ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ АНОНИМНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИЙ ВЕБ-ПРОКСИ

Маркин Д.О., Архипов П.А., Галкин А.С.[1]

В статье рассмотрена концепция построения системы анонимного доступа к удаленным ресурсам на базе веб–технологий с использованием языков программирования PHP/Perl. Проведен анализ типов прокси–серверов, на основе которых осуществляется построение анонимных сетей. Обосновано применение технологии веб–прокси–серверов для решения задачи построение анонимной сети. Выделены достоинства и недостатки данной технологии. Описаны принципы использования технологии терминальных программ и активных данных применительно к веб–прокси–серверам. Предложен перечень технических задач, которые могут быть решены при реализации технологии терминальных программ и активных данных на основе веб–прокси–серверов. Представлена структура прототипа анонимной сети на базе веб–прокси–серверов, на основе которой проведена серия экспериментов по исследованию устойчивости. Проведен анализ устойчивости программно–аппаратного обеспечения при нагрузочном тестировании с использованием веб–прокси–серверов. Описание и результаты экспериментов приведены в работе. Представлены выводы о перспективах применения технологии веб–прокси для реализации системы анонимного доступа. Показано, что анонимные сети на базе веб–прокси серверов являются уязвимыми к повышенной нагрузке, связанной с ограниченными вычислительными возможностями аппаратной платформы, однако в то же время, являются потенциальными источниками такой нагрузки в отношении сторонних ресурсов.

***Ключевые слова**: анонимная сеть, веб–прокси, самомаршрутизация, активные данные, терминальные программы, луковая маршрутизация, чесночная маршрутизация*

Введение

Существующие современные условия удаленного доступа к информационным ресурсам позволяют говорить о том, что простое обращение к информационному сервису оставляет значительное количество «следов» такого обращения в информационных log-файлах провайдеров услуг связи, промежуточных узлах на пути следования данных, а также программном обеспечении и удаленных базах данных разработчиков программного обеспечения, которое использует пользователь. Такое положение дел свидетельствует об установлении негласного тотального наблюдения за пользователями глобальной сети, что в ряде случаев является недопустимым. Это прямо нарушает право человека на тайну связи, являющееся неотъемлемым правом личности, признанным на международном уровне.

Одно из решений данной проблемы – это использование анонимных сетей, представляющих собой компьютерные сети, построенные поверх глобальной сети, в основе которых лежит распределенный характер ее узлов, а также многоуровневая криптографическая защита адресной информации.

1. Построение анонимной сети на основе технологий веб-прокси

При организации анонимной сети вместо одного прокси-сервера между компьютером пользователя и удаленными информационными ресурсами находится сеть прокси-серверов. Их классификация представлена на рисунке 1.

Выделяют отдельную категорию прокси-серверов – веб-прокси-серверы, представляющие собой веб-приложения, установленные на веб-сервере (например на базе Perl, Python или PHP-скриптов).

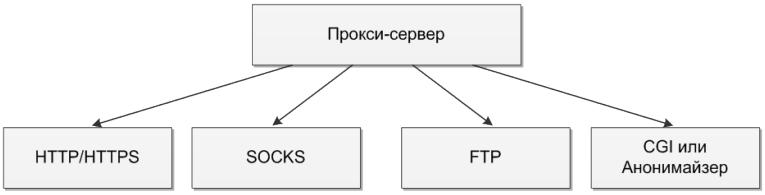

***Рис. 1** . Классификация прокси-серверов по типу*

1 Маркин Дмитрий Олегович, Архипов Павел Андреевич, Галкин Алексей Сергеевич, сотрудники Академии ФСО России, г. Орёл, admin@nikitka.net

