УДК 004.438

ОБ ОДНОМ МЕТОДЕ ЗАЩИТЫ МЕСТОПОЛОЖЕНИЯ (АДРЕСА) СЕРВЕРА БАЗ ДАННЫХ

Р.А. ДЬЯЧЕНКО, В.Е. БЕЛЬЧЕНКО, И.В. БЕЛЬЧЕНКО

Кубанский государственный университет,
350040, г. Краснодар, Российская Федерация, ул. Ставропольская, 149;
электронная почта: ilur@mail.ru

Рассматриваются вопросы защиты информации путем сокрытия адреса сервера данных. Приводится методика, позволяющая скрыть адрес сервера данных в сети Internet. Метод позволяет защитить информацию на примере системы “Электронное расписание колледжей”.
Ключевые слова: взлом, сокрытие адреса, сервер баз данных, защита информации.

В последнее время ценность информации существенно возросла. С ростом ценности и объемов информации растет и количество злоумышленников, пытающихся получить несанкционированный доступ к информации. Превентивным средством защиты информации является сокрытие адреса сервера данных [1]. Система «Электронное расписание колледжей» является высоконагруженной. Из-за большого количества одновременных подключений, система должна быть защищена не только логином и паролем. Большое количество подключений затрудняет отслеживание попыток взлома сервера. Необходимо скрывать адрес сервера данных. Злоумышленник, получив доступ к системе, может внести изменения в расписание занятий, изменить нагрузку преподавателей. Это повлечет за собой накладки в расписании,финансовые проблемы, связанные с оплатой труда. Проблема сокрытия адреса сервера данных возникла с появлением сети Internet [2].

Основными задачами исследования являются:

1. выделение группы пользователей системы;
2. определение цели взлома для нарушителя;
3. проведение анализа существующих методов и технологий сокрытия адреса;
4. предложение метода защиты местоположения (адреса) сервера баз данных;

5. формализация метода.

Пользователями WEB системы ”Электронное расписание колледжей“ являются:

1. учащиеся;
2. преподаватели;
3. диспетчеры из учебной части.

Основными технологиями и методами сокрытия настоящего IP-адреса являются: VPN (VirtualPrivateNetwork), Proxy, SOCKS, программы SocksChain и FreeCap, система анонимной передачи пользовательских данных TOR. VPN (VirtualPrivateNetwork, виртуальная частная сеть) - технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Когда программа обратится к удаленному ресурсу, на компьютере будет создан специальный GRE-пакет (GenericRoutingEncapsulation, общая инкапсуляция маршрутов), который в зашифрованном виде будет отправлен VPN-серверу. VPN-сервер, в свою очередь, этот пакет расшифрует, и выполнит от своего лица соответствующее действие [3]. Далее, получив ответ от удаленного ресурса, VPN-сервер поместит его в GRE-пакет, зашифрует и в таком виде отправит обратно клиенту. Достоинства технологии Технологию поддерживают практически все операционные системы. При использовании VPN подключения, программы видят его как обычную локальную сеть. Нет необходимости создавать специальные модули для работы приложения с VPN. Недостатки Главным недостатком является открытый адрес VPN сервера и ненадежные средства шифрования пакетов. HTTP-прокси сервер — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам [4]. Клиент подключается к прокси- серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом 2 сервере. Затем прокси-сервер подключается к указанному серверу, получает ресурс у него и передает клиенту. Достоинства технологии Основным достоинством технологии является ее доступность и простота. Недостатки К недостаткам относится

отсутствие шифрования HTTP запроса. Некоторые HTTP-прокси добавляют в заголовок запроса адрес клиента. SocksChain — программа, позволяющая работать через цепочку SOCKS или HTTP- прокси. Достоинства подхода К основным достоинствам подхода цепочки прокси серверов является доступность такого подхода для пользователей. Существуют тысячи бесплатных цепочек HTTP-прокси серверов. Недостатки Основным недостатком является то, что на HTTP-прокси серверах ведется лог обращений. Следовательно обладая правами на чтение лога не трудно вычислить клиента даже через цепочку из десятка HTTP-прокси серверов. Tor (TheOnionRouter) — свободная (BSD) реализация второго поколения onionrouter. Система, позволяющая пользователям соединяться анонимно, обеспечивая передачу пользовательских данных в зашифрованном виде. Рассматривается как анонимная сеть, предоставляющая безопасную передачу данных. С помощью Tor пользователи могут сохранять анонимность при посещении web-сайтов, публикации материалов, отправке сообщений и работе с другими приложениями, использующими протокол TCP [5]. Безопасность трафика обеспечивается за счёт использования распределённой сети серверов. При правильном использовании обеспечивает анонимность клиента, но сервер должен быть открыт в интернете. С другой стороны, система обеспечивает анонимность клиента, а не сервера, что является недостатком. Запрос может проходить через другой континент. Это замедлит время получения на запрос от сервера [6]. Каждое из существующих решений подходит больше для сокрытия клиентских адресов, чем адреса высоконагруженного сервера данных с дорогостоящей коммерческой или секретной информацией. Для сокрытия такого рода информации предлагается использовать метод, использующий положительные стороны рассмотренных существующих средств сокрытия адреса.

