УДК 004.032.26
DOI: 10.15827/0236-235X.125.092-102
Дата подачи статьи: 24.09.18
2019. Т. 32. № 1. С. 092–102

Разработка удаленного клиента для автоматизированной передачи данных в UNIX-подобных системах

Е.В. Пальчевский [1], *аспирант, teelxp@inbox.ru*
А.Р. Халиков[1], *к.ф.-м.н., доцент, khalikov.albert.r@gmail.com*

[1] *Уфимский государственный авиационный технический университет, г. Уфа, 450008, Россия*

Статья посвящена разработке аппаратно-программного модуля для UNIX-подобных систем, который получил название RCM (англ. Remote client management, рус. удаленный клиент для управления). Он предназначен для передачи данных между модулями аппаратно-программного комплекса Protection. Его основными возможностями являются скоростная обработка данных и защита от DDoS-атак на основе нейронных сетей.

В работе рассмотрена проблема обработки данных ПО и обоснована необходимость проведения математического анализа для выявления новых способов самообучения нейронных сетей. Представлены разработанные самообучаемые нейронные сети, необходимые для передачи данных и защиты от DDoS-атак. Разработан новый метод самообучения нейронной сети, основанный на объединении сигнального и дифференциального способов обучения. Это дает возможность нейронной сети быстро обучаться в короткие сроки. Функционал разработанного удаленного клиента позволяет управлять данным модулем как через веб-интерфейс, так и через консольный режим.

Проведено тестирование разработанного ПО в условиях «боевого» режима, в результате которого были получены нагрузочные значения на ресурсы ЭВМ. Длительное тестирование RCM показывает достаточно низкую нагрузку на центральный процессор и твердотельный накопитель при DDoS-атаках. Соответственно, оптимальная нагрузка позволяет не только обрабатывать большие потоки информации, но и параллельно запускать ресурсоемкие вычислительные процессы без какого-либо нарушения функционирования операционной системы.

Тестирование проводилось на серверах вычислительного кластера в одном из московских центров обработки данных, где RCM показал стабильную работоспособность.

Ключевые слова: *информация, передача данных, сети, DDoS, AntiDDoS, UNIX, ОС, данные, обработка данных, информационная безопасность.*

В современном мире информационных технологий одним из важнейших направлений является *автоматизированная обработка данных* (АОД) [1]. В большинстве областей, где применяется АОД, как правило, используют программные, аппаратные и аппаратно-программные средства обеспечения анализа и обработки какой-либо информации [2]. Например, на крупных производственных предприятиях используются различные аппаратно-программные комплексы АОД [3]. Их основными преимуществами являются высокая производительность (при наличии необходимых вычислительных мощностей), а также достаточно большая скорость обработки данных [4]. Но при всех плюсах имеются и явные недостатки: высокое потребление выделенных ресурсов физических серверов и невозможность интеграции со многими *информационными системами* (ИС) [5]. Как следствие – повышение финансовых затрат на оборудование и обслуживание ПО, а также при нехватке вычислительных мощностей потеря производительности всей системы, что влияет на работоспособность производственной части предприятия [6]. Если рассматривать программные средства, то в большинстве случаев они применяются в организациях среднего и мелкого масштабов: в университетах, медицинских учреждениях, хостинговых компаниях и т.п. В качестве основных преимуществ необходимо отметить низкую стоимость, возможность быстрой модификации ПО и интеграцию с различными ИС [7, 8], а в качестве недостатков – довольно низкую отказоустойчивость данных систем к внешним воздействиям [9–11]. Например, в случае взаимодействия с внешними ресурсами данные программные комплексы могут подвергаться массивным DDoS-атакам, что увеличивает риск частичной или полной дестабилизации системы посредством направленности внешнего несанкционированного трафика на сетевую инфраструктуру ЭВМ [12]. Аппаратные средства АОД применяются, как правило, специализированными предприятиями [13, 14]. Например, аппаратные комплексы обработки данных широко используются в дата-центрах, специализирующихся на защите от атак внешним несанкционированным трафиком. Основными преимуществами аппаратных систем АОД являются высокая сетевая пропускная способность, производительность, отказоустойчивость, а недостатком – большие финансовые затраты на покупку и обслуживание оборудования.

В настоящее время разработками и исследованиями в области обработки данных занимаются многие ученые. Например, в [15] была реализована классификация угроз информационной безопасности распределенной системы АОД; в [16] усовершенствованы социально-экономические системы путем использования методов защиты персональных данных при их автоматизированной обработке; в [17] рассмотрены современные методы АОД тестирования. В работе [18] описана разработка алгоритма автоматизированной обработки F-рассеяния, дополняющего имеющиеся

средства автоматической обработки ионограмм для сетевых ионозондов типа DPS-4. Авторы [19] применили распределенную систему обработки данных в задаче построения автоматизированной системы видеонаблюдения, в [20] исследуется разработанный метод автоматического формирования телекоммуникационных модулей структурных элементов автоматизированных систем на основе XML-описания.

Функциональные спецификации и возможности современных информационных технологий позволяют разрабатывать альтернативные варианты АОД. Это дает возможность не только совершенствовать существующие разработки, но и создавать полностью инновационные и уникальные продукты обработки данных, которые повышают производительность ЭВМ, снижают затраты на закупку и обслуживание оборудования, а также автоматизируют обработку данных в различных организациях.

Целью авторов данной статьи является разработка модуля, предназначенного для управления физическим сервером, а также синхронной и многопоточной передачи данных (с возможностью защиты от DDoS-атак) о состоянии нагрузки удаленных выделенных физических серверов вычислительного кластера в UNIX-подобных системах.

Аналогичные решения

Удаленный клиент представляет собой инструмент для передачи и обработки информации в операционных системах по принципу «клиент–сервер». В отличие от программ удаленного администрирования такие клиенты более узкопрофильные: создаются под определенный программный комплекс. В качестве аналогичных решений, где присутствуют удаленные агенты (клиенты), рассматриваются системы, классификация которых осуществляется по критерию возможности обработки и передачи информации в высоконагруженных системах и сфере применения:

– программные комплексы по удаленному мониторингу серверного оборудования;

– программные комплексы по обслуживанию сферы IT-услуг (например, игровых сервисов, хостинг-провайдеров).

Рассмотрим принцип работы системы удаленного мониторинга серверного оборудования (рис. 1).

На физический сервер устанавливается веб-сервер. Далее инсталлируется СУБД MySQL. Соответственно, после установки данных компонентов ставится веб-система мониторинга серверного оборудования, которая управляет удаленным клиентом. Затем направляется сформированный запрос на физический сервер, где установлен удаленный клиент. После поступления запроса на получение информации о сервере (например, о его нагрузке) происходит передача данных в веб-систему, где передаваемые показатели сохраняются в MySQL и выводятся в веб-интерфейс, например, в виде графика.

