УДК 004.492.3

ОБМАННАЯ СИСТЕМА ДЛЯ ВЫЯВЛЕНИЯ ХАКЕРСКИХ АТАК, ОСНОВАННАЯ НА АНАЛИЗЕ ПОВЕДЕНИЯ ПОСЕТИТЕЛЕЙ ВЕБ-САЙТОВ

Вишневский А.С.[1]

Целью *данной работы является разработка способа эффективного независимого сбора черных и белых списков IP-адресов, основанном на анализе поведения посетителей веб-сайтов, которые нужны для современных средств защиты информации.*

Метод достижения цели *заключается в разработке веб ориентированных обманных систем, которые бы собирали черные и белые списки ip-адресов, и классифицировали IP-адреса посетителей с помощью специальным образом сформированного контента, опубликованного на группе веб-сайтов. Текст, изображения и ссылки на веб-сайтах подобраны таким образом, чтобы по списку посещенных страниц легко было отличить обходчик сайтов от человека, и обычного пользователя от злоумышленника. Накопленные обманной системой черные и белые списки ip-адресов будут использоваться при обнаружении хакерских атак антивирусами, межсетевыми экранами, песочницами и другими средствами защиты информации.*

Результаты: *обманная система была запущена на двадцати веб-сайтах в доменной зоне RU и накапливала сведения об атаках в течение года. В собранных трассах содержится информация о хакерских атаках на системы управления контентом и уязвимые скрипты. При этом значительная часть ip-адресов из обнаруженных атак отсутствует в зарубежных черных списках. Накапливаемые предложенной обманной системой черные и белые списки ip-адресов и способ их получения могут быть использованы для повышения качества отечественных средств защиты информации.*

Ключевые слова: *ложная система, альтернативные методы защиты (honeypot), поведенческий анализ, контент, обнаружение аномалий, вебсайты, черные списки, белые списки, ip-адреса.*

DOI:10.21681/2311-3456-2018-3-54-62

Введение

В условиях информационного противоборства, когда цена информации весьма высока, становится очевидным, что для обеспечения успешного противодействия атаке необходимо, чтобы нарушитель действовал в условиях априорной неопределенности. Этого добиваются введением в контур защиты обманной системы (ОБС), целью которой является вовлечение нарушителя в своего рода «игру», увеличивая тем самым время, необходимое на обход СЗИ. Работа обманных систем заключается в том, что они эмулируют те или иные известные уязвимости, которых в реальности не существует.

Рассматриваемая в данной работе обманная система классифицирует посетителей веб-сайтов на основе запрошенных ими веб-страниц. Основная цель - отделить атакующих от обходчиков и обычных пользователей, и составить белые и черные списки IP-адресов.

Актуальные черные и белые списки IP-адресов важны для современных средств защиты информации. Песочницы и другие инструменты динамического анализа обнаруживают вредоносную активность по обращениям к IP-адресам с плохой репутацией. Антивирусы и средства статического анализа могут извлекать IP-адреса из сканируемых файлов и выдавать вердикт на основе сведений об этих адресах. Межсетевые экраны, системы по обнаружению и предотвращению вторжений и другие инструменты для отслеживания сетевого взаимодействия могут в своей работе опираться на списки известных IP-адресов источников атак. Черные и белые списки IP-адресов в целом востребованы в индустрии информационной безопасности. Их можно купить либо составить самостоятельно.

В черный список должны попадать IP-адреса атакующих обманную систему. Сетевые адреса обходчиков, которые безопасно считывают контент, должны сохраняться в белом списке. Для классификации посетителя обманная система определяет три поведенческих признака.

Во-первых, рассчитывается число обращений посетителя веб-сайта к несуществующим страницам.

Во-вторых, определяется число веб-сайтов, на которые зашли с одного и того же IP-адреса.

В-третьих, фиксируется число таких переходов по ссылкам, которые показывают, что посетитель понимает смысл текста на сайте.

Обходчики, как правило, считывают контент веб-сайтов с одного и того же IP-адреса и не могут сравниться в понимании семантики текста с человеком. Хакеры же в свою очередь запускают автоматизированные сканеры уязвимостей, которые проверяют наличие определенных страниц на множестве сайтов. В предложенной обманной системе таких уязвимых страниц нет.

На каждом веб-сайте в разработанной обманной системе заранее известен список выложенных файлов. В ходе анализа файлов журнала веб-сервера обращения

1 Вишневский Андрей Сергеевич, аспирант кафедры ИУ8 «Информационная безопасность», МГТУ им. Н.Э.Баумана, Москва, Россия. E-mail: andreyryu@yandex.ru

к несуществующим файлам легко находятся. Все вебсайты в обманной системе созданы по одному шаблону и отличаются только доменным именем и языком контента. Доменные имена зарегистрированы в один день, поэтому обходчики, зашедшие на один из сайтов, как правило, заходят и на остальные. Тесты, содержащиеся на вебсайтах, написаны на чистом HTML посредством гиперссылок, чтобы упростить анализ журналов вебсервера.

В результате эксперимента была зафиксирована активность обходчиков известных поисковых компаний и поведение автоматизированных хакерских утилит. Были выявлены пути к файлам, в которых злоумышленники ожидали найти уязвимости. Поведение реальных пользователей отличалось от активности автоматизированных утилит как по количеству ошибок в тестах, так и по языковым предпочтениям.