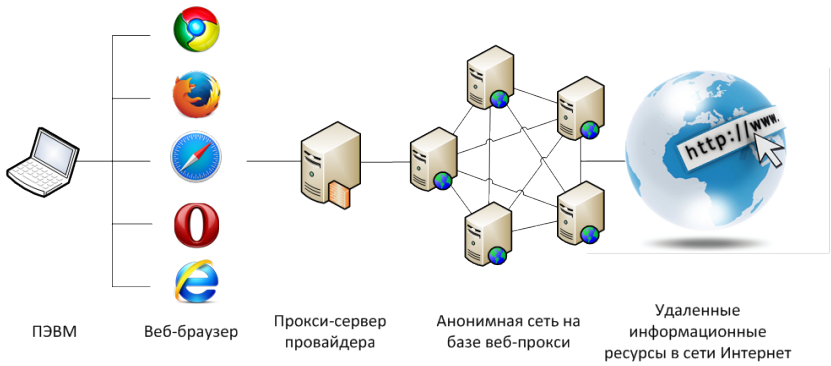

***Рис. 2**. Структура анонимной сети на основе технологии веб-прокси*

В настоящее время существует несколько готовых решений веб-прокси-серверов, к которым относятся CGIProxy (на базе CGI-скриптов и OpenSSL) [1]; Glype Proxy (на базе PHP) [2]; PHProxy [3]; Zelune (на базе PHP); Cohula (на базе Java) [4].

Построение анонимных сетей на базе веб-прокси является достаточно тривиальной задачей, однако она не получила широкого распространения в связи с рядом проблем, связанных с ограниченной функциональностью веб-серверов. К таким проблемам относятся:

– внесение адреса веб-сервера, на котором функционирует веб-прокси, в список запрещенных и, соответственно, блокирование доступа к нему на уровне сети;

– низкая скорость соединения между веб-прокси и удаленными ресурсами;

– наличие скриптов в коде удаленного информационного ресурса, которые исполняются на клиентской стороне и должны в «прозрачном» режиме передаваться через веб-прокси.

В то же время использование веб-прокси, в отличие от классических программно-аппаратных платформ, имеет ряд преимуществ:

– может быть использована арендованная или бесплатная программно-аппаратная платформа, не требующая существенных материальных и временных затрат для развертывания;

– установка и настройка программного обеспечения веб-прокси не требует глубоких специальных знаний и позволяет в сжатые сроки получить работоспособный прокси-сервер;

– существует большое количество доступных программно-аппаратных платформ – хостингов, которые могут быть использованы в качестве веб-прокси за сравнительно низкую плату или вовсе бесплатно.

Совокупность данных факторов предопределяет высокую доступность технологии веб-прокси, а современные технические возможности веб-серверов и серверных расширений, позволяющих обрабатывать Perl, Python, PHP и другие скрипты, предоставляют широкие возможности для разработчиков.

Веб-прокси, выступающий в качестве посредника между пользователем и информационными ресурсами глобальной сети, позволяет частично решить задачу анонимного доступа к ресурсам или обойти ограничения локальной сети пользователя, однако он достаточно уязвим к обнаружению и блокированию как со стороны администраторов локальной сети пользователя, так и со стороны ресурсов глобальной сети.

Схема доступа к удаленным ресурсам посредством анонимной сети на базе веб-прокси представлена на рисунке 2 .

Сеть представляет собой совокупность не связанных между собой веб-узлов. Каждый узел является веб-сервером. На каждом веб-узле располагается скрипт или набор скриптов, разработанных на PHP и Perl. Такие скрипты предназначены для обработки поступающих на веб-сервер специальным образом сформированных запросов и последующей передачи их следующему веб-узлу в цепочке маршрута в анонимной сети.

Использование технологий веб-прокси позволяет реализовать концепцию активных данных [5] и так называемых терминальных программ [6]. Активные данные, одновременно являясь терминальными программами, способны настраивать программно-определяемое оборудование, требуемое для их распространения, и могут управлять процессом своего распространения в коммуникационной среде.

