В. Е. Лобанов, Б. Н. Оныкий, А. А. Станкевичус

АРХИТЕКТУРА СИСТЕМЫ ЗАЩИТЫ ГРИД ОТ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» И «РАСПРЕДЕЛЕННЫЙ ОТКАЗ В ОБСЛУЖИВАНИИ»[1]

Основная идея технологии Грид (Grid) [1, 2] заключается в объединении ресурсов путем создания компьютерной инфраструктуры нового типа, обеспечивающей глобальную интеграцию информационных и вычислительных ресурсов на основе сетевых технологий и специального программного обеспечения [3]. В настоящее время атаки типа «отказ в обслуживании» (далее — DoS) и «распределенный отказ в обслуживании» (далее — DDoS) [4] являются одними из наиболее распространенных и опасных сетевых атак и представляют серьезную угрозу для Грид. В результате успешной DoS- или DDoS-атаки может быть нарушено обслуживание пользователей и связь между узлами Грид, что может привести к длительным простоям Грид и соответствующему ущербу.

Источник DoS- и DDoS-атаки на Грид может быть внешним (атака на Грид осуществляется из «свободной» сети) и внутренним (атака на Грид проводится со стороны ресурсов Грид). При этом целью атаки может быть ЭВМ, включенная в состав Грид, или сервер Грид, кроме того, интерес представляют и случаи, когда Грид атакует удаленную ЭВМ, не входящую в состав Грид. Атака на отдельный рядовой узел не является опасной для Грид, так как при этом планировщик Грид перераспределит выполнение задачи между другими узлами. Атака на один из центральных серверов может привести к выходу из строя целого сегмента Грид. Широко распространенные средства фильтрации трафика, такие как межсетевые экраны, могут несколько снизить уровень опасности внешней атаки на сервер Грид, но должной безопасности не гарантируют. В случае же когда ресурсы Грид атакуют внутренние сервера, возможен выход из строя всей Грид на неопределенный срок.

Крайне важно своевременное выявление и принятие защитных мер по минимизации последствий DoS- и DDoS-атак, однако без специализированной системы профилактики эти процессы могут быть весьма дорогостоящими и трудоемкими [5]. Известны случаи успешных атак, которые были замечены пользователями лишь через несколько суток.

Методы обнаружения DoS- и DDoS-атак можно разделить на статистические, сигнатурные и гибридные.

Статистические методы основаны на количественном анализе трафика, их использование более выгодно там, где в единицу времени проходит большое количество трафика. Таким местом, например, может являться узловой маршрутизатор или шлюз. В случае начинающейся DDoS-атаки будет накоплена необходимая информация об особенностях именно этой атаки (например, какого типа атака и адреса атакующих машин) для дальнейшего ее предотвращения.

Сигнатурный анализ основан на качественном анализе трафика и более выгоден на уровне отдельно взятой машины или приложения. Здесь нет такого обилия входящего и исходящего трафика, поэтому можно проанализировать пакеты при непосредственном приеме на наличие различного рода «вредных» модификаций. Также возможно отследить запуск ненужных или потенциально опасных сторонних приложений, на которые ссылается запускаемое. Данный метод особенно эффективен против различных DoS-атак.

Гибридный анализ, сочетающий в себе достоинства двух предыдущих методов, хорош многосторонностью, но он сравним скорее с антибиотиками широкого спектра, когда надо вылечить что-то, но точно не ясно, что именно. Этот тип анализа имеет смысл использовать на уровне отдельно взятой машины, например в том случае, когда невозможно установить наблюдение на

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

узловом маршрутизаторе. В Грид подобная ситуация возникает достаточно часто, когда одна или несколько машин являются вычислительными ресурсами, но при этом не являются частью большого кластера. Также подобный метод анализа может быть эффективен при использовании на сервере, при применении его в комбинации с сигнатурным, применяемым на уровне приложений.

После определения трафика атаки нужно выработать ответную реакцию. Возможны следующие действия: отслеживание источника атаки, ограничение допустимого предела («rate limit») и фильтрация «черной дыры» [6]. Необходимо отметить, что при DDoS-атаках часто используются поддельные IP-адреса источника трафика, что делает отслеживание источника атаки малоэффективным.

Архитектура системы защиты Грид. Для защиты Грид от DoS- и DDoS-атак предлагается система защиты, состоящая из следующих компонентов: блока управления, детектора, анализатора, фильтра, архива, блока оповещения и блоков расширения.

Блок управления отвечает за контроль и управление системой. Блок управления получает сведения от других компонентов и блоков оповещения соседних систем и принимает решение о следующем шаге на основе набора управляющих правил.

Детектор осуществляет непосредственное слежение за проходящими сетевыми пакетами. При выявлении аномального трафика детектор отправляет уведомление об этом в блок управления и переправляет трафик в анализатор, после чего продолжает слежение. Также этот блок распознает и передает на блок управления уведомления от соседних систем.

Анализатор проводит анализ аномального трафика, в ходе которого определяется тип аномалии и адреса атакующих ЭВМ. Анализатор передает блоку управления информацию о результатах анализа, а исследованный трафик отправляется в фильтр.

