.7%	64.2%	70.7%

Механизм защиты “нервная система сети” показал большую эффективность по сравнению с другими кооперативными механизмами защиты.

Следует отметить, что из-за высокой сложности разработки кооперативных механизмов защиты, основанных на многоагентном подходе, модели представленных механизмов защиты не были реализованы в системе имитационного моделирования, а результаты брались из [4, 5, 16], потому данное сравнение может быть не совсем точным, так как эксперименты проводились в разных системах, хотя и имеют сходные условия.

8. Заключение. Регулярно появляющиеся сообщения о тех или иных успешно проведенных атаках на инфраструктуру компьютерных сетей говорят о необходимости разработки новых адаптивных и интеллектуальных механизмов защиты.

В настоящей статье предложено использовать механизмы защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода “нервная система сети”. Рассмотрена одна из возможных архитектур системы, реализующей данный механизм защиты, и алгоритмы его работы. Анализ указанных механизмов проведен на основе имитационного моделирования на уровне сетевых пакетов. Проведенные эксперименты показали эффективность кооперации “нервной системы сети” с базовыми механизмами защиты в случае противодействия инфраструктурным атакам распространения сетевых червей и “распределенный отказ в обслуживании”. Решающую роль здесь играет своевременная передача информации об обнаруженных атаках по всем подсетям, содержащим сервера “нервной системы сети”, вследствие чего атакующий трафик, возникающий в различных сегментах сети, сразу же блокируется.

Представленная работа показывает возможность использования биологических метафор в области защиты компьютерных сетей от инфраструктурных атак. Конечно, далеко не все биологические подходы сегодня можно полностью реализовать. Однако многие из них могут оказаться жизнеспособными и дать новый толчок в развитии перспективных систем защиты информации.

Литература

1. *Биддик М.* Автономные вычисления: представления и реальность // Сети и системы связи, 2007, N 4. С.34-38.

2. *Котенко И.В., Коновалов А.М., Шоров А.В.* Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Изв. вузов. Приборостроение, Т.53, № 11, 2010, С.42-45.
3. *Котенко И.В., Коновалов А.М., Шоров А.В.* Исследовательское моделирование бот-сетей и механизмов защиты от них. Приложение к журналу "Информационные технологии". Москва: Издательство Новые технологии, 2012, № 1. 32 с.
4. *Котенко И.В., Уланов А.В.* Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет // Известия РАН. Теория и системы управления, № 5, 2007, С.74-88.
5. *Котенко И.В., Уланов А.В.* Команды агентов в кибер-пространстве: моделирование процессов защиты информации в глобальном Интернете // Проблемы управления кибербезопасностью информационного общества. Сборник Института системного анализа РАН, URSS, Москва, 2006. . С.108-129.
6. *Котенко И.В., Шоров А.В.* Использование биологической метафоры для защиты компьютерных систем и сетей: предварительный анализ базовых подходов // Защита информации. Инсайд, 2011. № 1, С.52-57. № 2, С.66-75.
7. *Котенко И.В., Шоров А.В., Нестерук Ф.Г.* Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. Вып.3 (18). СПб.: Наука, 2011. С.19–73.
8. *Котенко И.В., Шоров А.В., Нестерук Ф.Г.* Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // XIV Всероссийская научно-техническая конференция "Нейроинформатика-2012": Сборник научных трудов. Том 2. М.: НИЯУ МИФИ, 2012. С.61-71.
9. *Anagnostakis K., Greenwald M., Ioannidis S., Keromytis A., Li D.* A Cooperative Immunization System for an Untrusting Internet // ICON2003. The 11th IEEE International Conference on Networks, 2003. P.403–408.
10. *Chen Y., Chen H.* NeuroNet: An Adaptive Infrastructure for Network Security // International Journal of Information, Intelligence and Knowledge, 2009. Vol.1, No.2. P. 143-168.
11. *Chen Y., Hwang K., Ku W-S.* Collaborative Detection of DDoS Attacks over Multiple Network Domains // Parallel and Distributed Systems IEEE. Vol. 18 Is. 12, 2007. P. 1649 – 1662.
12. *Chen S., Tang Y.* Slowing Down Internet Worms // Proceedings of the 24th International Conference on Distributed Computing Systems, 2004.
13. *Dressler F.* Bio-inspired mechanisms for efficient and adaptive network security // Service Management and Self-Organization in IP-based Networks, 2005.
14. *Hofmeyr S., Forrest S.* Architecture for an artificial immune system // Evolutionary Computation, vol. 8, no. 4, 2000. P. 443–473.
15. *Jin C., Wang H., Shin K.* Hop-count filtering: an effective defense against spoofed DDoS traffic // Proceedings of the 10th ACM conference on Computer and communications security. ACM New York, USA, 2003. P. 30 – 41.
16. *Kotenko I.* Agent-Based Modelling and Simulation of Network Cyber-Attacks and Cooperative Defence Mechanisms // Discrete Event Simulations. Sciyo, In-teh. 2010. P.223-246.
17. *Kotenko I., Konovalov A., Shorov A.* Agent-based Modeling and Simulation of Botnets and Botnet Defense // Conference on Cyber Conflict. CCD COE Publications. Tallinn, Estonia, 2010. P.21-44.
18. *Li J., Mirkovic J., Wang M., Reither P., Zhang L.* Save: Source address validity enforcement protocol // Proceedings of IEEE INFOCOM, 2002. P.1557–1566.