Предоставление терминальным программам возможности производить активные действия как на устройствах-приемниках, так и на всех промежуточных узлах, участвующих в процессе инфокоммуникации, расширяет возможности сетей передачи

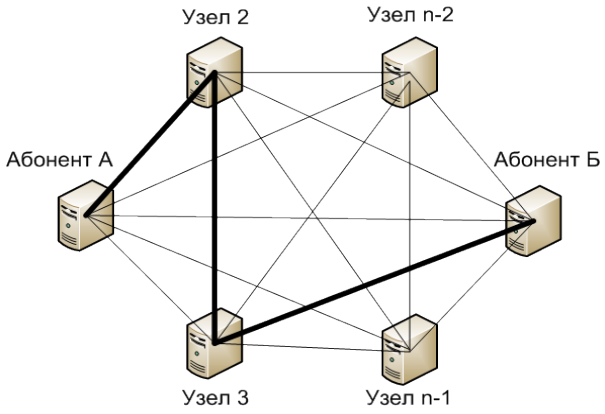

***Рис. 3**. Пример построения маршрута в анонимной сети*

данных, делая их программно-определяемыми системами [7], что, в свою очередь, обеспечивает возможность динамически создавать специализированные сети передачи данных из устройств общего назначения. Одной из задач создания таких сетей является реализация функции самомаршрутизации, рассмотренной в работе [5]. Для реализации функций самомаршрутизации (функции, при которой пакет, попав на промежуточный узел сети, принимает решение о маршруте своего дальнейшего перемещения на основе текущих данных об инфокоммуникационном окружении) [5] должен предоставляться список «ближних соседей» – устройств, с которыми соединение уже установлено или может быть установлено непосредственно. Такой список может формироваться и обновляться в реальном времени за счет функции мониторинга коммуникационного ресурса.

Технологии веб-прокси являются подходящим инструментом, не требующим разработки дополнительных механизмов реализации концепции терминальных программ. Иными словами, при передаче данных по анонимной сети на базе веб-прокси в качестве полезной нагрузки в данных приложения HTTP могут быть заложены инструкции в виде скрипта. Такой скрипт, попав на i-й удаленный узел – веб-прокси, после его исполнения может решать ряд задач, позволяющих существенно усилить защищенность анонимной сети:

– сгенерировать новый маршрут следования передаваемых данных;

– сгенерировать новый исполняемый скрипт с необходимыми функциями;

– выполнить запрос к удаленному узлу(ам) или осуществить информационный обмен со сменой протокола доступа (например по протоколу Telnet, SSH и др.).

Принцип работы сети анонимного доступа на базе веб-прокси заключается в следующем.. Пусть абонент А желает связаться с абонентом Б. У абонента А хранится полный список узлов анонимной сети. Он формирует маршрут пересылки запроса и отсылает запрос на первый узел из этого списка со своим сообщением и с параметром узла назначения (в качестве параметра выступает его имя). В нашем случае параметром является абонент Б. К примеру, запрос пришел на узел 2, который выступает в роли прокси-сервера. Узел 2 выбирает следующий узел и отправляет запрос с передаваемым сообщением и узлом назначения. Эти операции производятся до тех пор, пока запрос не достигнет получателя. Пример работы анонимной сети представлен на рисунке 3.

Одной из основных проблем реализации сети является ее устойчивость к раскрытию параметров и атакам типа «отказ в обслуживании». Устойчивость определяется надежностью, живучестью и помехоустойчивостью сети. Для повышения устойчивости сети используются различные меры:

– оптимизация топологии сети для упрощения ее адаптации к условиям, возникающим в результате воздействия различных дестабилизирующих факторов;

– рациональная маршрутизация между узлами сети

– применение специальных мер защиты сети и ее элементов от влияния источников помех различного характера;

– развитие системы резервирования;

– внедрение автоматизированных систем управления, организующих работу по перестройке и восстановлению сети, поддержанию ее работоспособности в различных условиях и др.

2. Постановка задачи

В данной работе предложена схема эксперимента, позволяющая исследовать устойчивость прототипа анонимной сети на базе веб-прокси, построенной на PHP- и Perl-скриптах. Для иссле-

дования устойчивости проведен ряд экспериментов. Задача – исследовать особенности передачи данных через группу веб-узлов, являющихся промежуточными, для маршрута передаваемых через моделируемую анонимную сеть данных.