Все собранные IP-адреса были размечены по предполагаемым странам-источникам с помощью сервиса геолокации. Это позволило выявить страны, из которых чаще всего осуществлялись атаки на сайты в доменной зоне RU, и страны, из которых проводились наиболее мощные атаки.

Обзор работ

Логика предложенной в данной работе обманной системы основана на анализе поведения посетителей веб-сайта. Действия пользователя на вебсайте рассматривались с позиций информационной безопасности в ряде научных работ.

В 2013-м году Лукас Олейник и Клавдия Кастелюсия предложили биометрический метод вебаутентификации на основе анализа интересов пользователя и характерной ему манере просмотра вебконтента. Согласно этому исследованию, факты посещения пользователем сайтов определенных банков, политических организаций и интернет-магазинов позволяют построить поведенческий портрет, который можно использовать в качестве дополнительного признака при аутентификации [1].

В 2014-м году Дзуньжу Жонг также предложил метод аутентификации, основанный на поведении пользователя на вебсайте. Под подведением в его работе понимался набор веб-страниц, посещенных пользователем. Выборка посещенных страниц передавалась алгоритму машинного обучения, который возвращал шаблоны поведения, характерные для атакующих и для обычных пользователей. Эксперимент, проведенный с помощью журналов из десяти вебсайтов показал, что предложенный метод позволяет достигнуть 91.3% точности классификации [2].

В 2014-м году Дэвид Канали, Лэйла Билье и Дэвид Бальцаротти опубликовали исследование по предсказанию рисков информационной безопасности на основе поведения пользователя в Интернете. Получив от компании Symantec историю веб-запросов 160 тысяч пользователей антивируса, они смогли классифицировать пользователей на тех, чьи компьютеры подвержены риску заражения, и тех, кто находится в безопасности. Классификация опиралась на количество веб-запросов пользователя, время наибольшей активности, разнообразие посещаемых вебсайтов и их категории, тип устройства, с которого пользователь выходил в Интернет, популярность посещенных веб-страниц, устойчивость списка посещаемых Интернет-ресурсов. Было показано, что чем больше различных веб-сайтов посещает пользователь и чем чаще он посещает веб-сайты с агрессивным контентом, тем выше риск заражения его компьютера [3].

В 2015-м году Шуй Ю, Сонг Го и Иван Стойменович разработали полумарковскую модель поведения пользователя на вебсайте для обнаружения хакерских атак. Они теоретически доказали, что если атака на вебсайт ведется с большего числа IP-адресов, чем приходит обычных пользователей, то создается эффект толпы, из-за которого становится сложно статистически обнаружить атаку [4].

В 2015-м году Ванг Джин предложил алгоритм кластеризации для защиты веб-серверов от распределенных атак по типу отказ-в-обслуживании. Алгоритм опирается на число посещенных пользователем веб-страниц и связи интересов конкретного пользователя с популярностью веб-страницы среди всех посетителей [5].

В 2015-м году Бин Джао и Пхен Лиу опубликовали результаты исследования о деанонимизации вебпользователей из-за ошибок расширений браузеров. Было показано, что большинство современных браузеров не гарантируют, что в режиме конфиденциального просмотра (режим инкогнито, Private Browsing Mode) расширения сохраняют в тайне историю веб-запросов и персональные данные пользователя [6].

В 2016-м году Таро Ишитаки, Тэтсуя Ода и Леонард Баролли разработали нейронную сеть, отличающую обычных веб-пользователей от тех, кто пользуется браузером Tor. В качестве признаков в нейронную сеть передавали число сетевых пакетов, время отклика, джиттер и число потерянных сетевых пакетов [7].

Существующие применяемые на практике обманные системы, как правило, обнаруживают атаки на один информационный ресурс, опираясь на события, связанные только с этим защищаемым ресурсом. Кроме того, существующие обманные системы не используют контент при анализе поведения потенциальных атакующих.

Например, веб-ориентированная обманная система Glastopf [8] собирает информацию об атаках на веб-приложения. В ловушке сохраняются вредоносные файлы, которые злоумышленники пытаются распространить, эксплуатируя различные уязвимости, которые эмулирует Glastopf. В частности, в описании системы указана возможность эмулирования PHP-инъекций и SQL-инъекций.

Загруженные вредоносные файлы сохраняет также обманная система Герарда Вагенера [9]. Эта высоко интерактивная обманная система замаскирована под SSH-сервер. Поведение ловушки определяется теоретико-игровой моделью и машинным обучением. Действия злоумышленник в рамках этой модели – это ввод различных команд в командную оболочку SSH. Действия обманной системы – выполнение команд злоумышленника либо подмена программы, которая должна выполнить команду. Выигрыш обманной системы определяется количеством новых обнаруженных опасных объектов, в частности вредоносных файлов, которые загрузил атакующий.

Таким образом, в опубликованных исследованиях сказано о том, что для составления поведенческого портрета веб-пользователя использовались данные с сетевого уровня, сведения о веб-браузере и его расширениях, а также история запросов, интересы и характер взаимодействия пользователя с веб-сайтом. В упомянутых статьях сказано, что такие поведенческие признаки полезно собирать для обнаружения хакерских атак. Следовательно, на этих признаках можно строить обманные системы, накапливающие черные и белые списки IP-адресов.