Предлагаемый метод защиты основан на симбиозе технологий VPN и TOR [7]. Запрос от клиента проходит несколько узлов сокрытия адреса: узел распределитель, узел доступа. Адрес сервера распределителя открыт в сети

Internet. Сервер распределитель перенаправляет запрос на узлы доступа. Узлы доступа шифруют запрос и пересылают его случайному узлу из списка IP адресов. Список IP адресов содержит адреса узлов доступа и адрес сервера данных. Пересылка зашифрованного запроса между узлами доступа скрывает истинный 3 адрес сервера данных. Диаграмма работы метода представлена на рисунке 1.

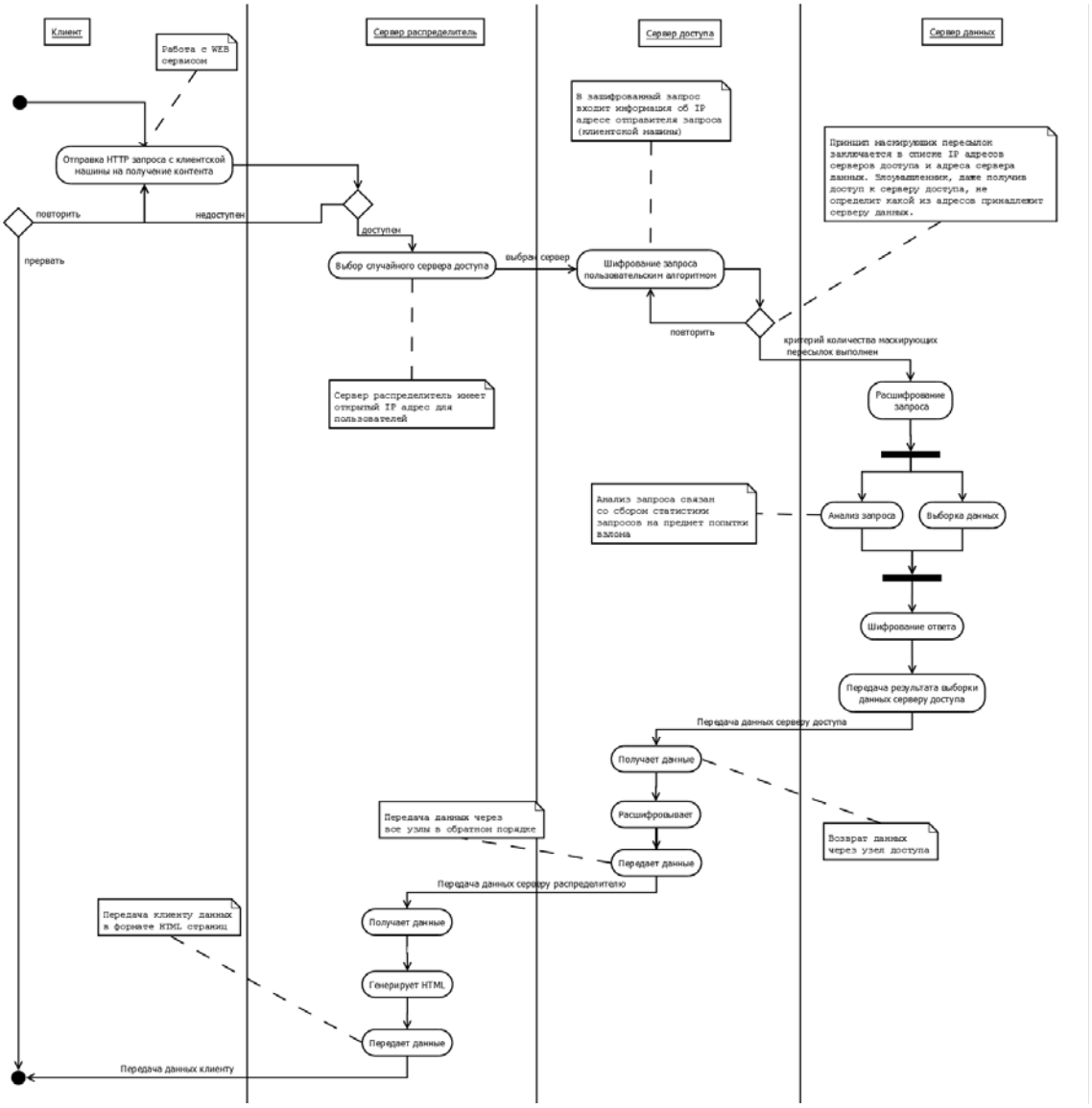

Рис. 1. Схема работы предлагаемого метода сокрытия адреса.