Условия эксперимента

Аппаратное обеспечение: ЭВМ на базе Intel Core i5-3230M 2.60GHz, 8 Гбайт ОЗУ, система x64, Windows 10.

Программное обеспечение:

1. Веб-сервер Apache 2.x.
2. Модуль PHP.
3. Perl.
4. Веб-обозреватели «Яндекс.Браузер», Opera.

На локальном веб-сервере развернута группа виртуальных узлов с заданными доменными именами. На виртуальных узлах установлены скрипты на PHP и Perl, выполняющие задачи прокси-серверов.

Эксперимент № 1. Цель эксперимента – проверить максимальную длину цепочки веб-прокси-серверов при условии эксплуатации в качестве прокси-серверов скриптов на PHP и Perl. Схема эксперимента представлена на рисунке 4.

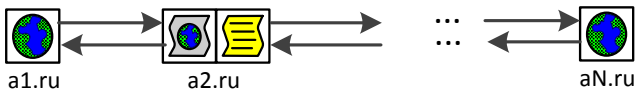

Рис. 4. *Схема эксперимента № 1*

Результаты эксперимента № 1. В результате натурного моделирования максимальная длина цепочки для веб-прокси:

на базе PHP-скрипта – 32 виртуальных узла;

на базе Perl-скрипта – 8 виртуальных узлов.

Выводы

Длина цепочки ограничена временем ответа веб-сервера, в связи с этим возникает ошибка веб-сервера «500 read timeout».

Для повышения устойчивости сети необходимы оптимизация скриптов, а также использование более производительной аппаратной платформы.

Эксперимент № 2. Реализация нагрузочного тестирования методом зацикливания запросов между двумя узлами, исследование сети на предмет временных задержек.

Эксперимент осуществлялся следующим образом: узел_1 отправлял запрос на узел_2, узел_2 обрабатывал запрос и отправляет его на узел_1. Этот процесс продолжался до тех пор, пока не произошел сбой в передаче запросов (не возник «отказ в обслуживании»). Схема эксперимента представлена на рисунке 5.

На рисунке 5а представлен маршрут передвижения запросов по анонимной сети, анализируя который можно определить время получения пакета и время отправки, номер узла, а также порядковый номер узла в цепочке (маршруте). Зацикливание запросов осуществлялось между двумя виртуальными узлами, развернутыми на базе единой программно-аппаратной платформы.

Результаты эксперимента № 2. В таблице 1 представлены результаты эксперимента.

Среднее время задержки составило:

$$\overline{t}_{\text{задержки}} = \frac{\sum_{i=0}^{n} t_{\text{задержки}_i}}{n} = 15{,}7 \text{ мс}$$

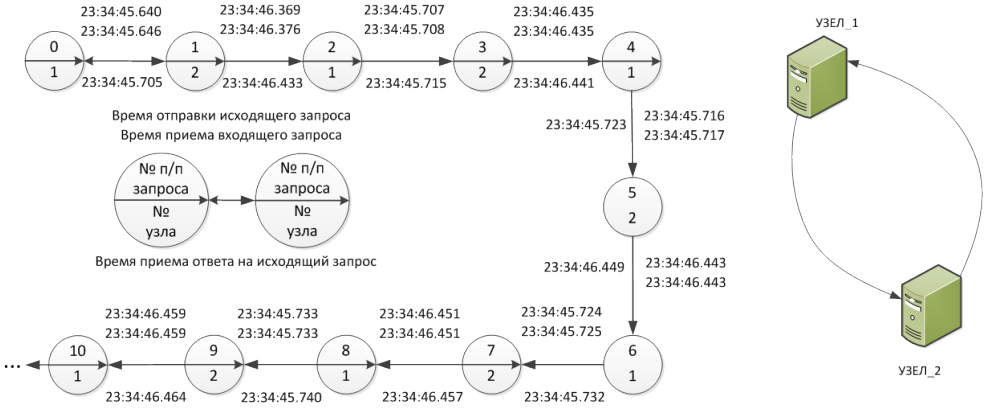

Рис. 5. *Схема эксперимента № 2:*
а – маршрут продвижения запроса с временными задержками;
б – схема обмена запросами между веб-прокси

Таблица 1.

