МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»

(Самарский университет)

Институт \_информатики, математики и электроники

Факультет \_\_\_\_\_ математики\_\_\_\_\_\_

Кафедра \_\_ безопасности информационных систем\_\_

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**«Проектирование и разработка веб-фильтра для обеспечения контроля доступа к сетевым ресурсам»**

по специальности 10.05.01 Компьютерная безопасность

(уровень специалитета)

специализация

«Информационно-аналитическая и техническая экспертиза компьютерных систем»

Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.А. Бизин

Руководитель ВКР,

к.ф.-м.н., старший преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Бурлов

Консультант (*при наличии)*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Нормоконтролер(*при наличии*)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Самара 2019

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc527904237)

[ВВЕДЕНИЕ 3](#_Toc527904238)

[1 Предметная область 5](#_Toc527904239)

[1.1 Веб-фильтр 6](#_Toc527904240)

[1.2 Методы контентной фильтрации 10](#_Toc527904241)

[1.3 Категоризация ресурсов сети интернет 13](#_Toc527904242)

[2 Технологии 16](#_Toc527904243)

[3 Наработки 17](#_Toc527904244)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 18](#_Toc527904245)

[СПИСОК СОКРАЩЕННЫХ ОБОЗНАЧЕНИЙ 19](#_Toc527904246)

# ВВЕДЕНИЕ

Веб-фильтр (контент-фильтр) – это программное или программно-аппаратное устройство, которое ограничивает доступ к веб-сайтам на основании анализа их содержимого. Кроме анализа содержимого сайтов контент-фильтры также могут ограничивать доступ по *IP*-адресу ресурса (черные списки сайтов).

В настоящее время контентную фильтрацию нельзя выделить в отдельную область компьютерной безопасности, настолько она переплелась с другими направлениями. В обеспечении компьютерной безопасности контентная фильтрация очень важна, поскольку позволяет вычленять потенциально опасные вещи и корректно их обрабатывать. Подходы, появившиеся при разработке продуктов для контентной фильтрации, находят применение, например, в продуктах для предотвращения вторжений (*IDS*).

В последнее время в интернете все больше появляется противозаконного контента, ориентированного на школьников и подростков. Блокирование таких ресурсов по *IP*-адресу не приносит особого результата, т.к. в основном эти сайты создаются сотнями каждый день, и требуется время для их обнаружения и внесения в черный список. В такой ситуации фильтрация на основании содержимого сайта будет давать наилучший результат. В связи с этим тема фильтрации (классификации) веб-контента очень актуальна в образовательных учреждениях. Также с целью соблюдения политики информационной безопасности на предприятиях можно использовать веб-фильтр для ограничения доступа сотрудников к нежелательному контенту (например, социальные сети), что также добавляет актуальности теме контент-фильтрации.

Таким образом, целью работы является проектирование и разработка веб-фильтра для обеспечения контроля доступа к сетевым ресурсам.

Для достижения поставленной цели были сформулированы следующие задачи:

* проектирование веб-фильтра (выбор и обоснование используемых технологий);
* выбор и обоснование алгоритма классификации текста;
* разработка веб-фильтра;
* тестирование работы веб-фильтра.

# Предметная область

Одна из общих тенденций развития продуктов информационной безопасности — стремление реализовать различные функции в одном устройстве или программном решении. Как правило, разработчики стараются выполнить решения, которые кроме функций контентной фильтрации еще выполняют и функции антивируса, межсетевого экрана и/или системы обнаружения и предотвращения вторжений. С одной стороны, это позволяет снизить затраты компаний на покупку и сопровождение систем безопасности, но с другой — функциональность таких систем часто оказывается ограниченной. Например, во многих продуктах функции фильтрации веб-трафика сведены только к проверке адресов сайтов относительно какой-либо базы данных категорий сайтов.

В существующих уже достаточно давно областях контентной фильтрации — контроле почты и интернет-трафика — также происходят изменения, появляются новые технологии.

В продуктах для контроля почтового обмена стала выходить на первый план функция защиты от фишинга. А в продуктах для контроля интернет-трафика происходит смещение от использования заранее подготовленных баз данных *IP*/*URL* сайтов к категоризации по содержимому «на лету», что является очень актуальным решением, т.к. современные сайты могут часто изменять свой контент.

Кроме двух указанных выше областей, возникают и новые области применения контентной фильтрации — некоторое время назад начали появляться продукты для контроля за передачей мгновенных сообщений (*instant messaging*) и *peer-to-peer* (*p*2*p*) соединений [1]. В настоящее время также активно разрабатываются продукты для контроля за *VoIP*-трафиком [1].