19. *Peng T., Leckie C., Ramamohanarao K.* Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring // Lecture Notes in Computer Science, Vol.3042/2004, 2004. P.771-782.
20. *Philip R. et al.* Enabling Distributed Security in Cyberspace. Departament of Homeland Security, 2011.
21. *Wang H., Zhang D., Shin K.* Detecting SYN flooding attacks // Proceedings of IEEE INFOCOM, 2002. P.1530–1539.
22. *Williamson M.* Throttling Viruses: Restricting propagation to defeat malicious mobile code // Proceedings of ACSAC Security Conference, 2002. P.61–68.

Котенко Игорь Витальевич — д.т.н., проф.; заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер-терроризму, искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений, телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Kotenko Igor Vitalievich — Prof. of Computer Science; head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism, artificial intelligence, including multi-agent frameworks and systems, agent-based modeling and simulation, soft and evolutionary computing, machine learning, data mining, data and information fusion, telecommunications, including decision making and planning for telecommunication systems. The number of publications — 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Шоров Андрей Владимирович — аспирант лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: имитационное моделирование, безопасность компьютерных сетей, обнаружение вторжений. Число научных публикаций — 33. ashorov@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450. Научный руководитель — Котенко И.В.

Shorov Andrey Vladimirovich — Ph.D. student of Laboratory of Computer Security Problems, SPIIRAS. Research interests: modeling and simulation, computer network security, intrusion detection. The number of publications — 33. akonovalov@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450. Scientific leader — I.V. Kotenko.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00826), программы фундаментальных исследований ОНИТ РАН (проект № 2.2), государственного контракта 11.519.11.4008 и проектов Евросоюза SecFutur и Massif, а также в рамках других проектов.

Рекомендовано СПИИРАН, лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 7.03.2012.

РЕФЕРАТ

Котенко И.В., Шоров А.В. **Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “нервная система сети”.**

В настоящее время защита от инфраструктурных атак на компьютерные сети является одной из наиболее актуальных проблем. Мощность атак типа “распределенный отказ в обслуживании” значительно возросла, постоянно появляется информация о различных вирусных эпидемиях, провоцируемых сетевыми червями. Все это говорит о необходимости проведения исследований в области защиты от инфраструктурных атак на компьютерные сети.

Примером перспективных механизмов защиты являются подходы, основанные на биологической метафоре. Одним из таких подходов к защите компьютерных сетей от инфраструктурных атак является биоинспирированный подход “нервная система сети”. Система защиты, построенная на основе данного подхода, включает два основных компонента — сервер “нервной системы сети” и узел “нервной системы сети”. Серверы устанавливаются в различных подсетях и реализуют большую часть процессов обработки и анализа информации, а также координацию действий близлежащих сетевых устройств. Узлы служат для сбора, первоначальной обработки и передачи информации о состоянии сети серверам и работают на основе маршрутизаторов. Серверы находятся в разных подсетях и обмениваются информацией о состоянии своих подсетей. Таким образом, на основе метафоры “нервной системы сети” предлагается адаптивная сетевая инфраструктура, обеспечивающая получение информации, ее передачу на специальный сервер и принятие решений на основе сложившейся ситуации.

Оценка эффективности функционирования механизма защиты на основе подхода “нервная система сети” проводилась с помощью разработанной среды имитационного моделирования инфраструктурных атак и механизмов защиты от них. Для исследования механизмов защиты от инфраструктурных атак выполнялись эксперименты по моделированию распространения сетевых червей и выполнения атак “распределенный отказ в обслуживании” (DDoS-атак). При этом проводилось сравнение механизма защиты “нервная система сети” с другими механизмами защиты. Для противодействия распространению сетевого червя в качестве базовых механизмов защиты анализировались подходы Failed Connection и Virus Throttling. При выполнении DDoS-атак работа механизма защиты “нервная система сети” сравнивалась с механизмами защиты SAVE и SIM, а также кооперативными механизмами защиты. Механизм защиты “нервная система сети” показал большую эффективность по сравнению с другими механизмами защиты в случае противодействия инфраструктурным атакам распространения сетевых червей и DDoS.

SUMMARY

Kotenko I.V., Shorov A.V. **Simulation of protection mechanisms against infrastructure attacks based on the "nervous network system" approach.**

Protection of computer networks against infrastructure attacks is one of the most actual problems. The total capacity of DDoS attacks has grown considerably; information on the various viral epidemics triggered by network worms does constantly appear. Therefore, it is necessary to carry out research in the field of protection against infrastructure attacks on computer networks.

The approaches based on a biological metaphor are the examples of such advanced security mechanisms. One of such approaches for protecting computer networks against infrastructure attacks is a bio-inspired approach "nervous network system". The protection system consists of two main components – the server of the "nervous network system" and the node of the "nervous network system". Servers are installed in different subnets and implement most functions of information processing and analysis, as well as the coordination of nearby network devices. Nodes are used for data collection, initial processing and transmission of network status information to servers. Nodes can be installed on routers. Servers are located in different subnets and exchange information on the status of their subnets. Thus, on the basis of the metaphor of the "nervous network system", the paper proposes an adaptive network infrastructure which provides information collection and its transfer to the special server and making decisions based on the current situation.

Efficiency assessment of the protection mechanism based on the "nervous network system" approach was carried out by the developed simulation system. For the investigation of the protection mechanisms against infrastructure attacks we carried out the experiments to simulate the spread of computer worms and DDoS attacks. The comparison of the "nervous system network" mechanism with other protection mechanisms was fulfilled. To counteract the worm spreading, the Failed Connection and Virus Throttling mechanisms were analyzed as the basic security approaches. When DDoS attacks were performed, the work of the "nervous network system" was compared with the protection mechanisms SAVE and SIM. Experiments have shown the higher effectiveness of the "nervous networks system" in comparison with the basic protection mechanisms against infrastructure attacks.