Фильтр отвечает за блокировку того типа трафика, о котором сообщает ему блок управления. Получив инструкцию, фильтр начинает блокировать проходящий трафик указанного вида до тех пор, как команда «блокировать» не будет отменена. Также фильтр блокирует выполнение процессов, указанных управляющим блоком. Названия процессов указываются блоком управления и берутся из архива.

Архив предназначен для хранения журналов, в которых ведутся записи о запуске процессов, о трафике, а также учет событий системы защиты. По команде от блока управления необходимые записи из журналов отсылаются в фильтр и блок оповещения.

Блок оповещения отвечает за рассылку на соседние системы уведомления о начале и завершении работы, текущем состоянии, опасных процессах, начале атаки и пр. Также он отсылает сигнал тревоги оператору.

Предложенная архитектура приведена на рис. 1.

До запуска системы детектор работает некоторое время в режиме обучения и проводит накопление данных о проходящем трафике и загруженности сети. После запуска система переходит в режим слежения. Детектор просматривает проходящий трафик, сравнивает его с имеющимся у него представлением о типе трафика и загруженности сети на данном участке, а также получает уведомления о функционировании соседних систем. В архив в соответствующие журналы заносятся заголовки пакетов, а также информация о запускаемых на ЭВМ процессах. Фильтр работает в соответствии со своей политикой. Блок оповещения генерирует и отсылает уведомления о функционировании к соседним системам. Алгоритм работы системы в режиме слежения приведен на рис. 2.