Структура обманной системы

Предложенная система представляет собой набор из двадцати доменных имен в зоне RU, привязанных к сайтам на одном выделенном сервере. На сервере установлен Apache и выложены HTML-файлы с текстом и изображениями. Текст страниц на каждом из двадцати вебсайтов соответствует названию домена. На каждом сайте есть главная страница и страницы с тестами на знание иностранных языков. В тестах нужно выбрать из трех слов то, которое соответствует изображению. Клик по неверному ответу ведет на страницу с ошибкой. Переход на страницу с ошибкой так же, как и выбор правильного ответа фиксируется в файле журнала веб-сервера Apache. Программа на языке Python разбирает полученные журналы и классифицирует IP-адреса.

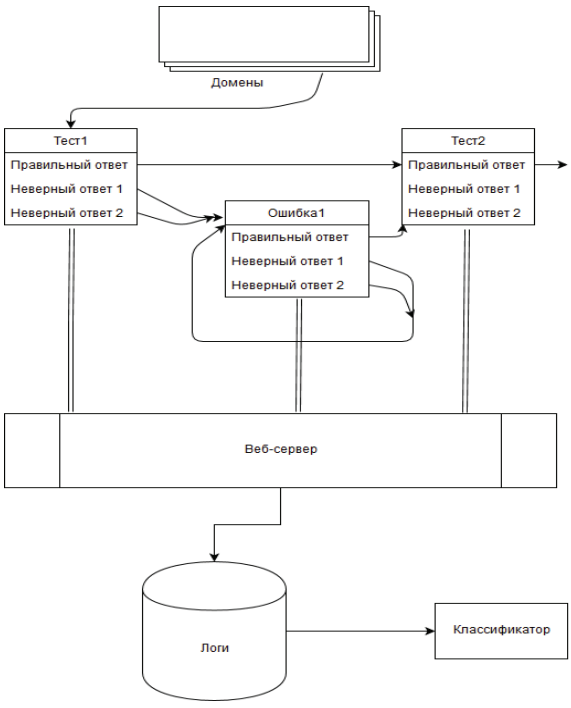

Рис. 1.Структурная схема обманной системы

Принцип работы

Поскольку все внутренние ссылки на веб-сайтах в обманной системе вели на существующие страницы, попытки доступа к несуществующим страницам считались атаками. У обычного пользователя нет возможности кликнуть по ссылке так, чтобы была зафиксирована атака. Ложное срабатывание возможно только, если пользователь неумышленно ошибется при ручном вводе названия веб-страницы.

Распознавание обходчиков основано на количестве веб-сайтов, на которые зашли с одного и того же IP-адреса. Доменные имена веб-сайтов в обманной системе выбраны так, как будто это сайты для изучения иностранных языков по карточкам с картинками. Для этой цели были выбраны арабский, китайский, английский, финский, французский, немецкий, греческий, итальянский, японский, корейский, литовский, норвежский, польский, португальский, испанский, турецкий, украинский языки, а также иврит, фарси и хинди.

Хотя людей, владеющих двумя языками достаточно много [10,11], чаще всего они знают диалекты одного языка или государственные языки соседних стран. Например, в ЕС людей, которые говорят одновременно на трех иностранных языках не более 10%[2] . Поэтому решение обманной системы о том, что запрос исходит от автоматизированного обходчика, принимается если с IP-адреса было посещено хотя бы два подконтрольных домена.

Способ сбора подозрительных IP-адресов

Анализатор разбивает файл журнала веб-сервера на группы запросов от каждого отдельного IP-адреса, затем вычисляет число ошибок в тестах, число посещенных доменов среди двадцати подконтрольных обманной системе и определяет наличие обращений к веб-страницам, отсутствующим на сайте.

При классификации поведения с помощью теста допускается, что человек может ошибаться. Предполагается, что обычный пользователь может допускать в тесте не более трех ошибок. Если допущено четыре и больше ошибок, считается, что это похоже на поведение веб-обходчика, который переходит по всем ссылкам подряд.

Число допустимых ошибок было выбрано эмпирически на основании ручной проверки зафиксированных событий. Результаты классификации не изменяются либо изменяются незначительно при допуске больше трех ошибок, как видно из (рис. 2). Однако если усилить критерий до двух или одной допустимой ошибки, то десятки сетевых запросов от реальных пользователей неверно классифицируются как взаимодействие с веб-обходчиками

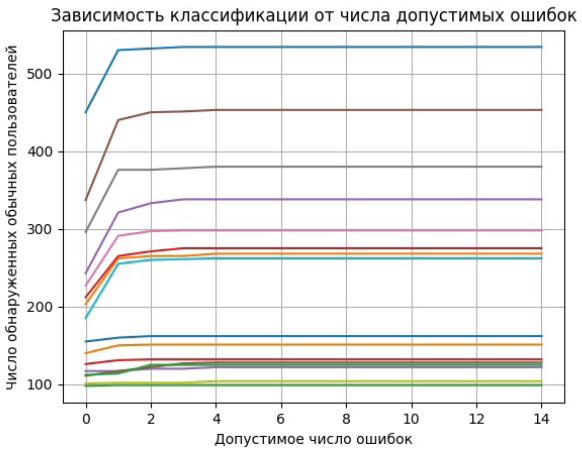

Рис. 2. Зависимость классификации от числа допустимых ошибок

2 Europeans and their languages // Special Eurobarometer 386, 2012. URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_386_en.pdf (дата обращения: 06.04.2018)

Описание и результаты эксперимента

Журналы веб-сервера накапливались с января по декабрь 2017-го года. В них зафиксированы запросы атакующих к потенциально уязвимым веб-страницам. Статистика геолокации IP-адресов показала основные тренды атак на домены в зоне RU. Геоданные взяты из сервиса Maxmind[3].