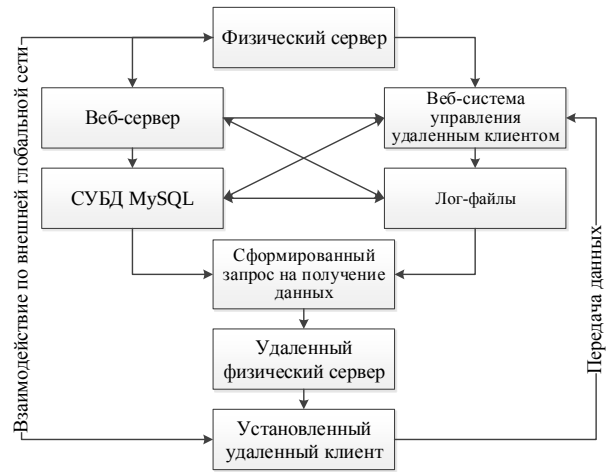

Рис. 1. Общая схема работы системы удаленного мониторинга серверного оборудования

Fig. 1. A general scheme of the remote monitoring system for server hardware

Явным преимуществом данных систем является достаточно простая реализация, что позволяет без каких-либо проблем производить мониторинг серверного оборудования. Но простая реализация таких систем является и недостатком. Например, при высокой загруженности физического сервера удаленный клиент просто не сможет обрабатывать и отправлять информацию в веб-систему из-за нехватки физических ресурсов. В качестве примера можно привести ситуацию с DDoS-атаками. Если DDoS-атака на физический сервер, где установлен удаленный клиент, не будет отражена полностью, данное ПО не сможет передавать информацию через внешнюю глобальную сеть, так как сетевой канал переполнен несанкционированным трафиком.

Одним из ярких представителей программных комплексов по удаленному мониторингу серверного оборудования является бесплатное решение Zabbix. Схема работы данного мониторинга показана на рисунке 2.

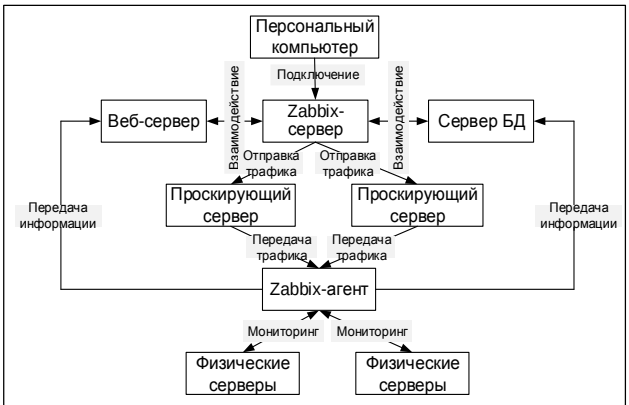

Рис. 2. Схема работы мониторинга Zabbix

Fig. 2. Zabbix monitoring operation scheme

Если рассматривать программные решения по обслуживанию сферы IT-услуг, то необходимо отметить, что данные системы представляют собой комплексные системы по обработке различных данных: платежные транзакции, считывание трафика с внешнего сетевого интерфейса, удаленная активация физических серверов и других ЭВМ. Как правило, к таким программным решениям относятся биллинговые панели управления и панели управления физическими серверами.

Биллинговые панели управления. Биллинг представляет собой систему взаимодействия с клиентами в рамках следующих операций: проведение транзакций, удаленная активация услуг, удаленная интеграция с панелями управлений физических серверов. Общая схема работы биллинговых панелей управления для предоставления телематических услуг представлена на рисунке 3.

Как правило, сначала необходимо произвести вход в веб-интерфейс. Следующий шаг – заказ услуги клиентом. Зачастую заказ выполняется только после полной оплаты клиентом стоимости услуги (исключение – тестовый период). Далее (после заказа и оплаты) осуществляется обработка услуги. Это происходит следующим образом:

– активация и обработка заказа (отправка запроса удаленному клиенту на разрешение доступа к активации заказа);

– подключение к панели управления (удаленный клиент подключается к панели управления сервером для выделения ресурсов на услугу, например, виртуальный сервер);

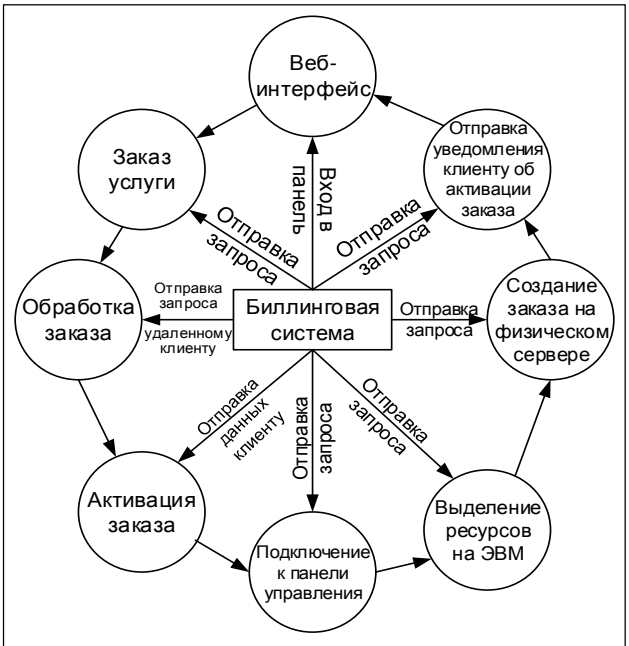

Рис. 3. Общая схема работы биллинговой системы управления

Fig. 3. A general scheme of the billing management system

– выделение ресурсов на ЭВМ с целью создания и предоставления качественной услуги клиенту;

– создание заказа на физическом сервере (создается специальный контейнер (если заказываемая услуга – виртуальный сервер), работающий на основе гипервизора);

– отправка уведомления клиенту об активации заказа (данный этап включает также отправку учетных данных от сервера; соответственно, после успешной активации услуги (в том числе и отправки всех данных для авторизации на виртуальном сервере) клиент может пользоваться предоставляемой услугой в полном объеме).

Основным преимуществом данных программных продуктов является интеграция с другими платформами с возможностью обмена информацией посредством удаленного клиента, основным недостатком – невозможность корректной работы во время атак внешним несанкционированным трафиком (DDoS-атак).

Таким образом, данное решение подходит для автоматизации бизнес-процесса с возможностью интеграции с другими сервисами посредством удаленного клиента. Однако необходимо отметить, что при массивных DDoS-атаках данное программное решение не может обрабатывать и принимать заказы от клиентов, что обусловливает финансовые убытки предприятия.

Панели управления физическими серверами. Как правило, данное программное решение представляет собой веб-интерфейс для выполнения различных команд на физическом сервере. Например, закачивание/скачивание/редактирование конфигурационных файлов различного ПО, создание БД, разграничение прав доступа (см. http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/2.jpg).

В данном случае разрешены права доступа для создания FTP-пользователей, работы с PHP, использования SSL-сертификата, ssh-клиента в браузере (Shell-клиент), а также к WWW-доменам, их директориям, к веб-диску.

Общие компоненты панелей управления физическими серверами представлены на рисунке 4.