Во многих странах стали активно развивать средства для перехвата и анализа многих видов информации, которая используется для различного вида расследований. Данные мероприятия проводятся на государственном уровне и наиболее часто привязываются к расследованию террористических угроз. Такие системы перехватывают и анализируют не только данные, передаваемые по каналам сети интернет, но также и по другим видам связи — телефонным линиям, радиоканалам и т.п. Наиболее известной системой для перехвата информации является *Echelon* — система, использовавшаяся американской разведкой для сбора информации [2]. В России также существуют различные реализации СОРМ, которые используются для захвата и анализа информации в интересах спецслужб [3].

## Веб-фильтр

Как уже говорилось выше, веб-фильтр (контент-фильтр) – это программное или программно-аппаратное устройство, которое ограничивает доступ к веб-сайтам на основании анализа их содержимого. В данной работе будет рассмотрена программная реализация. По своей сути контент-фильтр – это веб прокси-сервер, который перехватывает *HTTP/HTTPS*-запросы и анализирует их.

Упрощенный алгоритм работы веб-фильтра по шагам:

1. Перехват *HTTP/HTTPS*-запроса пользователя к интернет-ресурсу.
2. Анализ запроса (проверка *IP*-адреса интернет-ресурса, анализ самого *HTTP/HTTPS-*запроса).
3. На основании анализа принять решение: позволить осуществить запрос к интернет-ресурсу или отклонить его.
4. Если было принято решение об отклонении запроса, то производится возврат пользователю информации об отклонении (например, веб-страница). Если же было решено пропустить запрос, то веб-фильтр делает запрос к ресурсу.
5. Перехват ответа от интернет-ресурса.
6. Анализ ответа (анализ возвращенного контента, классификация контента).
7. На основании анализа контента принять решение: пропустить ответ от ресурса пользователю или отклонить его.
8. Если было принято решение об отклонении ответа, то производится возврат пользователю информации об отклонении (например, веб-страница). Если же было решено пропустить ответ, то веб-фильтр возвращает ответ от интернет-ресурса пользователю.

На рисунке 1 показана схема работы веб прокси-сервера.



Рис. 1 – Схема работы веб-фильтра

В приведенном выше алгоритме умалчивается один факт: контент, передаваемый по протоколу *HTTPS*, зашифрован. Поэтому анализировать его без расшифрования не представляется возможным. Это существенное ограничение функциональности контент-фильтра, т.к. на данный момент в интернете сайты, работающие по протоколу *HTTPS*, преобладают над сайтами, работающими по незащищенному протоколу *HTTP*. Поэтому для того, чтобы веб-фильтр работал максимально эффективно, нужно расшифровывать контент с использованием поддельного сертификата и применением технологии *Trusted MITM* [4].

Взаимодействие пользователя и веб-сервера с использованием протокола *HTTPS* выглядит следующим образом:

1. Клиент (браузер) запрашивает у веб-сервера ресурс (веб-страницу) по протоколу *HTTPS*.
2. Веб-сервер отправляет клиенту свой открытый ключ и сертификат.
3. Браузер выполняет проверку сертификата сервера: по сроку действия, не отозван ли сертификат, совпадение поля *Common Name* в сертификате и запрашиваемого доменного имени. Если все проверки пройдены успешно, браузер генерирует симметричный ключ, шифрует его открытым ключом сервера и отправляет его обратно.
4. Веб-сервер расшифровывает симметричный ключ, используя свой закрытый ключ. Затем шифрует контент симметричным ключом и отправляет его клиенту.
5. Браузер расшифровывает контент симметричным ключом и отображает его.

Взаимодействие браузера с веб-сервером по протоколу *HTTPS* по шагам показано на рисунке 2.



Рис. 2 – Взаимодействие браузера и веб-сервера по протоколу *HTTPS*

Схема использования технологии *Trusted MITM* веб-фильтром (который в данной ситуации также называется прозрачным прокси-сервером) упрощенно показана на рисунке 3.



Рис. 3 – Упрощенная схема перехвата и обработки *HTTPS* трафика

Более подробная схема описана ниже:

1. Перехват веб-фильтром запроса браузера к веб-серверу по протоколу *HTTPS*.
2. Прозрачный прокси-сервер делает запрос из шага 1 к веб-серверу по протоколу *HTTPS*.
3. Веб-сервер отправляет прокси-серверу свой открытый ключ и сертификат.
4. Веб-фильтр генерирует симметричный ключ, зашифровывает его открытым ключом сервера и отправляет обратно веб-серверу.
5. Веб-сервер расшифровывает симметричный ключ, используя закрытую часть, и отправляет прокси-серверу контент, зашифрованный симметричным ключом.
6. Веб-фильтр расшифровывает контент при помощи симметричного ключа и сохраняет его. Затем прокси-сервер генерирует ключевую пару (открытый и закрытый ключи) и сертификат для запрашиваемого браузером доменного имени (в поле *Common Name* сертификата проставляется доменное имя). Сгенерированный сертификат подписывается доверенным корневым сертификатом (которому доверяет браузер). Веб-фильтр отправляет сгенерированный открытый ключ и сгенерированный сертификат клиенту.
7. Браузер проверяет сгенерированный сертификат веб-фильтра. В случае прохождения проверок, браузер генерирует симметричный ключ, шифрует его открытым ключом прокси-сервера и отправляет обратно.
8. Веб-фильтр расшифровывает симметричный ключ, используя закрытую часть ключа. Затем шифрует сохраненный контент симметричным ключом и отправляет его клиенту.
9. Браузер расшифровывает контент при помощи симметричного ключа и отображает его.