Результаты эксперимента № 2

№ п/п	№ узла	Время получения запроса	Время отправки запроса	Время получения ответа	Задержка
0	1	45.640	45.646	45.705	00:059
1	2	46.369	46.376	46.433	00:057
2	1	45.707	45.708	45.715	00:007
3	2	46.435	46.435	46.441	00:006
4	1	45.716	45.717	45.723	00:006
5	2	46.443	46.443	46.449	00:006
6	1	45.724	45.725	45.732	00:007
7	2	46.451	46.451	46.457	00:006
8	1	45.733	45.733	45.740	00:007
9	2	46.459	46.459	46.464	00:005
10	1	45.742	45.742	45.749	00:007

На рисунке 6 представлен график загрузки центрального процессора (ЦП) и оперативной памяти (ОЗУ) при проведении нагрузочного тестирования методом зацикливания между двумя узлами.

Выводы. Из анализа результатов загрузки ЭВМ следует, что текущая аппаратная платформа успешно справлялась с режимом зацикливания запросов между двумя виртуальными узлами, выполняющими роль веб-прокси-серверов. При этом загрузка ЦП составила не более 55 %, загрузка ОЗУ – не более 38 %.

Эксперимент № 3. Цель данного эксперимента – произвести нагрузочное тестирование сети