За счет этих компонентов происходит удаленное управление ЭВМ:

– веб-интерфейс представляет собой точку входа для авторизации с последующим получением доступа к функционалу панели управления;

– удаленный клиент необходим для выполнения команд на удаленном сервере;

– модуль интеграции предназначен для взаимодействия с другими панелями управления, что необходимо для расширения функциональности панели управления, предоставляющей клиенту больше возможностей и удобств для администрирования физического сервера;

– модуль лицензирования используется для активации, деактивации и проверки лицензии панели

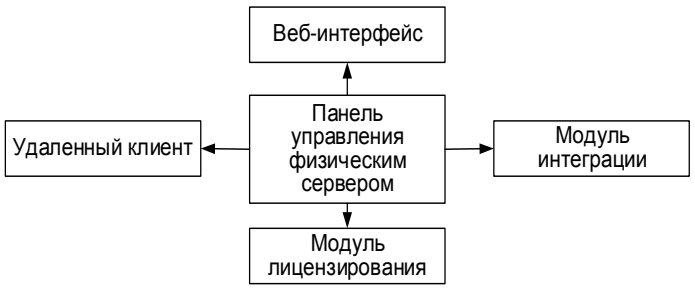

Рис. 4. Компоненты панелей управления физическими серверами

Fig. 4. The components of physical server control panels

управления (в случае, если является коммерческим проектом).

Основным преимуществом данных панелей является универсальность: они устанавливаются на множество операционных систем и имеют в своем арсенале возможность удаленного администрирования физического сервера через веб-интерфейс.

Основным недостатком данных программных решений является частичный или полный отказ в обработке данных во время DDoS-атак. Как правило, в данных панелях управления нет фильтров для отражения даже минимальных атак внешним несанкционированным трафиком. Соответственно, если на сервере канал (пропускная способность) имеет ширину 1 Гбит и атака будет идти, например, со скоростью 800 Мбит/сек., то появляются два варианта развития событий:

– панель управления будет функционировать частично (в данном случае подразумевается работа веб-интерфейса, но невозможность управления сервером посредством удаленного клиента);

– полная невозможность функционирования панели управления (в том числе и недоступность веб-интерфейса).

Таким образом, приведенные аналогичные решения, как правило, используются большинством хостинговых провайдеров в силу финансовой доступности и необходимой базовой функциональности. Существенным минусом использования данных решений является то, что при атаке несанкционированным трафиком в случае отсутствия защиты от DDoS-атак происходят частичная или полная дестабилизация в работе панели управления и, как следствие, отказ в удаленном обслуживании ЭВМ.

Разработка и реализация аппаратно-программного модуля RCM

Модуль RCM предназначен для управления физическим сервером с возможностью автоматизированной передачи данных с ЭВМ.

Применение RCM логично в области защиты информации вычислительных кластеров, физических серверов и персональных компьютеров. Например, на ЭВМ происходит атака внешним сетевым трафиком, направленная на нарушение доступности и целостности информации. Аппаратно-программный модуль RCM фиксирует DDoS и уведомляет системного администратора (по SMS и электронной почте) о необходимости предпринять меры для нейтрализации данной угрозы. В случае, если угроза не была устранена в течение одного часа, аппаратно-программный модуль начинает использовать нейронные сети для самостоятельной ликвидации DDoS-атаки. Также RCM (ежечасно) уведомляет о нагрузке на вычислительные ресурсы.

Аппаратно-программный модуль RCM обладает следующим функционалом:

– вывод данных в веб-интерфейс;

– защита от атак внешним несанкционированным трафиком в рамках выделенного канала за счет нейронной сети;

– разграничение прав доступа;

– ведение статистики с последующим отображением в веб-интерфейсе;

– взаимодействие между модулями аппаратно-программного комплекса Protection, служащего для отражения низко- и высокоактивных DoS- и DDoS-атак [21];

– удаленное управление физическим сервером.

Один из модулей под управлением клиента RCM представлен на рисунках (см. http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/3.jpg и http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/4.jpg).

Принципиальная схема модуля RCM изображена на рисунке 5. На ней представлены следующие модули:

– OAM, необходимый для вывода оценки загруженности процессоров физического сервера/вычислительного кластера в веб-часть из СУБД MySQL;

– Distribution, позволяющий равномерно распределять различные процессы по физическим и логическим ядрам процессоров физических серверов/вычислительного кластера, что позволяет более рационально использовать ресурсы ЭВМ и запускать другие ресурсоемкие задачи;

– IDLP, необходимый для распараллеливания вычислительных процессов ЭВМ, что позволяет повысить производительность сервера;

– TIS, реализованный для автоматизированной оптимизации сетевого стека в UNIX-подобных системах с возможностью анализа параметров значений приема входящего и исходящего трафиков, а также их изменения в режиме реального времени;

– модульный фильтр AntiDDoS, являющийся нейросетевым комплексным решением по фильтрации и отделению легитимного трафика от вредоносного (данный трафик направлен на отказ в удаленном обслуживании ЭВМ).

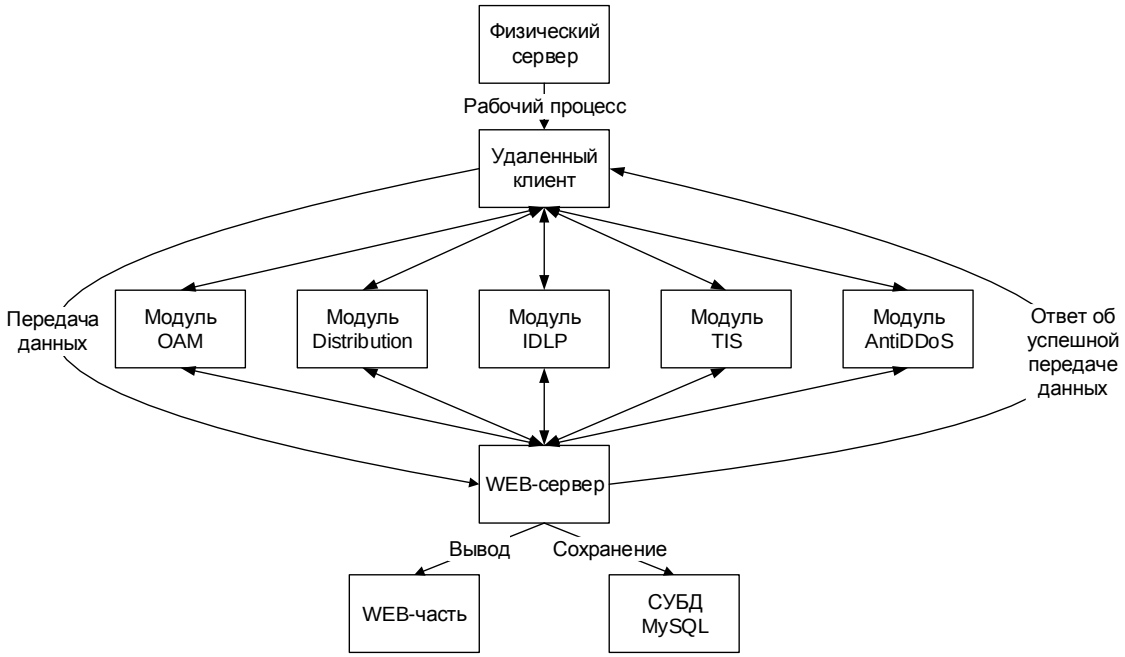

Рис. 5. Схема работы модуля RCM

Fig. 5. RCM module operation scheme

Таким образом, разработанный удаленный клиент является интегрируемой частью аппаратно-программного комплекса Protection с возможностью обработки больших объемов данных и защитой от DDoS-атак.