Примеры запросов, реализующих атаку приведены ниже.

<IPaddress1> - - [31/Jan/2017:02:06:43 +0100] «GET /admin/ HTTP/1.1» 404 445 «-» «Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; MRSPUTNIK 2, 4, 0, 270; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET4.0C)»

<IPaddress2> - - [27/Jun/2017:06:09:01 +0200] «GET /bitrix/admin/index.php HTTP/1.1» 404 517 «http://italian-cards.ru/bitrix/admin/index.php» «Mozilla/5.0 (compatible; uCrawlr/1.0; +https://blog.ucoz.ru/upolicy)»

На (рис. 2—5) показаны распределения атак на развернутые вебсайты. По горизонтальной оси отмечены коды стран, из которых, согласно базе данных maxmind, исходили атаки. По вертикальной оси отложено число уникальных IP-адресов, с которых приходили запросы к ловушкам. Гистограммы запросов атакующих и обычных пользователей показаны разным цветом и текстурой на графиках.

Можно заметить, что распределение стран-источников атак отличается от распределения стран, из которых заходили обычные пользователи. Интерес русскоязычных пользователей к изучению иврита можно объяснить культурными связями, так же как и востребованность материалов по немецкому языку среди жителей Нидерландов. С другой стороны, атаки с российских и украинских IP-адресов были распределены равномерно по всем сайтам, за исключением английского и корейского.

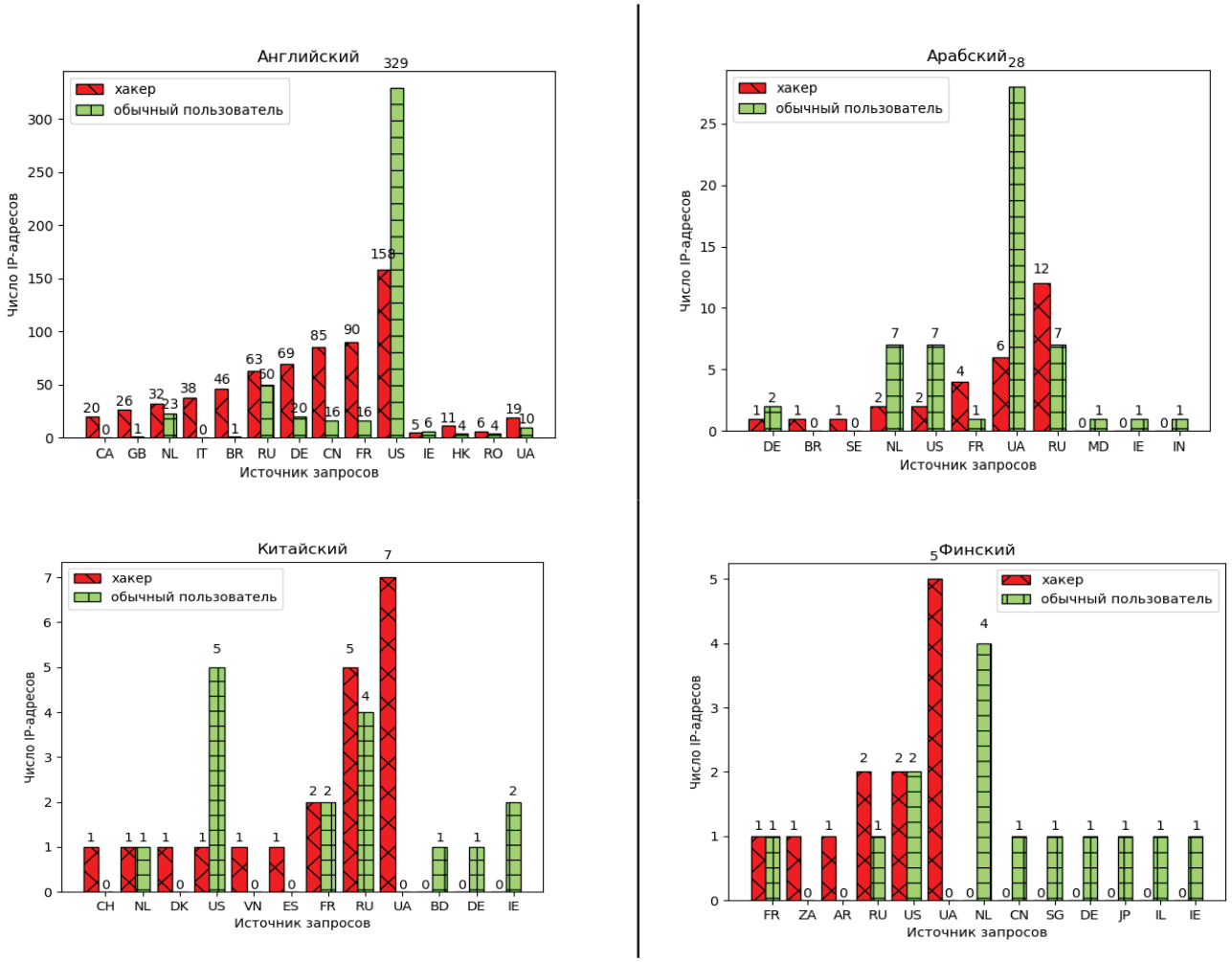

Рис. 3. Статистика атак на сайты об изучении английского, арабского, китайского и финского языков