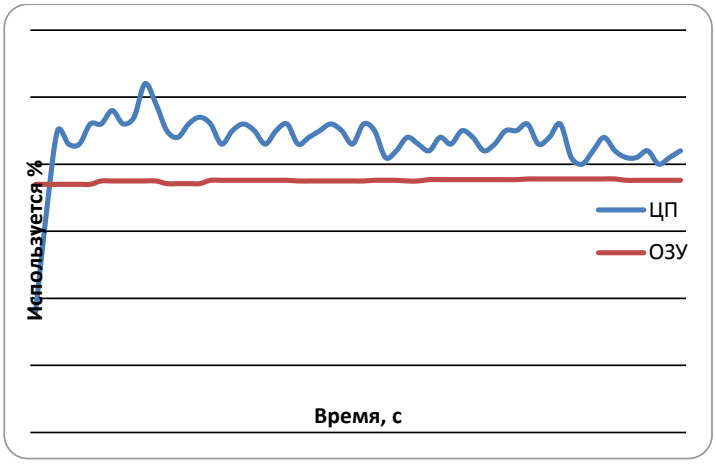

Рис. 6. *Производительность системы во время эксперимента № 2*

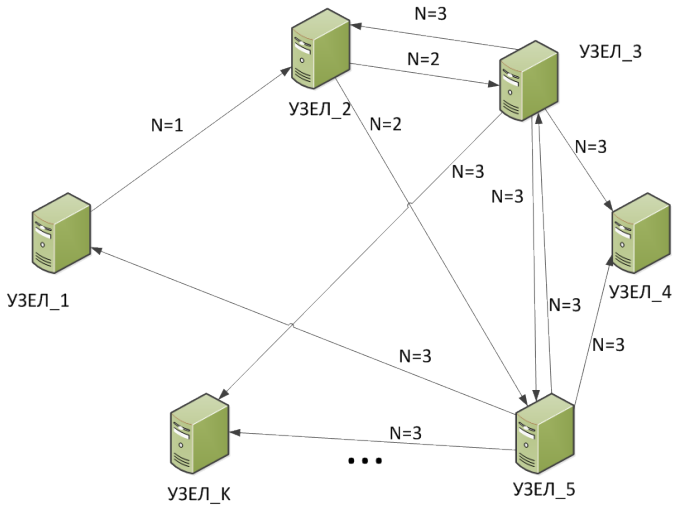

Рис. 7. *Маршрут продвижения запросов в эксперименте № 3*

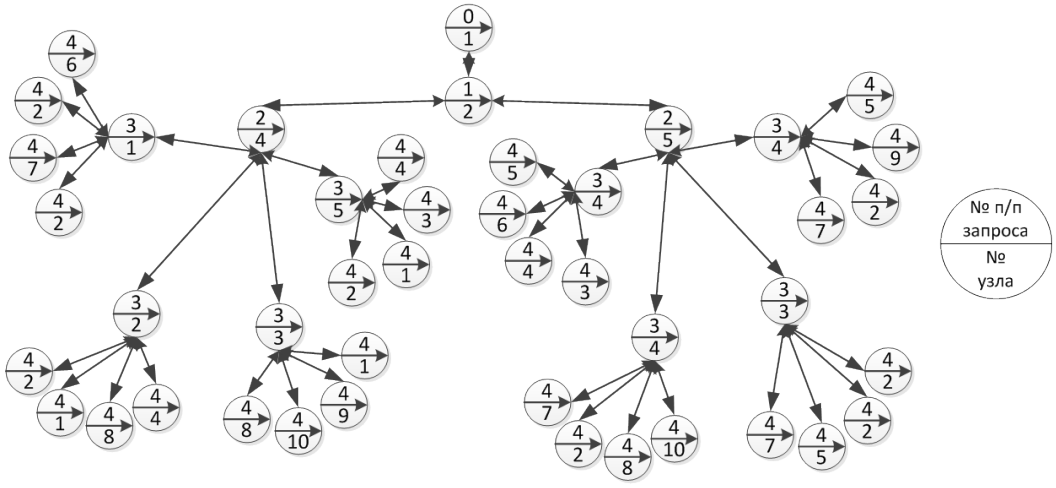

Рис. 8. *Маршрут продвижения запросов с размножением*

на базе веб-прокси за счет зацикливания запросов между двумя и более узлами сети с размножением запросов (отправка двух и более запросов после получения одного).

Схема эксперимента представлена на рисунках 7 и 8.

Результаты эксперимента № 3

На рисунке 9 представлен график загрузки ЦП и ОЗУ при проведении нагрузочного тестирования методом зацикливания запросов с размножением между узлами.

Выводы. Анализ результатов загрузки ЭВМ показал, что загрузка ЦП росла в арифметической прогрессии, однако не превысила значения в 80 %, загрузка ОЗУ – не более 38 %. Данный эксперимент показал повышение нагрузки на ЦП при обработке запросов к веб-прокси, однако загрузка ОЗУ осталась на прежнем уровне.

Эксперимент № 4. Цель эксперимента – произвести нагрузочное тестирование виртуального узла путем формирования множественных запросов, исследовать производительность системы, проанализировать отказоустойчивость узлов анонимной сети.

На рисунке 10 представлена схема эксперимента.

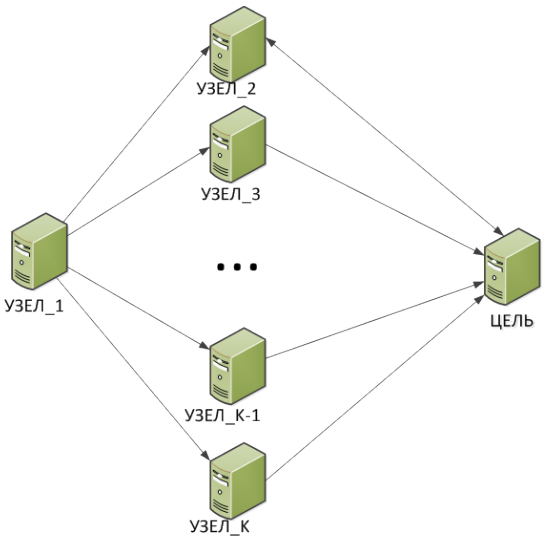

Рис. 10. *Множественный запрос к узлу сети*

Рис. 9. *Производительность системы при проведении эксперимента № 3*

***Рис. 11**. Производительность системы при множественных запросах к ресурсу*

Результаты эксперимента № 4

На рисунке 11 представлена диаграмма загруженности ЦП и ОП при проведении множественного доступа к единственному узлу.