Основные преимущества и научная новизна

Основными преимуществами разработанного авторами программного решения являются следующие.

- Возможность быстрой обработки данных. RCM позволяет передавать данные в СУБД MySQL для вывода в веб-интерфейс со скоростью 3,4 Гбит/сек.
- Самообучающаяся нейронная сеть, позволяющая защищать от DDoS-атак физический сервер/вычислительный кластер в рамках выделенного канала. Это повышает устойчивость программного модуля к внешним воздействиям.
- Передача данных с помощью нейронных сетей. Позволяет обрабатывать и равномерно получать данные со всех подключенных к данному модулю физических серверов. Это необходимо для отслеживания состояния и загруженности физических серверов/вычислительного кластера.

Сравнение функциональных возможностей предлагаемого авторами решения и других программных продуктов представлено в таблице 1. Для него взяты одни из самых популярных решений с наличием одной из двух составляющих: удаленного клиента и аналогичных функций, которые могут выполнять как удаленный клиент, так и сама панель управления.

Таблица 1

Сравнение функциональных возможностей

Table 1

Feature comparison

Функция	RCM (авторов статьи)	ISPmanager	Game CP
Нейросетевая передача данных	+	-	-
Защита от DDoS-атак в рамках выделенного канала	+	+	-
Защита от DDoS-атак в рамках кластера	+	-	-
Вывод данных с внешнего сетевого интерфейса	+	+	-
Вывод общей загруженности ЭВМ	+	+	+
Фиксирование количества DDoS-атак с выводом в веб-интерфейс	+	-	-
Удаленное управление сервером	+	+	+
Взаимодействие с программными модулями в рамках одного аппаратно-программного комплекса	+	-	-
Возможность передачи данных в СУБД MySQL до 3,4 Гбит/сек.	+	-	-
Ведение логирования действий с сохранением в БД	+	+	+

Таким образом, из таблицы видно, что функциональность предлагаемого решения (именно удаленного клиента) больше, нежели у рассматриваемых ми-

ровых аналогов. Соответственно, RCM предоставляет больше возможностей по защите и обработке информации.

Нейронная сеть для защиты от DDoS-атак

Если рассматривать разработанную самообучающуюся нейронную сеть для защиты от DDoS-атак, то необходимо отметить, что при атаках внешним несанкционированным трафиком правила автоматически активируются для повышения защиты доступности информации ЭВМ или вычислительного кластера. Структура реализованной нейронной сети показана на рисунках (см. http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/3.jpg, http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/4.jpg, http://www.swsys.ru/uploaded/image/2019-1/2019-1-dop/5.jpg).

Под входной информацией подразумеваются пакеты сетевого трафика. Соответственно, каждый пакет распределяется в нейрон для обработки по формуле

$$R = \frac{N}{P}, \qquad (1)$$

где R – распределение сетевых пакетов по нейронам; N – количество нейронов; P – количество сетевых пакетов. Это необходимо для более быстрой фильтрации легитимного сетевого трафика от вредоносного.

Необходимо отметить, что количество нейронов в каждом слое формируется в зависимости от мощности DDoS-атаки по формуле

$$K = \sum_{i=1}^{R} P_1(x_1 + x_2 + x_3 + x_4 + \ldots + x_n), \qquad (2)$$

где K – количество нейронов; R – количество распределенных сетевых пакетов на каждый слой нейронной сети; P_1 – количество слоев нейронной сети; соответственно, x_1, x_2, x_3, x_4, x_n – количество входной информации (выражается в сетевых пакетах). Формирование количества нейронов в автоматическом режиме необходимо для рационального использования ресурсов физического сервера. Например, при атаке 100 Мбит/сек. используется гораздо меньше ресурсов, нежели при атаке мощностью 1 Гбит/сек. Соответственно, сформировавшихся и задействованных нейронов будет меньше при атаке в 100 Мбит/сек.

Количество слоев в нейронной сети формируется также автоматически по формуле

$$T = \frac{P}{Q}, \qquad (3)$$

где T – количество слоев в нейронной сети; P – количество сетевых пакетов; Q – количество свободных вычислительных ресурсов. Данная процедура, как и автоматическое формирование количества нейронов (2), необходима для рационального использования ресурсов ЭВМ. Скрытые слои (промежуточные) необходимы для обработки основного потока входящей информации (сетевых пакетов).

Самообучение нейронной сети для защиты от DDoS-атак

Самообучение нейронной сети для защиты от атак внешним несанкционированным трафиком является одним из компонентов разработанного программного модуля RCM. Структура самообучения достаточно проста и представлена в виде алгоритма на рисунке 6.

Входные данные (сетевые пакеты) берутся с внешнего сетевого интерфейса. Далее происходит автоматическое формирование слоев и нейронов сети. Следующим этапом является выборка нейронной сетью, представляющая собой входной набор полученных сетевых пакетов с распределением по нейронам. Далее происходит распространение сигнала по нейронной сети (обработка) данных. В конечном итоге нейронная сеть сама определяет, ошибочно обучение или нет.

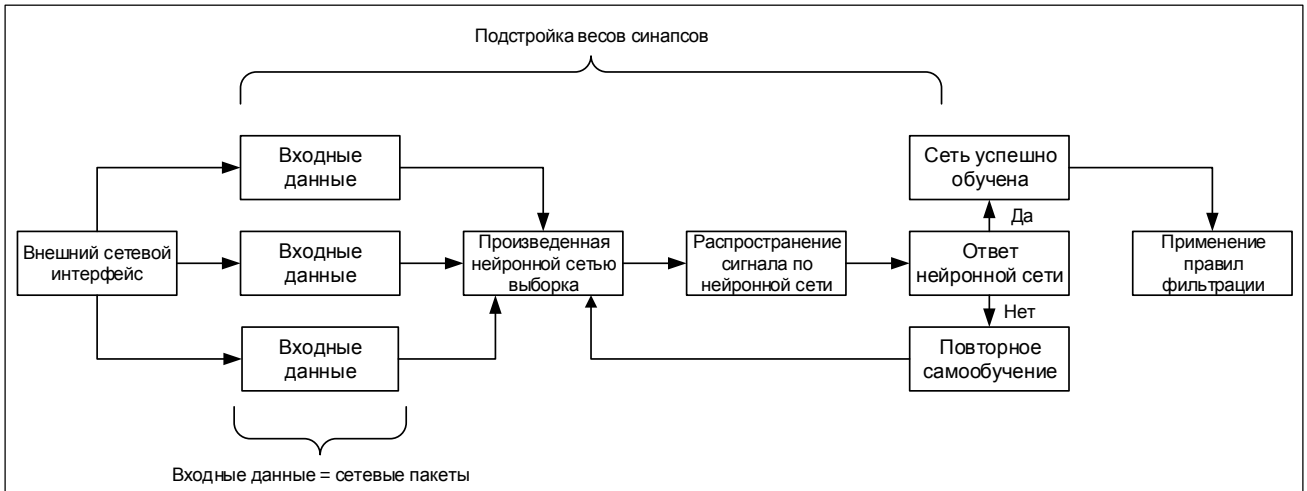

Рис. 6. Разработанный алгоритм обучения нейронной сети

Fig. 6. The developed neural network learning algorithm

Если ошибочно, то производится повторное обучение. Если ответ сети положительный, применяются правила фильтрации несанкционированного трафика.