3 Maxmind. Базы данных GeoIP. URL:https://www.maxmind.com/ru/home (дата обращения: 14.03.2018)

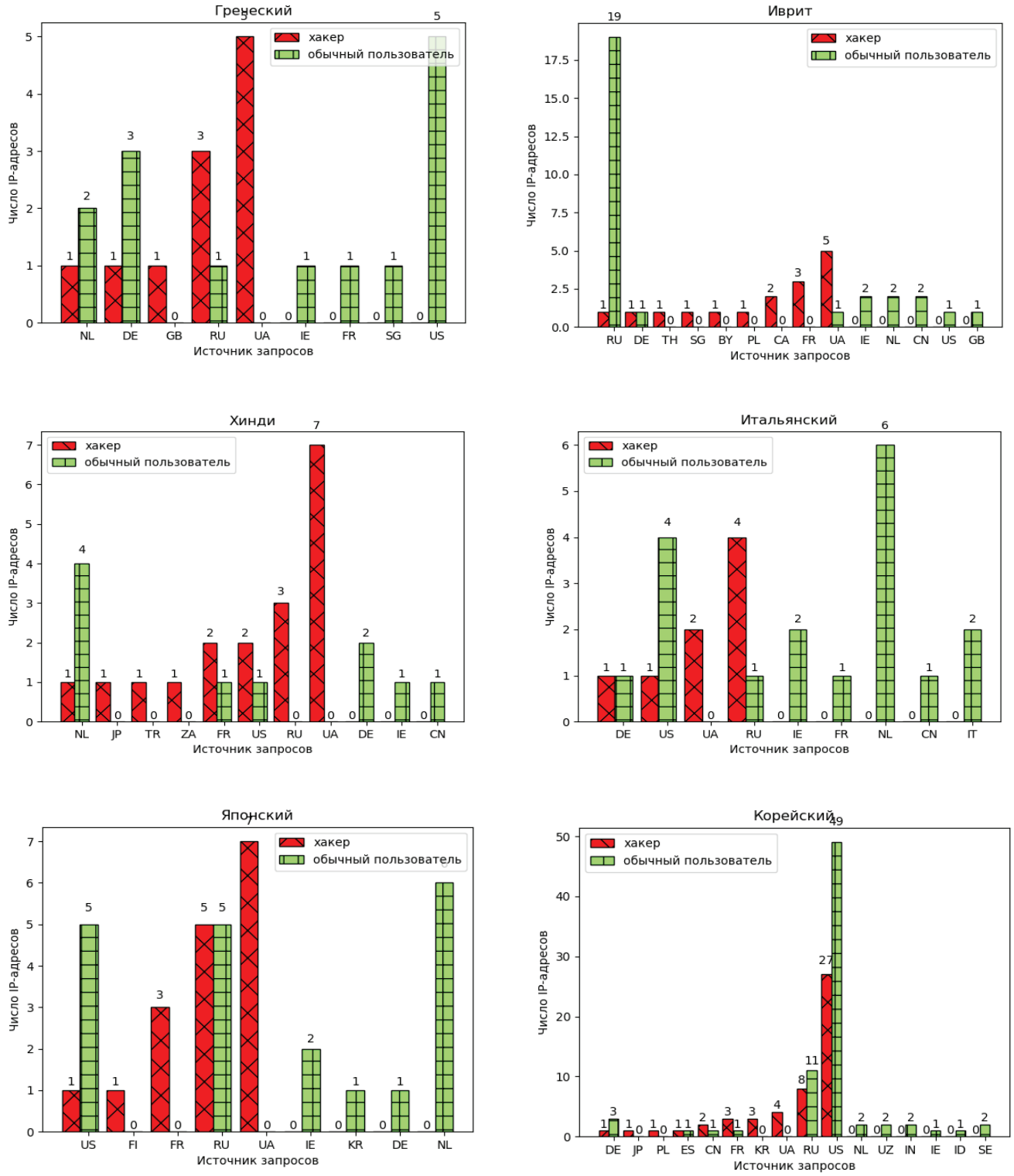

Рис. 4. Статистика атак на сайты об изучении греческого, итальянского, японского, корейского языков, хинди и иврита

