www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.4.1

УДК 004.738.5:004.42
ББК 32.972.53

СИСТЕМА ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНЫХ ПРИЛОЖЕНИЙ ИНТЕРНЕТ-РЕСУРСОВ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
ba_benko@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Романовна Алеева

Студент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Был разработан проект программного комплекса фильтрации интернет-трафика на языке программирования C# и описаны его функциональные возможности. В результате проведенных экспериментов системой фильтрации были: удачно проверена корректность работы фильтрации по DNS-записи, удачно проверена корректность работы фильтрации по URL-адресу, сформированы отчеты о выявленных заблокированных сайтах в журнале фильтрации. Таким образом успешное проведение экспериментов позволяет утверждать о выполнение про-

граммного комплекса контент- фильтрации интернет-трафика поставленных перед ним задач.

Ключевые слова: интернет-трафик, фильтрация, конфиденциальная информация, информационная безопасность, программный комплекс.

Необходимость фильтрации интернет-трафика возникает, как и дома, так и для корпоративных сетей. Неограниченный доступ к интернету повышает шанс заражения ПЭВМ вредоносным программным обеспечением, фишинговым атакам и т.п. Второй проблемой, возникающей как в следствии внешних атак, заражения вредоносным программным обеспечением, так и в следствии действий внутреннего злоумышленника (или нарушителя, в т. ч. и неосознанного) – утечка конфиденциальной информации в следствии доступа к Интернет [7].

Согласно исследованию, реальный трафик в Интернете за 10 минут от средней корпоративной сети содержал приблизительно 57 000 пакетов, 1 100 сеансов и 26 протоколов. Большая часть трафика приходится на TCP-протоколы. Причем порты соединений – 80 и 443, которые чаще всего ассоциированы с протокола HTTP или HTTPS/TLS. Причем именно эти 2 протоколы составляют большую часть трафика, относящуюся к web-трафику (то есть использование пользователями web-браузеров) [2].

Анализ результатов содержимого интернет-трафика по информации, содержащейся в нем, показал, что среди интернет-трафика наиболее часто встречающимся является протокол HTTP, причем если рассматривать передаваемое содержимое, то большая часть трафика приходится на видео-трафик и web-контент [1; 4].

В результате анализа назначения фильтрации интернет-трафика с целью выбора подходящего вида фильтрации интернет-трафика было выделено 3 вида фильтрации [3; 5; 6; 8]:

1) пакетная фильтрация;

2) фильтрация по протоколам прикладного уровня;

3) фильтрация по контенту.

Для дальнейшей работы был выбран метод фильтрации по контенту.

Были проанализированы системы и методы контент-фильтрации, а также определена их применимость для каждого из каналов утечки информации: блокирование по IP-адресу, блокировка по DNS-записи, блокирование по URL-адресу, фильтрация по текстовому содержимому, фильтрация по расширениям и типам файлов, фильтрация результатов поиска.

В результате были выбраны два метода: блокировка по DNS-записи и блокировка по URL-запросу.

Разработка формализованной модели программного комплекса фильтрации интернет-трафика

Процесс блокировки по URL-адресам представляет собой:

$$Den_{URL} = \begin{cases} u_i \in U^D, \text{ресурс подлежит блокировке} \\ u_i \notin U^D, \text{ресурс не подлежит блокировке} \end{cases}$$

Процесс блокировки по DNS-именам представляет собой:

$$Den_{DNS} = \begin{cases} d_i \in D^D, \text{ресурс подлежит блокировке} \\ d_i \notin D^D, \text{ресурс не подлежит блокировке} \end{cases}$$

Множество URL-адресов $U = \{u_1, \ldots, u_n\}$, где URL-адрес u_i представляется двойкой:

$$u_i = (d_i, p_i),$$

где d_i – доменное имя *в* URL-адресе, p_i – путь запроса в URL-адресе.

Множество доменных имен (DNS-записей) $D = \{d_1, \ldots, d_m\}$, где $m \le n$,

Множество запрещенных URL-адресов $U^d = \{u_1^D, \ldots, u_{n'}^D\}$,

Множество запрещенных DNS-имен $D^d = \{d_1^D, \ldots, d_{m'}^D\}$.

Разработка архитектуры программного средства, реализующего программный комплекс фильтрации интернет-трафика

Архитектура программного комплекса, состоит из 6 основных модулей: модуль пользовательского интерфейса, модуль настройки, модуль отчета, модуль анализа трафика, модуль работы с трафиком, модуль базы данных запрещенных / разрешенных DNS, URL.

Архитектура программного комплекса представлена на рисунке 1 и в таблице.

Разработка алгоритмов работы программного комплекса фильтрации интернет-трафика

Программный комплекс фильтрации интернет – трафика предусматривает два метода фильтрации:

1) фильтрация по DNS-именам,

2) фильтрация по URL-адресу.