Самообучение основано на комплексном подходе: объединены сигнальный и дифференциальный способы обучения. Первым шагом является изменение весовых коэффициентов синапсов:

$$b_{ij}(t) = b_{ij}(t-1) + mv_i^{(P_1-1)}v_j^{(P_1)}, \quad (4)$$

где $b_{ij}(t)$ и $b_{ij}(t-1)$ – весовые коэффициенты синапса, соединяющего нейроны на этапах итерации t и $t-1$; $v_i^{(P_1-1)}$ – полученное выходное значение нейрона i-го слоя (P_1-1); $v_j^{(P_1)}$ – значение нейрона (выходное) j-го слоя P_1; m – значение скорости самообучения нейронной сети (коэффициент).

Далее необходимо дифференцировать данную формулу для получения синтеза сигнального и дифференциального методов самообучения нейронной сети:

$$b_{ij}(t) = b_{ij}(t-1) + m\left[v_i^{(P_1-1)}(t) - v_i^{(P_1-1)}(t+1)\right]\left[v_j^{(P_1)}(t) - v_j^{(P_1)}(t+1)\right], \quad (5)$$

где $v_j^{(P_1)}(t)$ и $v_i^{(P_1-1)}(t+1)$ – значения нейрона при выходе на итерациях t, $t-1$ и $t+1$. Необходимо отметить, что после синтеза сигнального и дифференциального способов обучения усилились связи между возбудимыми нейронами, а также повысилось обучение синапсов. Это позволяет нейронной сети самостоятельно обучаться в достаточно короткие сроки.

Нейронная сеть для передачи данных между модулями комплекса Protection

Если рассматривать искусственные нейронные сети для передачи данных между программными компонентами комплекса Protection, то необходимо отметить, что разработанная нейронная сеть позволяет ускорить обмен информацией между модулями разработанного решения по защите от атак внешним несанкционированным трафиком. Структура нейронной сети и алгоритм самообучения представлены на рисунках 7 и 8.

Входной слой представляет собой всю исходящую от модулей комплека Protection информацию. В исходящей информации передаются следующие данные: загруженность физических ресурсов кластера, количество DDoS-атак за различные промежутки времени, внесенные правила для отделения легитимного и вредоносного трафиков, количество перенесенных вычислительных процессов по физическим и логическим ядрам процессоров кластера, количество данных, отправленных в различные БД. Все вышеперечисленные данные обрабатываются в промежуточных слоях, и в качестве выходных данных удаленный модуль RCM получает отсортированные значения, показывающие состояние вычислительного кластера.

В данной нейронной сети, как и в искусственной нейронной сети, для защиты от атак внешним несанкционированным трафиком реализован синтез сигналь-