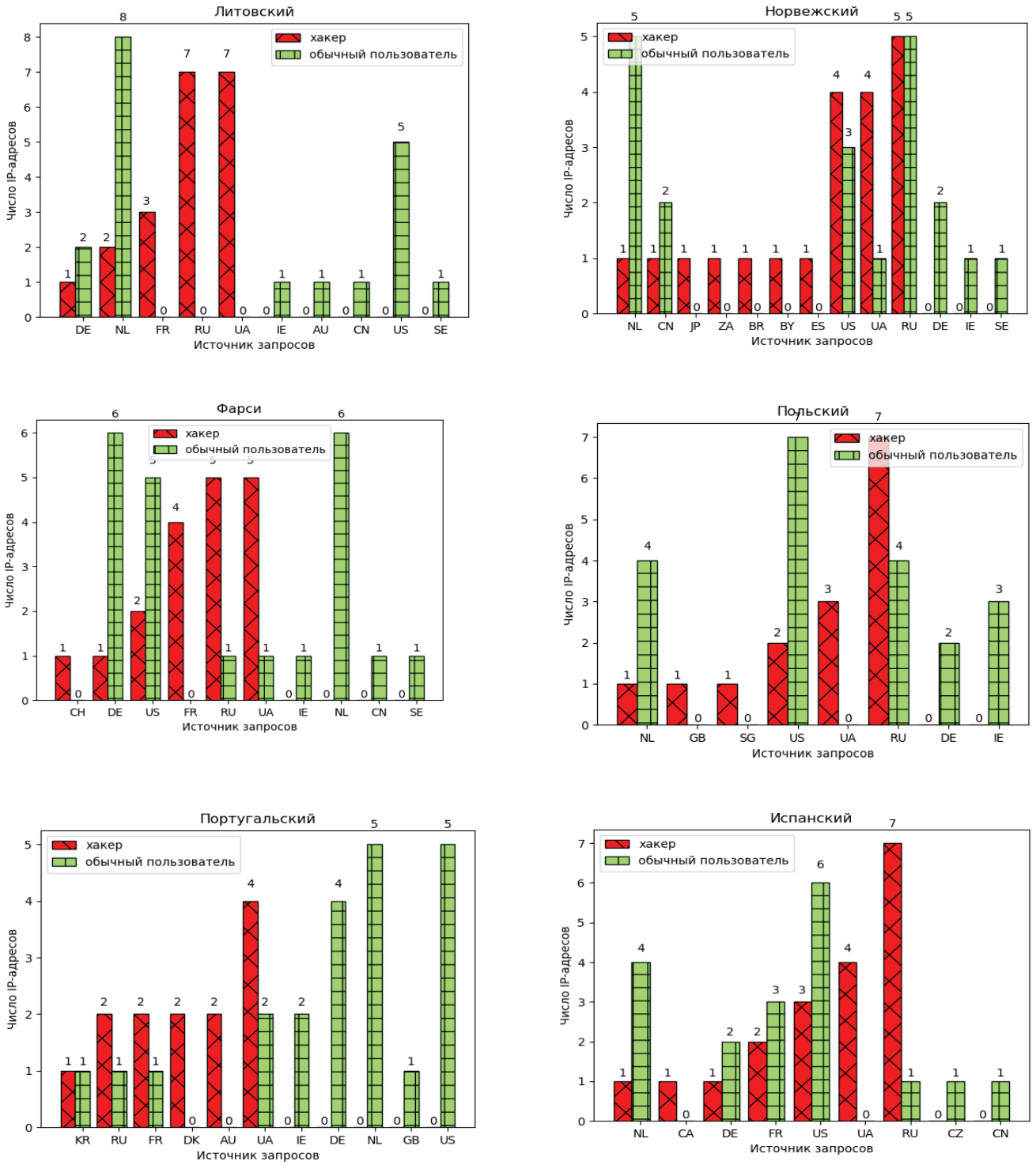

Рис. 5. Статистика атак на сайты об изучении литовского, норвежского, польского, португальского, испанского языков и фарси