Многоуровневая модель защиты системы повышает устойчивость системы к взлому, дает возможность отследить попытку взлома на каждом из узлов, участвующих в обработке клиентского запроса. Достоинства подхода заключаются в сокрытии адреса сервера данных даже при получении злоумышленником доступа к узлу доступа.

В результате проведенных исследований были получены следующие результаты:

1. сформулирована проблема защиты информации путем сокрытия адреса сервера данных;
2. проведен анализ существующих подходов и технологий по сокрытию адреса, выявлены их достоинства и недостатки;
3. предложена методика сокрытия адреса сервера данных ссистеме “Электронное расписание колледжей”.

ЛИТЕРАТУРА

1. Бельченко В.Е. Технология организации Web-сайта учебного заведения // Высшее образование в России. 2014. № 4. С. 97-101.

2. Коновалов Д.П., Дьяченко Р.А., Богданов В.В. Современные средства разработки WEB-приложений. Сравнительный анализ // Сборник III Международной научно-практической конференции молодых ученых, посвященная 52-й годовщине полета Ю.А. Гагарина в космос. 2013. С. 303-306.

3. Фишер А.В., Дьяченко Р.А., Лоба И.С. Организация хранения хронологических данных в базах данных систем мониторинга и прогнозирования // Политематический сетевой электронный научный журнал Кубанского государственного агарного университета. 2012/ № 79. С. 271-280.

4. Дьяченко Р.А., Бельченко И.В., Терехов В.В. Иллюстрация применения метода дельфи для решения задачи выбора направления развития предприятия // Автоматизированные информационные и электроэнергетические системы. 2012. С. 243-244.

5. Шароватов А.С., Лоба И.С., Решетняк М.Г. Разработка алгоритма поиска оптимальной модели // Политематический сетевой электронный научный журнал Кубанского государственного агарного университета. 2012. № 77. С. 413-422.

6. Кучер В.А., Магомадов А.С., Чигликова Н.Д., Дьяченко Р.А. Обеспечение информационной безопасности вычислительной сети с использованием интеллектуальных систем // Политематический сетевой

электронный научный журнал Кубанского государственного агарного университета. 2015. № 110. С. 1811-1816.

7. Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. К вопросу организация хранения данных в мобильном приложении // Научные труды Кубанского государственного технологического университета. 2014. № 1. С. 189-197.

REFERENCES

1. Belchenko V.E. Tekhnologiya organizatsii Web-sayta uchebnogo zavedeniya // Vysshee obrazovanie v Rossii. 2014. № 4. S. 97-101.

2. Konovalov D.P., Dyachenko R.A., Bogdanov V.V. Sovremennye sredstva razrabotki WEB-prilozheniy. Sravnitelnyy analiz // Sbornik III Mezhdunarodnoy nauchno-prakticheskoy konferentsii molodykh uchenykh, posvyashchennaya 52-y godovshchine poleta Yu.A. Gagarina v kosmos. 2013. S. 303-306.

3. Fisher A.V., Dyachenko R.A., Loba I.S. Organizatsiya khraneniya khronologicheskikh dannykh v bazakh dannykh sistem monitoringa i prognozirovaniya // Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agarnogo universiteta. 2012/ № 79. S. 271-280.

4. Dyachenko R.A., Belchenko I.V., Terekhov V.V. Illyustratsiya primeneniya metoda delfi dlya resheniya zadachi vybora napravleniya razvitiya predpriyatiya // Avtomatizirovannye informatsionnye i elektroenergeticheskie sistemy. 2012. S. 243-244.

5. Sharovatov A.S., Loba I.S., Reshetnyak M.G. Razrabotka algoritma poiska optimalnoy modeli // Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agarnogo universiteta. 2012. № 77. S. 413-422.

6. Kucher V.A., Magomadov A.S., Chiglikova N.D., Dyachenko R.A. Obespechenie informatsionnoy bezopasnosti vychislitelnoy seti s ispolzovaniem intellektualnykh sistem // Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agarnogo universiteta. 2015. № 110. S. 1811-1816.

7. Atroshchenko V.A., Rudenko M.V., Dyachenko R.A., Bagdasaryan R.Kh. K voprosu organizatsiya khraneniya dannykh v mobilnom prilozhenii // Nauchnye trudy

Kubanskogo gosudarstvennogo tekhnologicheskogo universiteta. 2014. № 1. S. 189-197.

ON THE METHOD OF PROTECTION LOCATION (ADDRESS) DATABASE SERVER

R.A. DJACHENKO, V.E. BELCHENKO, I.V. BELCHENKO

Kuban State University,
149, Stavropolskaya st., Krasnodar, Russian Federation, 350040
e-mail: ilur@mail.ru

We consider data protection issues by hiding the data server address. The technique, which allows to hide the address of the data server on the Internet. The method allows to protect the information on the system as an example "Electronic college schedule."
Keywords: hacking, concealment addresses, database server, data protection.