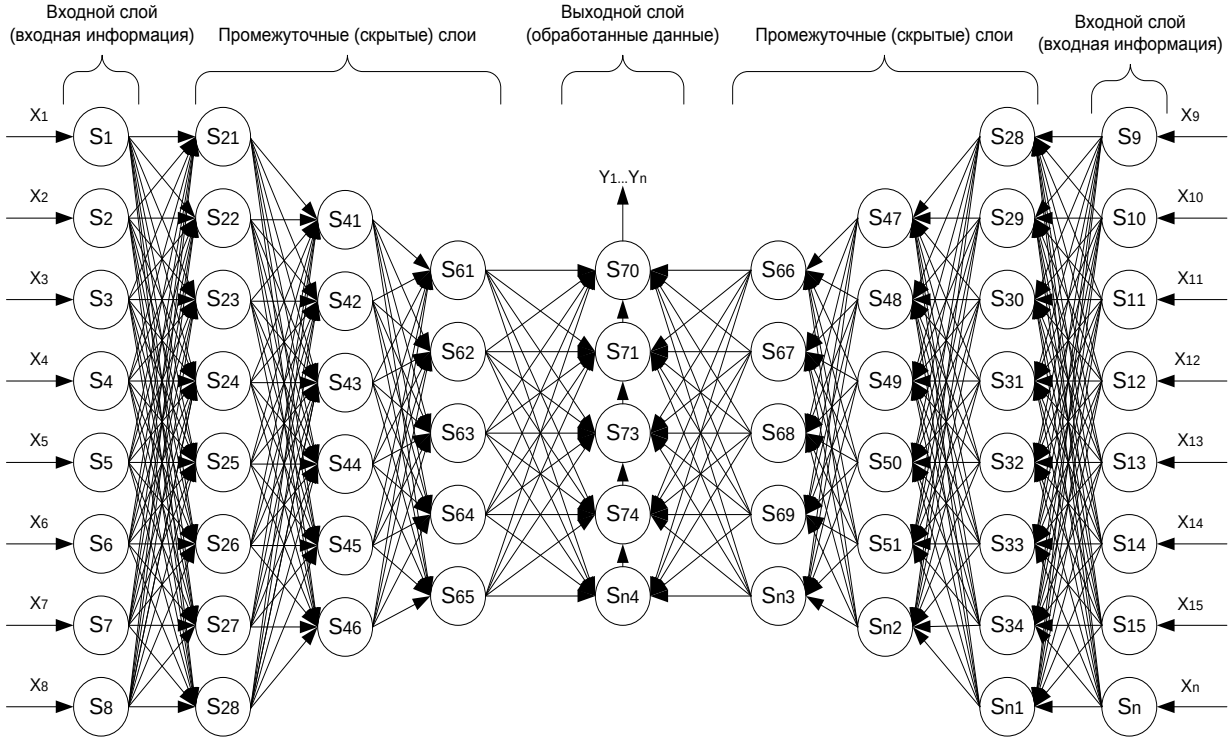

Рис. 7. Структура нейронной сети

Fig. 7. The neural network structure

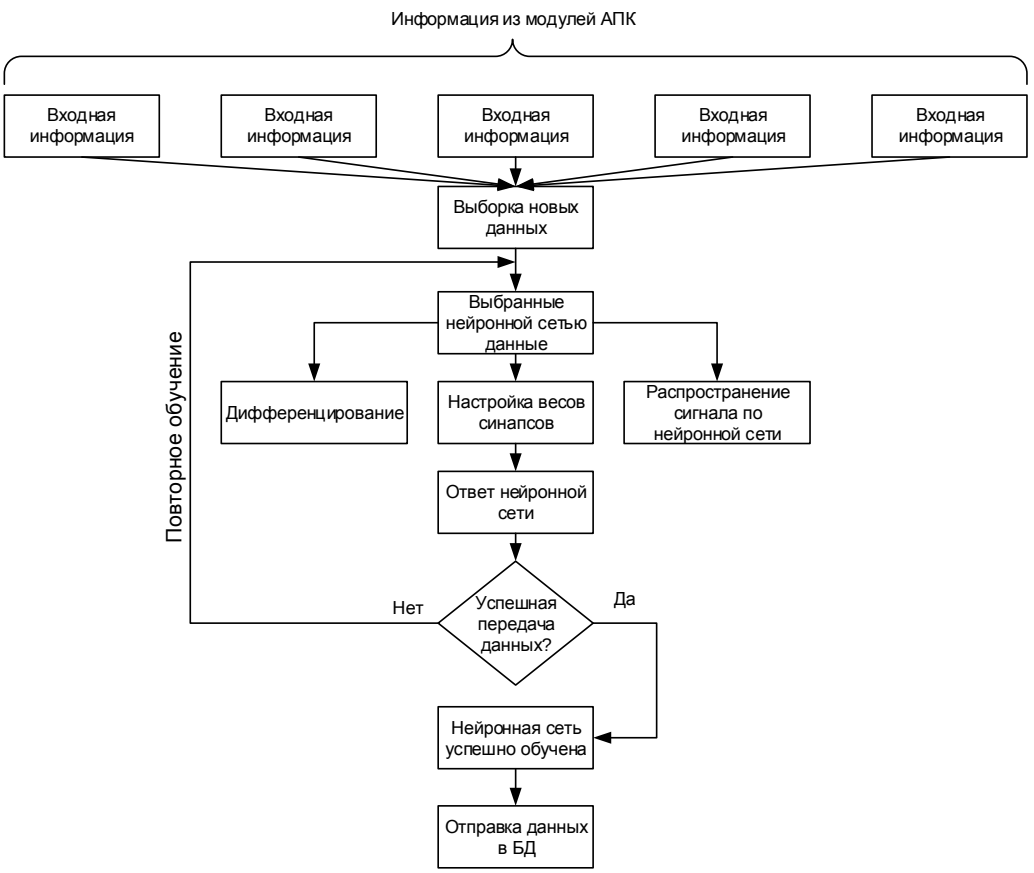

Рис. 8. Разработанный алгоритм самообучения искусственной нейронной сети

Fig. 8. The developed self-learning algorithm for an artificial neural network

ного и дифференцированного методов самообучения нейронной сети. Различие заключается во входных данных: в данном случае информация берется не из одного источника, а из нескольких (модули аппаратно-программного комплекса) и выходит на один модуль (RCM). В случае нейронной сети для отражения атак внешним несанкционированным трафиком один источник информации (внешний сетевой интерфейс).

Таким образом, реализованная нейронная сеть позволяет ускорить и сделать более качественный обмен данными между модулями Protection за счет обработки данных в нескольких слоях.

Апробация удаленного клиента RCM

После разработки удаленного клиента RCM проводится тестирование, необходимое для выявления эффективности предлагаемого авторами решения. С целью более точного определения значений средней нагрузки в календарный день данные вынесены в отдельные таблицы.

Потребление вычислительных ресурсов без каких-либо атак сетевым трафиком и при активированном удаленном клиенте (в течение 10 календарных дней) отражено в таблице 2. По данным этой таблицы, средняя нагрузка на физические ресурсы модулем RCM следующая: центральный процессор (CPU) – 0,34 %, твердотельный накопитель (SSD) – 0,57 %.

Потребление вычислительных ресурсов при атаках сетевым трафиком и при включенном удаленном клиенте RCM (в течение 10 календарных дней и с таким же количеством отправляемой информации) представлено в таблице 3. Исходя из ее данных, средняя нагрузка на физические ресурсы модулем RCM следующая: центральный процессор (CPU) – 4,62 %, твердотельный накопитель (SSD) – 2,53 %.

Таким образом, полученные результаты доказывают эффективность и целесообразность применения разработанного аппаратно-программного модуля.

Тестирование разработанного аппаратно-программного модуля в «боевом» режиме (при DDoS-атаках и большом количестве обрабатываемой информации) проводилось в одном из московских центров обработки данных на следующем оборудовании: количество физических серверов – 30, процессор Intel Xeon 5690 (CPU – 60, физических ядер – 360, количество потоков – 720), оперативная память – 960 Гб, твердотельные накопители – RAID 10 (Intel S3710 SSDSC2BA012T401 800 Гб каждый), внешний сетевой

Таблица 2

Потребление вычислительных ресурсов без DDoS-атак

Table 2

Computing resource consumption without DDoS attacks

Ситуация	День									
	1	2	3	4	5	6	7	8	9	10
	Количество отправляемой информации, Гбит/сек.									
	0,80	2,14	3,67	5,18	6,23	7,29	8,65	9,00	10,12	11,00
	Нагрузка на центральный процессор, %									
Старт модуля	0,02	0,04	0,06	0,12	0,18	0,24	0,43	0,50	0,54	0,62
Рестарт модуля	0,03	0,14	0,17	0,19	0,24	0,30	0,32	0,33	0,34	0,35
Отправка данных в СУБД MySQL	0,09	0,18	0,27	0,36	0,45	0,54	0,63	0,72	0,81	0,99
	Нагрузка на твердотельный накопитель, %									
Старт модуля	0,08	0,14	0,26	0,32	0,48	0,56	0,70	0,80	0,94	1,00
Рестарт модуля	0,09	0,23	0,67	0,69	0,70	0,73	0,75	0,80	0,85	0,90
Отправка данных в СУБД MySQL	0,15	0,18	0,24	0,33	0,48	0,99	1,09	1,19	1,25	1,26

Таблица 3

Потребление вычислительных ресурсов при DDoS-атаках

Table 3

Computing resource consumption during DDoS attacks

Ситуация	День									
	1	2	3	4	5	6	7	8	9	10
	Атака сетевым трафиком, Гбит/сек.									
	0,80	2,65	4,00	5,90	6,76	7,80	10,25	14,47	15,50	18,80
	Нагрузка на центральный процессор, %									
Старт модуля	0,90	1,80	2,40	3,20	3,87	4,90	5,11	6,18	7,14	8,00
Рестарт модуля	1,10	1,90	2,65	3,65	4,00	5,00	5,78	6,33	7,64	8,56
Отправка данных в СУБД MySQL	1,50	2,00	3,59	4,56	4,70	5,00	5,50	6,20	7,00	8,70
	Нагрузка на твердотельный накопитель, %									
Старт модуля	0,50	0,60	0,70	0,80	0,90	1,00	1,10	1,20	1,30	1,80
Рестарт модуля	0,60	0,70	0,80	0,90	1,00	1,10	1,20	1,30	1,40	2,00
Отправка данных в СУБД MySQL	1,00	2,00	3,00	4,00	5,00	6,00	7,00	8,00	9,00	10,00

канал – 20 Гбит/сек., внутренний сетевой канал (локальная сеть) – 100 Гбит/сек.