Выводы. Из анализа графика загруженности ЦП видно, что в период нагрузочного тестирования загрузка ЦП составляла 100 %, что фактически можно охарактеризовать как «отказ в обслуживании» системы.

Общие выводы

В работе был исследован прототип анонимной сети на базе веб-прокси на предмет устойчивости к множественным запросам. В связи с тем, что все эксперименты проводились на одной ЭВМ, численные показатели не соответствуют тем, которые могли бы быть получены в сети Интернет.

Использование «луковичной» [8,9] или «чесночной» [10] маршрутизации, с одной стороны, повысит защищенность (анонимность) такой сети, но с другой – повысит требования к производительности аппаратной платформы и снизит устойчивость к множественным запросам.

При разработке программного обеспечения веб-прокси необходимо решить ряд проблем, связанных с особенностями использования технологий веб-прокси: ограничениями, накладываемыми веб-сервером на выполнение скриптов, а также с устойчивостью соединения, которое может включать несколько промежуточных узлов. Кроме того, существенными факторами являются защищенность от раскрытия параметров такой сети [11] и надежность установленного удаленного соединения.

***Рецензент**: Скурнович Алексей Валентинович, кандидат технических наук, доцент, сотрудник Академии ФСО России, г. Орёл, alexeymail2010@mail.ru*

Литература:

1. CGIProxy 2.1.14 // CGIProxy [Электронный ресурс] : сайт. – Электрон. дан. – 1998–2015. – Режим доступа: http://www.jmarshall.com/tools/cgiproxy/. – Дата обращения: 08.10.2015.
2. Glype Proxy Script // Glype [Электронный ресурс] : сайт. – Электрон. дан. – 2006–2015. – Режим доступа: https://www.glype.com/. – Дата обращения: 08.10.2015.
3. PHProxy // PHProxy [Электронный ресурс] : сайт. – Электрон. дан. – 2006–2015. – Режим доступа: http://sourceforge.net/projects/poxy/. – Дата обращения: 08.10.2015.
4. Cohula веб-прокси Cohula – альтернатива Glype // Cohula [Электронный ресурс] : сайт. – Электрон. дан. – 2015. – Режим доступа: http://cohula.com/ru/. – Дата обращения: 08.10.2015.
5. Кулешов С. В., Цветков О. В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы. 2014. Т. 12. № 6. С. 12-19.
6. Кулешов С. В. Терминальные программы «цифровой» передачи и обработки данных, энергетическая и информационная эквивалентность // Информационно-измерительные и управляющие системы. 2007. Т. 5. № 9. С. 10-15.
7. Александров В. В., Кулешов С. В., Цветков О. В., Зайцева А. А. Концепция построения инфотелекоммуникации (прототип SDR) // Труды СПИИРАН. 2008. № 6. С. 51-57.
8. Michael G. Reed, Paul F. Syverson, David M. Goldschlag. Onion routing network for securely moving data through communication networks / Michael G. Reed, Paul F. Syverson, David M. Goldschlag ; assignee The United States Of America As Represented By The Secretary Of The Navy. – № US 09/086,541 ; filed. 29.05.1998 ; pub. 24.07.2001.
9. The Tor Project, Inc. Tor Project: Anonymity Online, The Tor Project, Inc., 2015. URL: https://www.torproject.org/index.html.en.

10. Garlic Routing Garlic Routing and «Garlic» Terminology, Garlic Routing, 2015. URL: https://geti2p.net/en/docs/how/garlic-routing.
11. Разработка методологии комплексного мониторинга инфокоммуникационных ресурсов в распределенных сложноорганизованных системах. Отчет о НИР по ПФИ ОНИТ РАН № 2 Научные основы создания гетерогенных телекоммуникационных и локационных систем и их элементной базы, направление Алгоритмическое и программное обеспечение телекоммуникационных сетей, руководитель Александров В.В., № 01201360808.