В первом случае сайт блокируется, если этот сайт находится в списке DNS-имен, которые следует блокировать.

Во втором случае страница сайта блокируется, если она находится в списке URL-адресов которые следует блокировать.

Описанные выше методы фильтрации легко формализовать в виде блок-схем, представленной на рисунке 2.

Блок-схема описывает обобщенный алгоритм фильтрации, включающий следующие шаги:

1) на втором шаге после ввода URL-адреса, загружается веб-страница;

2) на третьем шаге происходит фильтрация по DNS и URL;

3) на четвертом вывод результата: либо веб-страница заблокирована, либо страница загружается в первоначальном виде.

Далее был разработан проект программного комплекса фильтрации интернет-трафика на языке программирования C# и описаны его функциональные возможности.

Было проведено 3 экспериментальных исследования. В результате проведенных экспериментов системой фильтрации были: удачно проверена корректность работы фильтрации по DNS-записи, удачно проверена корректность работы фильтрации по

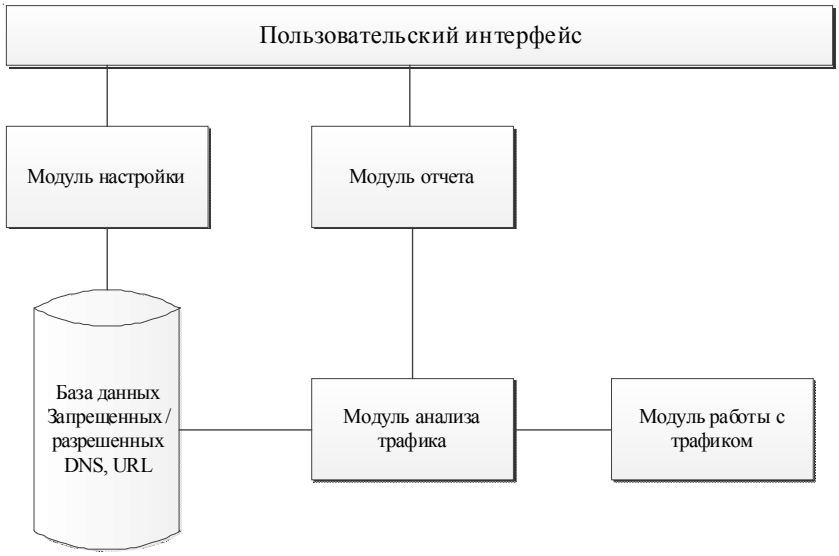

Рис. 1. Архитектура программного средства контент-фильтрации

Составные части архитектуры программного комплекса

Настройка	Состоит из создания и удаления списков доступа и по которым следует блокировать сайт
Анализ трафика	Выполняет анализ трафика на допуск к ним
Работа с трафиком	Выполняет задачу блокирования сайта
Отчет	Выводит список сайтов, к которым запрещен доступ

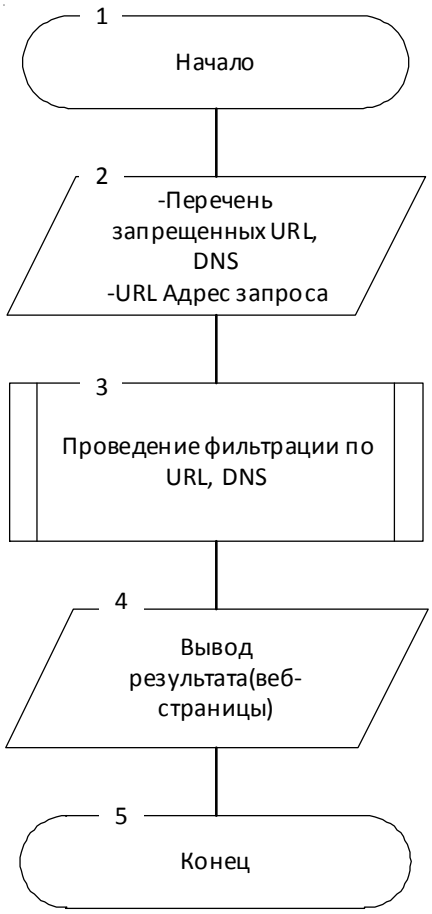

Рис. 2. Блок-схема алгоритма работы программного комплекса фильтрации интернет-трафика

URL-адресу, сформированы отчеты о выявленных заблокированных сайтах в журнале фильтрации.

Таким образом, успешное проведение экспериментов позволяет утверждать о выполнение программного комплекса контент-фильтрации интернет-трафика поставленных перед ним задач.

СПИСОК ЛИТЕРАТУРЫ

1. Лапонина, О. Р. Межсетевое экранирование / О. Р. Лапонина. – М. : Бином. Лаборатория знаний, 2007. – 343 с.