Данное оборудование соответствует современным требованиям и позволяет обрабатывать большие объемы данных.

Необходимо отметить, что после апробации аппаратно-программного модуля RCM он был окончательно инсталлирован в аппаратно-программный комплекс Protection и успешно автоматизировал обработку его информации.

Заключение

В ходе проведенных исследований, разработок и реализаций был предложен алгоритм обучения искусственной нейронной сети, позволяющий реализовать структуру ее самообучения (без учителя) на программном уровне. На вход подается информация из модулей комплекса Protection. При успешном выполнении данного алгоритма обработанная информация в автоматизированном режиме передается в БД.

Синтез сигнального и дифференциального способов обучения нейронной сети без учителя позволяет достаточно быстро обмениваться данными между модулями комплекса Protection, а также в автоматизированном режиме защищать от DDoS-атак физический сервер в рамках выделенного сетевого канала.

Кроме того, разработан удаленный клиент RCM, позволяющий передавать большие объемы данных в СУБД MySQL за счет разработанной нейронной сети. В процессе передачи вся информация сортируется по таблицам в БД и выводится в веб-интерфейс.

Проведено множество тестирований, доказывающих целесообразность использования удаленного клиента RCM. Средняя нагрузка на центральный процессор варьируется от 0,02 до 8,70 %. Достаточно низкая нагрузка на CPU позволяет запускать многочисленные ресурсоемкие процессы как в «боевом» (во время DDoS-атаки), так и в обычном режимах без каких-либо потерь производительности. Потребление ресурсов SSD-накопителя колеблется от 0,80 до 10,00 %. Столь небольшая нагрузка на твердотельный накопитель

предоставляет возможность увеличения пропускной способности канала передачи данных (передача информации между модулями комплекса Protection до 15,56 Гбит/сек.). Таким образом, низкая нагрузка на вычислительные ресурсы позволяет создавать скоростную обработку информации в автоматизированном режиме с возможностью выборочного уведомления системного администратора.

Литература

1. Пальчевский Е.В., Халиков А.Р. Равномерное распределение нагрузки аппаратно-программного ядра в UNIX-системах // Тр. ИСП РАН. 2016. Т. 28. Вып. 1. С. 93–102.
2. Атрощенко В.А, Тымчук А.И. К вопросу выбора наилучшего уровня RAID для хранилищ данных информационной системы, обеспечивающей быструю обработку больших данных // Современные наукоемкие технологии. 2017. № 4. С. 12–16.
3. Майоров А.А., Матерухин А.В. Анализ существующих технологий обработки потоков пространственно-временных данных для современных информационно-измерительных систем // Измерительная техника. 2017. № 4. С. 31–34.
4. Лебеденко Е.В., Минайчев А.А. Распределение нагрузки в системе обработки мультисервисных данных высокоскоростных каналов // Новые информационные технологии в автоматизированных системах. 2017. № 20. С. 146–149.
5. Пальчевский Е.В., Халиков А.Р. Автоматизированная система обработки данных в UNIX-подобных системах // Программные продукты и системы. 2017. Т. 30. № 2. С. 227–234. DOI: 10.15827/0236-235X.118.227-234.
6. Акимкина Э.Э. Рекомендации по развертыванию многомерных систем аналитической обработки данных // Информационно-технологический вестник. 2017. № 1. С. 68–80.
7. Бурдонов И.Б, Косачев А.С. Система автоматов: композиция по графу связей // Тр. ИСП РАН. 2016. Т. 28. Вып. 1. С. 131–150. DOI: 10.15514/ISPRAS-2016-28(1)-8.
8. Steinberg O.B. Circular shift of loop body – programme transformation, promoting parallelism // Вестн. ЮУрГУ: Математическое моделирование и программирование. 2017. Т. 10. № 3. С. 120–132 (англ.).
9. Посыпкин М.А., Тант Син С.Т. О распараллеливании метода динамического программирования для задачи о ранце // Intern. J. of Open Information Technologies. 2017. Т. 5. № 7. С. 1–5.
10. Овчаренко О.И. Об одном подходе к распараллеливанию метода циклической редукции для решения систем уравнений с трехдиагональной матрицей // Современные тенденции развития науки и производства: сб. матер. III Междунар. конф. Кемерово, 2016. С. 152–155.
11. Пелипец А.В. Распараллеливание итерационных методов решения систем линейных алгебраических уравнений на реконфигурируемых вычислительных системах // Суперкомпьютерные технологии (СКТ-2016): матер. IV Всерос. науч.-технич. конф. Ростов н/Д.: Изд-во ЮФУ, 2016. С. 194–198.
12. Белим С.В., Кутлунин П.Е. Выделение контуров на изображениях с помощью алгоритма кластеризации // Компьютерная оптика. 2015. Т. 39. № 1. С. 119–124.
13. Иванова Е.В., Соколинский Л.Б. Методы параллельной обработки сверхбольших баз данных с использованием распределенных колоночных индексов // Программирование. 2017. № 3. С. 3–21.
14. Мовчан А.В., Цымблер М.Л. Параллельный алгоритм поиска локально похожих подпоследовательностей временного ряда для ускорителей на базе архитектуры INTEL MIC // Суперкомпьютерные дни в России: тр. Междунар. конф. М., 2015. С. 332–343.
15. Волосенков В.О., Гаврилов А.Д. Классификация угроз информационной безопасности распределенной автоматизированной системы обработки данных // Проблемы безопасности Российского общества. 2016. № 1. С. 183–187.
16. Погребняк А.О. Совершенствование социально-экономических систем путем использования методов защиты персональных данных при их автоматизированной обработке // Современные проблемы управления природными ресурсами и развитием социально-экономических систем: матер. XII Междунар. научн. конф. М., 2016. С. 460–467.
17. Тагиев Р.Б., Тулаев А.А. Современные методы автоматизированной обработки данных тестирования // Молодой исследователь Дона. 2016. № 1. С. 32–36.
18. Телегин В.А., Панченко В.А., Жбанков Г.А., Рождественская В.И. Автоматизированная обработка данных f-рассеяния // Physics of auroral phenomena. 2016. Т. 39. № 1. С. 130–133.
19. Кондратьев А.А., Беззубцев А.Ю., Смирнов А.В. Применение распределенной системы обработки данных в задаче построения автоматизированной системы видеонаблюдения // Программные системы: теория и приложения. 2017. Т. 8. № 1. С. 135–149.
20. Молев А.А. Метод автоматического формирования телекоммуникационных модулей структурных элементов автоматизированных систем на основе XML-описания // Информационно-управляющие системы. 2017. № 1. С. 40–49.
21. Пальчевский Е.В., Халиков А.Р. Система распараллеливания нагрузки на ресурсы ЭВМ // Программные продукты и системы. 2018. Т. 30. № 2. С. 295–302. DOI: 10.15827/0236-235X.122.295-302.