ROBUSTNESS DEVELOPMENT OF ANONYMOUS NETWORK BASED ON WEB-PROXY TECHNOLOGIES

Markin D.O., Arhipov P.A., Galkin A.S.[2]

The article discusses the concept of constructing a system of anonymous access to remote resources based on web technologies using programming languages PHP/Perl. Anonymous remote access system to information resources is described. The analysis of the proxy servers types used for constructing anonymous networks is presented. The use of web technologies–proxy servers is proved for developing anonymous networks. The advantages and disadvantages of this technology are mentioned. The authors describe methods of using terminal programs and active data technologies for anonymous networks based on web proxy servers. The list of technical tasks which can be solved using terminal programs and active data technologies based on web proxy servers is offered. The principles of using terminal programs and active data technologies in relation to web proxy servers are described. The structure of an anonymous network prototype based on web proxy servers is described. The series of experiments on stability research of anonymous network based on web proxy servers is presented. The analysis of hardware and software stability used for providing load testing is carried out. The description and results of experiments are provided in the article. Conclusions about prospects of a web proxy technology application for realization of anonymous access system are presented. It is shown that anonymous networks based on a web proxy servers are vulnerable to the raised loading connected with limited computing of a hardware platform resources, however at the same time are potential sources of such loading concerning third–party resources.

***Keywords**: anonymous network, anonymous access, web–proxy, proxy–server*

References:

1. CGIProxy 2.1.14 // CGIProxy. 1998-2015. URL: http://www.jmarshall.com/tools/cgiproxy/.
2. Glype Proxy Script // Glype. 2006-2015. URL: https://www.glype.com/.
3. PHProxy // PHProxy. 2006-2015. URL: http://sourceforge.net/projects/poxy/.
4. Cohula Web-proxy Cohula – alternative Glype // Cohula. 2015. URL: http://cohula.com/ru/.
5. Kuleshov S. V., Cvetkov O. V. Aktivnye dannye v cifrovyh programmno-opredeljaemyh sistemah // Informacionno-izmeritel›nye i upravljajushhie sistemy, N 6, 2014 g. S.12-19.
6. Kuleshov S. V. Terminalnye programmy «cifrovoj» peredachi i obrabotki dannyh, jenergeticheskaja i informacionnaja jekvivalentnost // Informacionno-izmeritel›nye i upravljajushhie sistemy, №9, 2007.
7. Aleksandrov V. V., Kuleshov S. V., Cvetkov O. V., Zajceva A. A. Koncepcija postroenija infotelekommunikacii (prototip SDR) // Trudy SPIIRAN. – 2008. – Vypusk 6.
8. Michael G. Reed, Paul F. Syverson, David M. Goldschlag. Onion routing network for securely moving data through communication networks / Michael G. Reed, Paul F. Syverson, David M. Goldschlag ; assignee The United States Of America As Represented By The Secretary Of The Navy. – № US 09/086,541 ; filed. 29.05.1998 ; pub. 24.07.2001.
9. The Tor Project, Inc. Tor Project: Anonymity Online, The Tor Project, Inc. 2015. URL: https://www.torproject.org/index.html.en.
10. Garlic Routing Garlic Routing and «Garlic» Terminology, Garlic Routing. 2015. URL: https://geti2p.net/en/docs/how/garlic-routing.
11. Razrabotka metodologii kompleksnogo monitoringa infokommunikacionnyh resursov v raspredelennyh slozhnoorganizovannyh sistemah. Otchet o NIR po PFI ONIT RAN № 2 Nauchnye osnovy sozdanija geterogennyh telekommunikacionnyh i lokacionnyh sistem i ih jelementnoj bazy, napravlenie Algoritmicheskoe i programmnoe obespechenie telekommunikacionnyh setej, rukovoditel› Aleksandrov V.V., № 01201360808.

2 Dmitriy Markin, Pavel Arkhipov, Aleksey Galkin, The Academy of the Federal Guard Service of the Russian Federation, Orel, admin@nikitka.net