2. Медведовский, И. Д. Атака на Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – 2-е изд., перераб. и доп. – М. : ДМК, 2002. – 336 с.

3. Политики доступа и фильтрация трафика. – Электрон. текстовые дан. – Режим доступа: http://help.smart-soft.ru/index.html?howworkfilter. htm (дата обращения: 20.09.2020). – Загл. с экрана.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изм. и доп. в ред. от 13.07.2015). – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Фильтрация DNS запросов. – Электрон. текстовые дан. – Режим доступа: https://ospf-ripe.livejournal.com/2194.html (дата обращения: 23.09.2020). – Загл. с экрана.

6. Фильтрация HTTPS трафика. – Электрон. текстовые дан. – Режим доступа: https://www.carbonsoft.ru/фильтрация-https-трафика (дата обращения: 20.09.2020). – Загл. с экрана.

7. Чемодуров, А. С. Обзор средств фильтрации трафика в корпоративной сети / А. С. Чемодуров, А. Ю. Карпутина // Научно-методический электронный журнал «Концепт». – 2015. – № 2. – Электрон. текстовые дан. – Режим доступа: http://e-koncept.ru/2015/15039.htm. – Загл. с экрана.

8. URL-фильтрация или как пользователю ограничить доступ в интернет. – Электрон. текстовые дан. – Режим доступа: https://club.dns-shop.ru/forum/thread/46735 (дата обращения: 20.09.2020). – Загл. с экрана.

REFERENCES

1. Laponina O.R. *Mezhsetevoe ekranirovanie* [Firewall Protection]. Moscow, Binom. Laboratoriya znanij, 2007. 343 p.

2. Medvedovskij I.D., Sem'yanov P.V., Leonov D.G. *Ataka na Internet* [Attack on the Internet]. Moscow, DMK Publ., 2002. 336 p.

3. *Politiki dostupa i fil'traciya trafika* [Access Policies and Traffic Filtering]. URL: http://help.smart-soft.ru/index.html?howworkfilter.htm (accessed 20 September 2020).

4. *Federal'nyj zakon "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" ot 27.07.2006 № 149-FZ (s izm. i dopol. v red. ot 13.07.2015)* [Federal Law "About Information, Information Technologies and Information Protection" of 27 July 2006 no. 149-FZ (as Amended and Supplemented on 13 July 2015)]. Access from Reference Legal System "KonsultantPlyus".

5. *Fil'traciya DNS zaprosov* [DNS Query Filtering]. URL: https://ospf-ripe.livejournal.com/2194.html (accessed 23 September 2020).

6. *Fil'traciya HTTPS trafika* [Filtering HTTPS Traffic]. URL: https://www.carbonsoft.ru/fil'traciya-https-trafika (accessed 20 September 2020).

7. Chemodurov A.S., Karputina A.Yu. Obzor sredstv fil'tracii trafika v korporativnoj seti [Overview of Traffic Filtering Tools in the Corporate Network]. *Nauchno-metodicheskij elektronnyj zhurnal «Koncept»*, 2015, no. 2. URL: http://e-koncept.ru/2015/15039.htm.

8. *URL fil'traciya ili kak pol'zovatelyu ogranichit' dostup v internet* [URL Filtering or How to Restrict User Access to the Internet]. URL: https://club.dns-shop.ru/forum/thread/46735 (accessed 20 September 2020).

SYSTEM FOR FILTERING UNWANTED APPLICATIONS OF INTERNET RESOURCES

Alexey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Information Security,
Volgograd State University
ba_benko@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Yulia S. Bahracheva

Candidate of Sciences (Engineering), Associate Professor, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina R. Aleeva

Student, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru 100
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Currently, the role of the Internet in the life of society is growing, and the state's view of it is changing. Increasingly, the content posted on the Web goes beyond the laws of individual countries, their social norms, and the political lines of the authorities. Besides, Internet has a significant impact on intellectual property and telecommunications, jeopardizing the economic interests of many industries. These trends have contributed to the need to filter some types of content, and have caused disputes about the permissible limits of state intervention in the functioning of the network. Content filtering systems and methods were analyzed, and their applicability for each of the information leakage channels was determined: blocking by IP address, blocking by DNS record, blocking by URL, filtering by text content, filtering by

extensions and file types, filtering search results. The project of a software package for filtering Internet traffic in the C# programming language was developed and its functionality was described. As a result of the experiments carried out by the filtering system, the following results were obtained: the correctness of filtering by DNS record, the correctness of filtering by URL were successfully checked, reports on identified blocked sites in the filtering log were generated. Thus, the successful conduct of experiments allows us to assert that the software package of content filtering of Internet traffic performs the tasks assigned to it.

Key words: Internet traffic, filtering, confidential information, information security, software package.