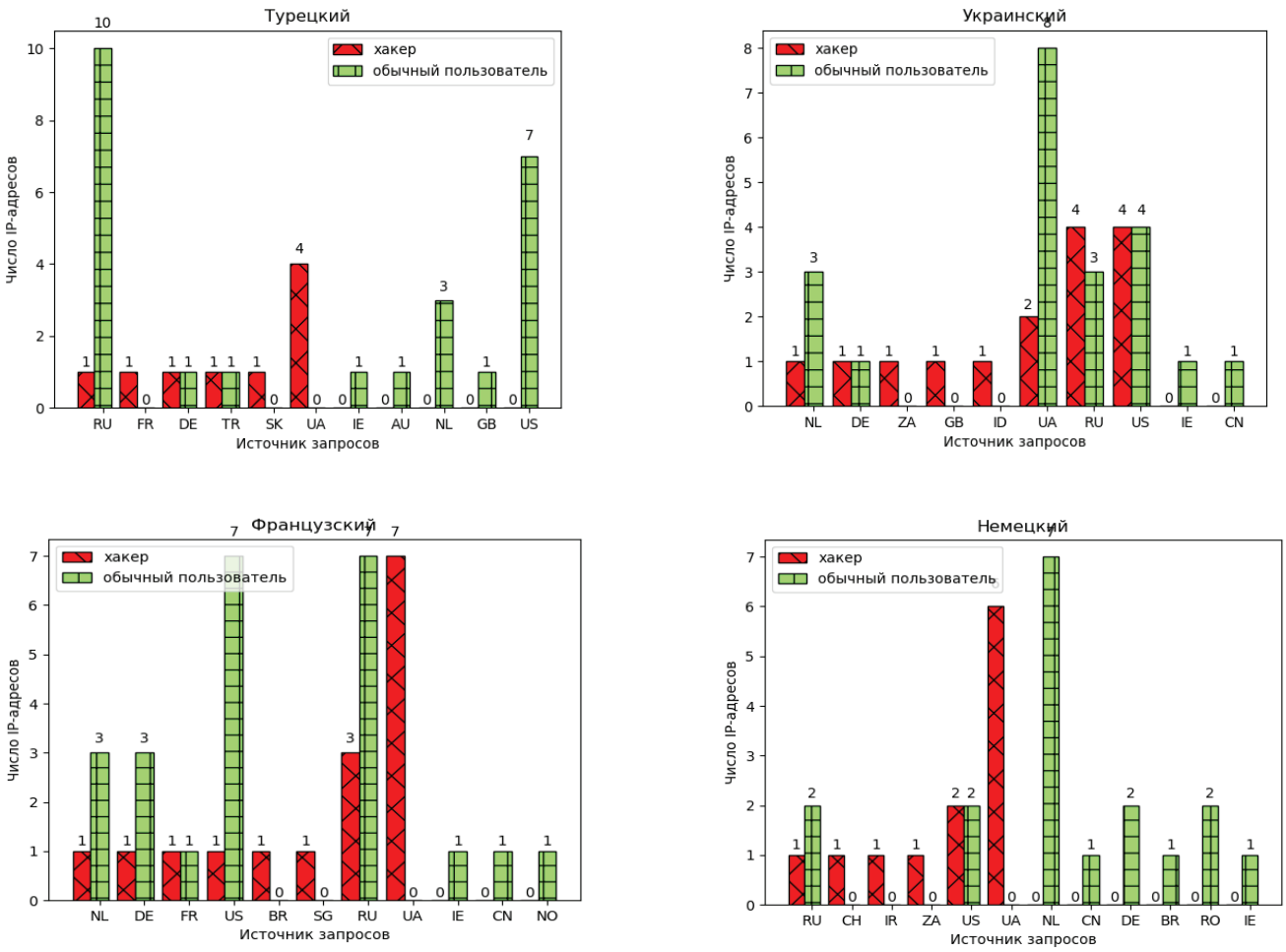

Рис. 6. Статистика атак на сайты об изучении турецкого, французского, немецкого и украинского языков

На (рис. 3—6) показано количество атак из различных стран на каждый из опубликованных веб-сайтов. Чаще всего атаки исходили с украинских IP-адресов, а самые продолжительные атаки осуществлялись с американских IP на домены, в названиях которых входили подстроки korean и angliysky. Вероятно, эти вебсайты были выбраны атакующими из-за ключевых слов в названиях доменов.

Классифицированные IP-адреса по двум странам из общего списка были проверены вручную и просканированы в авторитетном репутационном сервисе – Virustotal [4]. Портал Virustotal объединяет в себе экспертные знания о вредоносных файлах, ссылках и IP-адресах, собранные в 67-ми крупнейших антивирусных компаниях мира. В инфраструктуры этих компаний входят в том числе и обманные системы, на основе которых и публикуются данные о подозрительных IP-адресах.

Среди вручную подтвержденных источников атак Virustotal предупредил об опасности только в 21% случаев. Т.е. каждые четыре из пяти IP-адресов, с которых осуществлялись попытки подбора паролей, несанкционированной авторизации и эксплуатации уязвимостей в сайтах, расположенных в доменной зоне RU, считались безопасными.

На основании ручной проверки по двум странам были перепроверены результаты классификации. Точность (precision) классификации составила 94-97%, а полнота (recall) 97-98%. На точность негативно повлияли ложные срабатывания на безопасные обращения веб-обходчиков к несуществующим страницам. Полноту обнаружения атак снизили неожиданные опасные сетевые запросы, в которых эксплуатация осуществлялась не через путь к запрашиваемой веб-странице, а через поле User-agent. Значит, созданная обманная система обнаружила источники неизвестных атак.

Заключение

В данной работе поведение посетителей веб-сайтов было проанализировано с помощью веб ориентированной обманной системы. Использование обманной системы показало, что число посещенных сайтов-ловушек является существенным признаком, характеризующим хакерские атаки.

Было продемонстрировано, как с помощью специальным образом подобранного контента можно класси-

4 VirusTotal. URL: https://www.virustotal.com/ (дата обращения: 16.03.2018)

фицировать посетителей по поведению на хакеров, роботизированных обходчиков и реальных пользователей.

Предложенный поведенческий подход позволяет определить источники хакерских атак, которые не были известны крупным и авторитетным зарубежным репутационным сервисам. Значит, он может повысить качество отечественных средств информационной безопасности.

Научный руководитель: *Ключарев Петр Георгиевич[5] кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, Россия.* ***E-mail:*** *pk.iu8@yandex.ru*