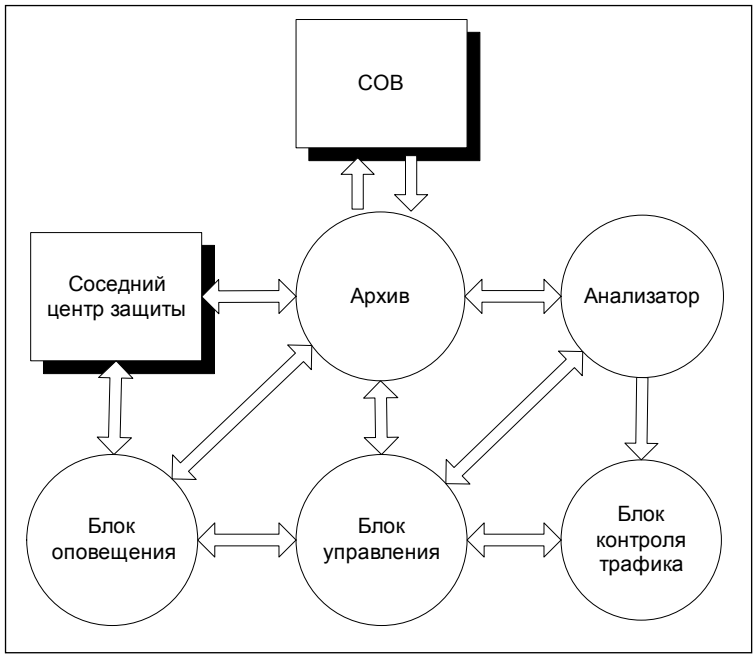

Рис. 1. Архитектура системы анализа и контроля трафика

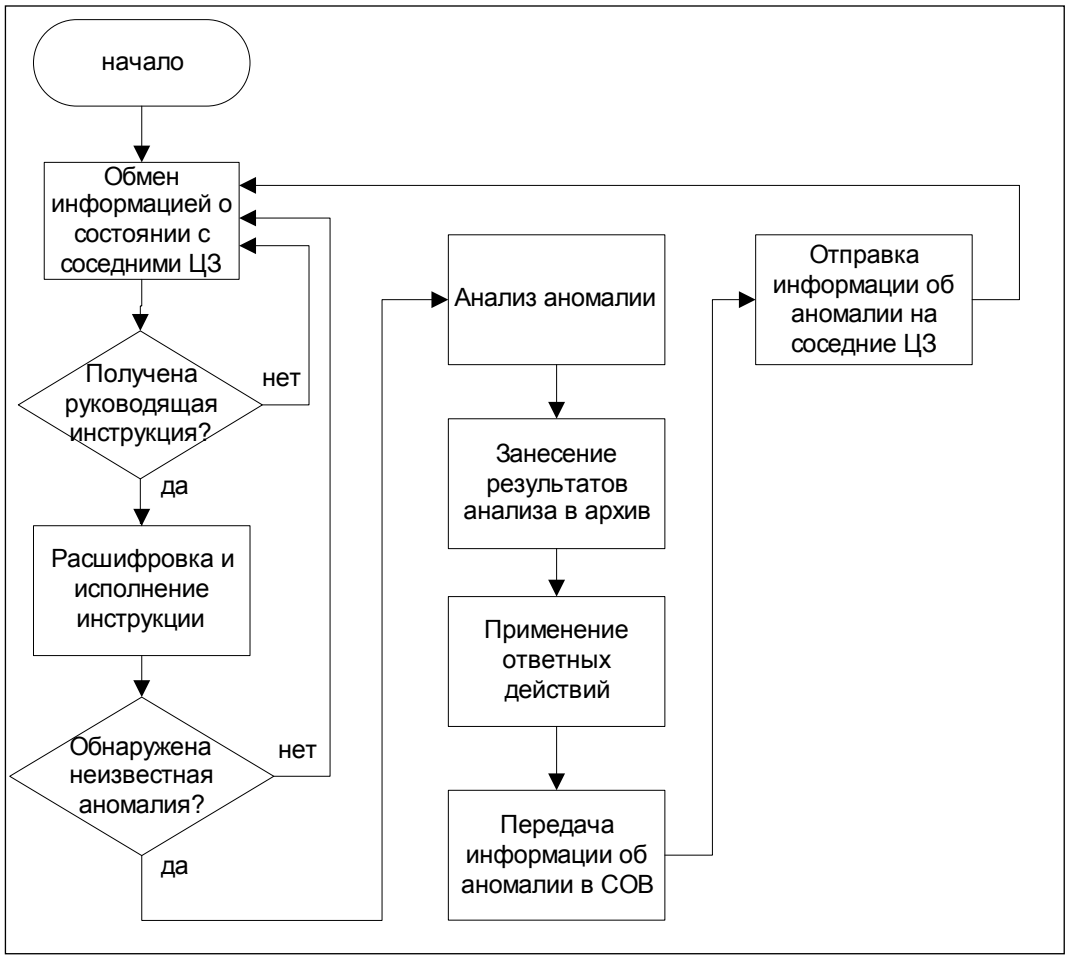

Рис. 2. Алгоритм работы системы анализа и контроля трафика

В случае обнаружения аномалии детектор отправляет уведомление в блок управления и «перенаправляет» трафик в анализатор. Блок управления переводит систему в режим анализа. Проверяется, имеет ли место атака, или аномалия случайна. Если в результате анализа подтверждается, что система атакована, то анализатор определяет тип атаки (внешняя или внутренняя), сопоставляя известные ему адреса ЭВМ, входящих в Грид, с адресами источника аномального трафика. Далее определяется, является ли выявленная атака DoS- или DDoS-атакой. Для этого просматриваются записи в соответствующем журнале.

Если атака определена как DoS, то блок управления переводит систему в режим запрета оправки и приема пакетов. Анализатор выбирает из журнала процессов и журнала трафика последние запущенные процессы и последний принятый трафик и передает эту информацию на блок оповещения и фильтр. Блок оповещения генерирует уведомление об опасном трафике и отсылает его соседним системам. Происходит блокировка вредоносных процессов и трафика. Проводится оповещение оператора и отсылка ему записей из журнала событий. Далее управляющий блок возобновляет прием и передачу трафика и переводит систему в режим слежения.

Если атака определена как DDoS, то управляющий блок переводит систему в режим фильтрации. В случае внешней атаки анализатор определяет узлы, с которых производится атака, и сообщает их адреса фильтру, который блокирует весь входящий трафик с этих адресов. Блок оповещения генерирует уведомление о начале атаки и отправляет его оператору. Управляющий блок переводит систему в режим слежения.

В случае внутренней атаки анализатор определяет адреса атакующих элементов в сети и передает их фильтру, который блокирует входящие (исходящие в случае, если Грид атакует ЭВМ, не включенный в Грид) пакеты на эти адреса (с этих адресов). После этого производится пошаговый откат по процессам, в ходе которого система по одному, шаг за шагом, завершает последние запущенные процессы до тех пор, пока не будет обнаружен процесс, спровоцировавший начало атаки. При обнаружении атакующего процесса он блокируется, а информация о нем передается в блок оповещения, который формирует уведомление о запрете на запуск этого процесса и рассылает его соседним системам. Оператор оповещается, и ему отсылаются записи журнала событий. Управляющий блок переводит систему в режим слежения.

Было проведено прототипирование системы и оценка производительности развернутого в лаборатории демонстрационного прототипа. Тестирование показало потерю производительности вычислений Грид в целом, вызванную функционированием системы защиты. Падение производительности зависит от количества подключенных к Грид ЭВМ как O(log(n)), производительность же вычислений зависит от него как O(n), что говорит о том, что предложенная архитектура хорошо подходит для систем защиты Грид.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. Введение в технологию Грид. URL: http://window.edu.ru/window/library?p_rid=49689.
2. *Foster I., Kesselman C.* The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann Publishers, 1998.
3. *Foster I., Kesselman C., Tuecke S.* The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International J. Supercomputer Applications. 2001. № 15 (3) URL: http://www.globus.org/ research/papers/anatomy.pdf.
4. Types of DDoS Attacks. 2001. URL: http://anml.iu.edu/ddos/types.html.
5. Угрозы распределенного отказа в обслуживании: риски, устранение и лучшие практические приемы. URL: http://www.cisco.com/web/RU/netsol/ns480/networking_solutions_ white_paper0900aecd8032499e.html.
6. Методы защиты от DDoS нападений. 2003. URL: http://articles.softportal.com/article-260.html.