Software & Systems
DOI: 10.15827/0236-235X.125.092-102

Received 24.09.18
2019, vol. 32, no. 1, pp. 092–102

The development of a remote client for automated data transfer in UNIX-based systems

E.V. Palchevsky [1], *Postgraduate Student, teelxp@inbox.ru*
A.R. Khalikov [1], *Ph.D. (Physics and Mathematics), Associate Professor, khalikov.albert.r@gmail.com*

[1] *Ufa State Aviation Technical University, Ufa, 450008, Russian Federation*

Abstract. This paper is devoted to the development of a hardware-software module for UNIX-based systems, called RCM (Remote Client Management). The module provides data transfer within the Protection hardware-software complex protecting from DDoS-attacks. The main RCM features are high-speed data processing and protection from DDoS attacks based on neural networks.

The paper discusses the problem of processing software data and substantiates the need for a mathematical analysis to identify new self-learning methods of neural networks. The paper also presents the developed self-learning neural networks necessary for data

transmission and protection from DDoS attacks. The developed method for self-learning a neural network is based on combining signal and differential learning methods. Therefore, the neural network can quickly learn in a short time. The functionality of the developed remote client allows managing this module both through the web interface and the console mode.

Testing of the developed software in the combat mode has shown the load values for computer resources. Long-term testing of RCM has shown quite a low load on the central processor and solid-state drive during DDoS-attacks. Naturally, optimal load allows not only processing large information flows, but also provides the possibility of parallel launch of resource-intensive computing processes without any disruption to the operating system operation.

The testing has been carried out on the computational cluster servers (together with APK "Protection") in one of the Moscow data centers, where RCM performed stably.

Keywords: information, data transfer, networks, DDoS, AntiDDoS, UNIX, operation system, data, data processing, information security.

References

1. Palchevsky E.V., Khalikov A.R. Uniform load distribution of the hardware-software core in UNIX-systems. *Proc. of ISP RAS*. 2016, vol. 28, no. 1, pp. 93–102 (in Russ.).

2. Atroshchenko V.A., Tymchuk A.I. To the question of choosing the best RAID level for data warehouses of the information system that provides fast processing of large data. *Modern Science Technologies*. 2017, no. 4, pp. 12–16 (in Russ.).

3. Maiorov A.A., Materukhin A.V. Analysis of existing technologies used to process streams of spatio-temporal data for modern information measurement systems. *Measurement Techniques*. 2017, vol. 60, iss. 4, pp. 350–354.

4. Lebedenko E.V., Minaychev A.A. Load distribution in the multiservice data processing system in high-speed channels. *New Information Technologies in Automated Systems*. 2017, no. 20, pp. 146–149 (in Russ.).

5. Palchevsky E.V., Khalikov A.R. Automated data processing system in UNIX-like systems. *Software & Systems*. 2017, vol. 30, no. 2, pp. 227–234 (in Russ.). DOI: 10.15827/0236-235X.118.227-234.

6. Akimkina E.E. Recommendations for multidimensional system deployment for analytical processing. *Information Technology Bulletin*. 2017, no. 1, pp. 68–80 (in Russ.).

7. Burdonov I.B., Kosachev A.S. System of automatons: composition by the connection graph. *Proc. of ISP RAS*. 2016, vol. 28, iss. 1, pp. 131–150 (in Russ.). DOI: 10.15514/ISPRAS-2016-28(1)-8.

8. Shteinberg O.B. Circular shift of the loop body – programme transformation, promoting parallelism. *Bulletin of South Ural State Univ. Series: Mathematical Modeling and Programming*. 2017, vol. 10, no. 3, pp. 120–132.

9. Posypkin M.A., Thant Sin Si Thu. On the parallelization of dynamic programming method for knapsack problem. *Intern. J. of Open Information Technologies*. 2017, vol. 5, no. 7, pp. 1–5.

10. Ovcharenko O.I. On one approach to parallelizing the cyclic reduction method to solve equation systems with a tridiagonal matrix. *Current Trends in the Development of Science and Production: Proc. 3rd Intern. Pract. Conf*. Kemerovo, West-Siberian Scientific Center, 2016, pp. 152–155 (in Russ.).

11. Pelipets A.V. Parallelization of iterative methods for solving linear algebraic equation systems on reconfigurable computing systems. *Supercomputer Technologies (SKT-2016): Proc. 4th All-Russ. Sci. and Tech. Conf*. Rostov-on-Don, Southern Federal Univ., 2016, pp. 194–198 (in Russ.).

12. Belim S.V., Koutlunin P.E. Isolation of image contours using the clustering algorithm. *Computer Optics*. 2015, vol. 39, no. 1, pp. 119–124 (in Russ.).

13. Ivanova E.V., Sokolinsky L.B. Methods of parallel processing of ultra-large databases using distributed column indexes. *Programming*. 2017, no. 3, pp. 3–21 (in Russ.).

14. Movchan A.V., Tsymbler M.L. A parallel algorithm for searching locally similar subsequences of a time series for accelerators based on the INTEL MIC architecture. *Supercomputer Days in Russia: Proc. Intern. Conf*. Moscow, MSU Publ., 2015, pp. 332–343 (in Russ.).

15. Volosenkov V.O., Gavrilov A.D. Classification of information security threats of a distributed automated data processing system. *The Problems of the Russian Society Security*. Moscow, MIIT Publ., 2016, no. 1, pp. 183–187 (in Russ.).

16. Pogrebnyak A.O. The development of socio-economic systems using personal data protecting methods during their automated processing. *Modern Problems of Natural Resources Management and Social And Economic Systems Development. Proc. 12th Intern. Sci. Conf*. Moscow, 2016, pp. 460–467 (in Russ.).

17. Tagiev R.B., Tulaev A.A. Modern methods of automated processing of testing data. *Young Researcher of Don*. Rostov-on-Don, Don state Technical Univ. Publ., 2016, no. 1, pp. 32–36 (in Russ.).

18. Telegin V.A., Panchenko V.A., Zhbankov G.A., Rozhdestvenskaya V.I. Automated processing of f-scattering data. *Physics of Auroral Phenomena*. Polar Geophysical Institute Publ., Murmansk, 2016, vol. 39, no. 1, pp. 130–133 (in Russ.).

19. Kondratyev A.A., Bezzubtsev A.Yu., Smirnov A.V. Application of the distributed data processing system in the task of constructing an automated video surveillance system. *Software Systems: Theory and Applications*. Veskovo, 2017, vol. 8, no. 1, pp. 135–149 (in Russ.).

20. Molev A.A. The method of automatic formation of telecommunication modules of structural elements of automated systems based on XML-description. *Information and Control Systems*. St. Petersburg, 2017, no. 1, pp. 40–49 (in Russ.).

21. Palchevsky E.V., Khalikov A.R. System for parallelizing the load on computer resources. *Software & Systems*. 2018, vol. 30, no. 2, pp. 295–302 (in Russ.). DOI: 10.15827/0236-235X.122.295-302.