Описанная выше схема по шагам показана на рисунке 4.



Рис. 4 – Схема работы прозрачного прокси-сервера

## Методы контентной фильтрации

Существует большое количество методов и алгоритмов контентной фильтрации. На практике обычно применяется совокупность методов, что необходимо для обеспечения лучших результатов работы веб-фильтра, поскольку различные методы позволяют достигать требуемых результатов только на определенном типе фильтруемых данных. Однако можно выделить три наиболее общих класса методов фильтрации [5]:

* фильтрация с использованием справочника ключевых слов;
* фильтрация на основе списков *IP*/*URL*;
* динамическая фильтрация.

Фильтрация по ключевым словам – наиболее простой способ фильтрации, поэтому он часто применяется как отдельно (в простых системах для домашнего использования), так и в комбинации с другими методами фильтрации. Этот метод позволяет включать блокировку страницы либо сайта целиком при наличии в них слов или словосочетаний из справочника. Метод прост в реализации и использовании, но имеет существенный недостаток: он может блокировать ресурсы, в которых фильтруемые слова используются в другом контексте (т.н. избыточная фильтрация).

*IP*/*URL*-фильтрация позволяет блокировать ресурсы по справочнику *IP*-адресов или *URL* (возможен смешанный режим). Справочник может наполняться как вручную, так и автоматически, на основе алгоритма предварительного анализа ресурсов. Также этот метод носит название черных списков.

Динамическая фильтрация – широкий класс методов, в которых содержимое ресурса анализируется в момент поступления запроса к ресурсу. Доступ к ресурсу блокируется, если его содержимое определяется как несоответствующее политике безопасности.

Основное отличие *IP*/*URL*-фильтрации и динамической фильтрации заключается в моменте анализа содержимого ресурса. Согласно рисунку 1 *IP*/*URL*-фильтрация происходит после шага 1, перед отправкой запроса на сервер, где расположен сайт, а динамическая фильтрация происходит после шага 3, после получения ответа от сервера.

В таблицах 1 и 2 приведено сравнение наиболее распространенных систем контентной фильтрации по ряду наиболее важных критериев (по принципу наличия или отсутствия функциональности) [5]. Из обзора существующих решений можно сделать вывод, что имеются системы различного класса и различной функциональности, но нет единого подхода к реализации одних и тех же функциональных возможностей даже среди систем одного класса. Лидирующие системы контентной фильтрации основываются на принципе анализа и категоризации интернет-ресурсов, что признано наиболее эффективным методом фильтрации нежелательного контента. Эти системы используют регулярно обновляемые базы *URL*, гибкие настройки фильтра и развитые системы отчетности.

Все рассмотренные системы фильтрации либо не используют центральные БД, либо используют закрытые БД ресурсов, свободный доступ к которым невозможен. Содержание таких БД обычно является наибольшей ценностью для компаний-разработчиков подобных систем.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Система контентной  фильтрации  Критерий | Дозор-Джет | Dans-  Guardian | Smooth-  Guardian | Cyber  Patrol | Cyber  Snoop |
| Фильтрация по *IP*/*URL* | Да | Да | Да | Да | Да |
| Фильтрация по терминам входящих данных | Да | Да | Да | Да | Да |
| Фильтрация по терминам исходящих данных | Да | Нет | Нет | Нет | Да |
| Фильтрация по портам | Да | Нет | Нет | Нет | Нет |
| Наличие локальной БД | Да | Да | Да | Да | Да |
| Наличие центральной БД | Да | Нет | Нет | Да | Да |
| Установка на рабочую станцию | Нет | Да | Да | Да | Да |
| Установка на шлюз | Да | Да | Да | Нет | Нет |
| Управление временем работы | Да | Нет | Да | Да | Нет |
| Сбор статистики | Да | Нет | Да | Да | Да |
| Встроенная поддержка русского языка | Да | Нет | Да | Нет | Нет |
| Наличие графического интерфейса | Нет | Нет | Нет | Да | Да |