Литература

1. Olejnik L., Castelluccia C. Towards Web-Based Biometric Systems Using Personal Browsing Interests. 2013 International Conference on Availability, Reliability and Security. Regensburg. 2013. P. 274-280. DOI: 10.1109/ARES.2013.36
2. Zhong J., Yan C., Yu W., Zhao P., Wang M. A Kind of Identity Authentication Method Based on Browsing Behaviors. 2014 Seventh International Symposium on Computational Intelligence and Design. Hangzhou. 2014. P. 279-284. DOI: 10.1109/ISCID.2014.205
3. Davide Canali, Leyla Bilge, and Davide Balzarotti. On the effectiveness of risk prediction based on users browsing behavior. In Proceedings of the 9th ACM symposium on Information, computer and communications security (ASIA CCS ‹14). ACM, New York. NY. USA. 2014. P. 171-182. DOI: 10.1145/2590296.2590347
4. Yu S., Guo S., Stojmenovic I. Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace. in IEEE Transactions on Computers. 2015. V. 64. N 1. P. 139-151. DOI: 10.1109/TC.2013.191
5. Wang J., Zhang M., Yang X., Long K., Xu J. HTTP-sCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs. In China Communications. 2015. V. 12. N 2. P. 118-128. DOI: 10.1109/CC.2015.7084407
6. Zhao B., Liu P. Private Browsing Mode Not Really That Private: Dealing with Privacy Breach Caused by Browser Extensions. 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro. 2015. P. 184-195. DOI: 10.1109/DSN.2015.18
7. Ishitaki T., Oda T., Barolli L. A Neural Network Based User Identification for Tor Networks: Data Analysis Using Friedman Test. 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana. 2016. P. 7-13. DOI: 10.1109/WAINA.2016.143
8. Glastopf Web Honeypot Project, Lukas Rist, “Glastopf honeypot,”glastopf.org/, last accessed on January 2016.
9. Wagener, Self Adaptive High Interaction Honeypots Driven by Game Theory, в Conference: Stabilization, Safety, and Security of Distributed Systems, 11th International Symposium, SSS 2009, Lyon, France, 2009.
10. Ansaldo, A. I., Marcotte, K., Scherer, L., & Raboyeau, G. (2008). Language therapy and bilingual aphasia: Clinical Implications of psycholinguistic and neuroimaging research. Journal of Neurolinguistics, 21, 539-557.
11. De Bot, K. (1992). A bilingual production model: Levelt’s ‘speaking’ model adapted. Applied Linguistics, 13 (1), 1-24.

CONTENT BASED ATTACK DETECTION IN WEB-ORIENTED HONEYPOTS

Vishnevsky A.S.[6]

Abstract. *Antiviruses, firewalls, sandboxes and other security tools operate the lists of black and white IP-addresses for attack detection. In this paper, the web-oriented server-side honeypot is developed to classify IP-addresses using specially crafted content on the group of websites. The text, images and links on the websites are chosen to simplify the recognition of web-crawlers and hackers, to distinguish them from benign users. The proposed honeypot system was implemented on the twenty websites and has been monitoring attacks during one year. The gathered data include information about attacks on content management systems and vulnerable scripts. The most of recognized malicious IP-addresses is absent in popular blacklists and reputation services. The blacklists of IP-addresses collected by the developed honeypot could be used for improving the quality of various security tools.*

Keywords: *honeypot, server-side, high interactive, web-attack, behavior analysis, content, anomaly detection, website, blacklist, whitelist, ip-addresses*

References

1. Olejnik L., Castelluccia C. Towards Web-Based Biometric Systems Using Personal Browsing Interests. 2013 International Conference on Availability, Reliability and Security. Regensburg. 2013. P. 274-280. DOI: 10.1109/ARES.2013.36
2. Zhong J., Yan C., Yu W., Zhao P., Wang M. A Kind of Identity Authentication Method Based on Browsing Behaviors. 2014 Seventh International Symposium on Computational Intelligence and Design. Hangzhou. 2014. P. 279-284. DOI: 10.1109/ISCID.2014.205
3. Davide Canali, Leyla Bilge, and Davide Balzarotti. On the effectiveness of risk prediction based on users browsing behavior. In Proceedings of the 9th ACM symposium on Information, computer and communications security (ASIA CCS ‹14). ACM, New York. NY. USA. 2014. P. 171-182. DOI: 10.1145/2590296.2590347
4. Yu S., Guo S., Stojmenovic I. Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace. in IEEE Transactions on Computers. 2015. V. 64. N 1. P. 139-151. DOI: 10.1109/TC.2013.191

5 Petr Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, Russia. Email: pgkl@yandex.ru
6 Andrey Vishnevsky, post-graduate student, Bauman Moscow State Technical University, Moscow, Russia. Email: andreyryu@yandex.ru

5. Wang J., Zhang M., Yang X., Long K., Xu J. HTTP-sCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs. In China Communications. 2015. V. 12. N 2. P. 118-128. DOI: 10.1109/CC.2015.7084407
6. Zhao B., Liu P. Private Browsing Mode Not Really That Private: Dealing with Privacy Breach Caused by Browser Extensions. 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro. 2015. P. 184-195. DOI: 10.1109/DSN.2015.18
7. Ishitaki T., Oda T., Barolli L. A Neural Network Based User Identification for Tor Networks: Data Analysis Using Friedman Test. 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana. 2016. P. 7-13. DOI: 10.1109/WAINA.2016.143
8. Glastopf Web Honeypot Project, Lukas Rist, "Glastopf honeypot,"glastopf.org/, last accessed on January 2016.
9. Wagener, Self Adaptive High Interaction Honeypots Driven by Game Theory, в Conference: Stabilization, Safety, and Security of Distributed Systems, 11th International Symposium, SSS 2009, Lyon, France, 2009.
10. Ansaldo, A. I., Marcotte, K., Scherer, L., & Raboyeau, G. (2008). Language therapy and bilingual aphasia: Clinical Implications of psycholinguistic and neuroimaging research. Journal of Neurolinguistics, 21, 539-557.
11. De Bot, K. (1992). A bilingual production model: Levelt's 'speaking' model adapted. Applied Linguistics, 13 (1), 1-24.