Системный анализ методов контроля доступа к web-ресурсам
Кобзева Е. А.

Кобзева Екатерина Александровна / Kobzeva Ekaterina Alexandrovna - студент,
кафедра информационной безопасности автоматизированных систем,
Северо-Кавказский университет, г. Ставрополь

Аннотация: *в статье рассматриваются актуальные проблемы контроля доступа к Web-ресурсам, решение этого вопроса и вывод о том, какие средства действительно являются наиболее приемлемыми, так как несанкционированный доступ в современном мире является одной из важных проблем науки.*

Ключевые слова: *Web-ресурс, нецелевые Web-ресурсы, методы контроля доступа.*

Web-ресурс является одной или набором страниц, размещенных в сети Интернет, которые отображаются в виде текстовой информации, а также мультимедийных компонентов. С помощью них каждый пользователь может воспользоваться нужной ему информацией, однако, зачастую, бесконтрольный доступ в Интернет может привести к нецелевому использованию сервисов сети.

Такими нецелевыми Web-ресурсами могут быть:

- социальные сети (ok.ru; vk.com и т. д.);
- электронная почта и ее агенты (yandex.ru; rambler.ru; mail.ru и т. д.);
- программы передачи мгновенных сообщений (ICQ , QIP и т. д.) [1].

В связи с таким набором бесконтрольного использования пользователем интернет-ресурсов разработаны методы контроля доступа, которые позволяют:

- минимизировать уровень угрозы утечки информации или несанкционированного доступа;
- избежать нежелательных атак, в качестве которых чаще всего является реклама, спам, вирус, что может сильно повлиять на работоспособность ПК;
- оптимизировать нагрузку на локальную сеть.

К методам контроля доступа к Web-ресурсам относятся:

1. Протоколы Radius и TACACS+.

Для обоих протоколов необходима настройка секретного ключа для клиента и сервера. В этом случае происходит следующее:

- TACACS+ зашифрует всю связь между сервером и клиентом;
- протокол RADIUS зашифрует только пароль.

2. Контентная фильтрация.

Система фильтрации состоит из следующих компонентов:

- утилит;
- приложений;
- дополнений браузера;
- отдельного сервера.

3. Межсетевое экранирование с использованием черного списка ресурсов позволяет:

- с помощью установленных правил запрещать пользователям использовать программы мгновенных сообщений для общения в сети;
- с помощью черного списка ресурсов, то есть Black-листов, блокировать доступ к нецелевым сайтам.

1. Разграничение доступа.

Прежде чем пользователь сможет воспользоваться необходимыми данными в сети Интернет, ему предстоит пройти через систему защиты информации, к которой относятся:

- шифрование;
- контроль доступа;
- аутентификация.

В результате прохождения цикла системы защиты информации происходит следующее:

- авторизованному пользователю система защиты информации открывает доступ к хранимой информации;
- подсистема разграничения доступа определяет, к каким данным у него разрешен доступ, а к каким запрещен.

2. Избирательные таблицы управления доступом (Discretionaryaccess control list, DACL) [2].

В таких таблицах явно указывается, разрешен или запрещен доступ к объекту пользователю или группе.

Если они не были явно указаны, то DACL запрещает доступ.

Разграничение доступа и протоколы Radius и TACACS+ будут наиболее компетентны в решении вопроса контроля доступа, так как их функциональность позволяет полностью защитить информацию Web-ресурса.

Конечное решение заключается в следующем:

- с помощью протоколов провести аутентификацию;
- работу разграничения доступа можно объединить с данными протоколами, так как именно после аутентификации и авторизации система дает пользователю право на определенные действия (чтение, запись или изменение информации). В конечном счете, можно использовать одновременно несколько методов контроля доступа.

Контроль доступа к Web-ресурсам необходим:

- чтобы обезопасить информацию, которую выкладывает владелец в сеть;
- защитить операционную систему со всеми файлами, на которую может повлиять «ложный»Web-сайт.

Отсюда следует, что выбор программного обеспечения и метода контроля доступа целиком и полностью зависит от конкретных условий определенной компании или одного пользователя. При правильном подборе средств можно решить проблему нецелевого использования ресурсов сети, атак различного уровня, несанкционированного использования информации и (или) ее утечки, изменения и удаления важных ресурсов без участия владельца.

Литература

1. *Михеев В. А*. Доступ к Веб-ресурсам: проблемы контроля. 2013.
2. *Николова Т. Н.* Анализ существующих методов управления доступом к интернет-ресурсам и рекомендации по их применению. 2013.