Таблица 1 – Сравнение систем контентной фильтрации по критериям

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Система контентной  фильтрации  Критерий | Net  Nanny | Cyber  Sitter | Wizguard | Cyber  Sentinel |
| Фильтрация по *IP*/*URL* | Да | Да | Да | Да |
| Фильтрация по терминам входящих данных | Нет | Нет | Нет | Да |
| Фильтрация по терминам исходящих данных | Нет | Нет | Да | Да |
| Фильтрация по портам | Нет | Нет | Нет | Нет |
| Наличие локальной БД | Да | Да | Нет | Да |
| Наличие центральной БД | Да | Да | Да | Да |
| Установка на рабочую станцию | Да | Да | Да | Да |
| Установка на шлюз | Нет | Нет | Нет | Нет |
| Управление временем работы | Нет | Нет | Нет | Нет |
| Сбор статистики | Да | Да | Да | Да |
| Встроенная поддержка русского языка | Нет | Нет | Нет | Нет |
| Наличие графического интерфейса | Да | Да | Да | Да |

Таблица 2 – Сравнение систем контентной фильтрации по критериям

## Категоризация ресурсов сети интернет

Все сайты сети интернет могут быть отнесены к одной или нескольким категориями. Категории задаются разработчиком системы контентной фильтрации. Можно выделить несколько способов категоризации ресурсов в сети интернет [5]:

* использование регулярно обновляемых баз данных категоризированных ресурсов (система категоризации работает со списком категорий, категоризирует новые ресурсы и обновляет связи между категориями и существующими ресурсами);
* категоризация контента «на лету» при помощи анализа содержимого страниц;
* использование данных о категории, информацию о принадлежности к которой предоставляет сам сайт.

Категоризация данных и формирование баз данных категорий обычно производится в полуавтоматическом режиме – сначала выполняются анализ содержимого и определение категории с помощью алгоритмов классификации. На втором этапе полученная информация часто проверяется людьми, принимающими решение о том, к какой категории можно отнести тот или иной сайт.

К преимуществам применения предопределенных баз категорий можно отнести то, что предоставление или запрет доступа производится еще до запроса к самому сайту, что может существенно снизить нагрузку на веб-фильтр. Главный же недостаток использования данного подхода — задержки в обновлении баз категорий сайтов, поскольку для анализа потребуется некоторое время. Кроме того, некоторые сайты достаточно часто меняют свое наполнение, из-за чего информация о категории, хранящаяся в базе, становится неактуальной.

Категоризация сайтов на лету также осуществляется самыми разными способами. Особенно часто используются методы, основанные на статистическом подходе к анализу содержания.

Один из простых вариантов реализации такого решения — использование байесовских алгоритмов, которые себя достаточно хорошо зарекомендовали в борьбе со спамом. Однако у этого варианта есть свои недостатки — необходимо периодически доучивать алгоритм, корректировать словари в соответствии с передаваемыми данными. Поэтому некоторые компании применяют более сложные алгоритмы определения категории сайта по содержимому в дополнение к простым способам.

Категоризация данных на лету позволяет быстро реагировать на появление новых сайтов, поскольку информация о категории сайта не зависит от его адреса, а только от содержания. Но такой подход имеет и недостатки — необходимо проводить анализ всех передаваемых данных, что вызывает некоторое снижение производительности веб-фильтра. Второй недостаток — необходимость поддержания актуальных баз категорий для различных языков. Тем не менее, некоторые продукты применяют этот подход с одновременным использованием баз данных категорий сайтов. Сюда можно отнести использование *Virtual Control Agent* в продуктах компании *SurfControl*, механизмы определения категорий данных в "Дозор-Джет".

## Методы автоматической классификации текстов

Следует отличать классификацию от кластеризации. При классификации документов категории определены заранее, при кластеризации они не заданы и даже информация об их количестве может отсутствовать.

Формально постановку задачи классификации можно записать следующим образом. Имеются множество документов и множество заранее заданных категорий (классов) . Неизвестная целевая функция задается формулой:

(1)

Требуется построить классификатор , максимально близкий к Ф.

Если классификатор определяется формулой (1), то он называется точным. Если же классификатор возвращает значение из диапазона [0,1] (вероятность попадания документа в категорию ), то он называется вероятностным.

### 1.3.1 Наивный байесовский классификатор

Наивный байесовский классификатор является один из алгоритмов классификации. Относится к категории алгоритмов машинного обучения с учителем.

# Технологии

# Наработки

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Современные тенденции в области контентной фильтрации [Электронный ресурс]. – 2013. – Режим доступа: http://alexott.net/ru/writings/cf/, свободный. – Яз. рус.

2 Антонов, И. Под колпаком Эшелона [Электронный ресурс]. – 2014. – Режим доступа: http://iantonov.me/page/pod-kolpakom-eshelona, свободный. – Яз. рус.

3 Хазов, В. СОРМ-1, СОРМ-2, СОРМ-3: особенности и отличия [Электронный ресурс]. – 2016. – Режим доступа: https://vasexperts.ru/blog/osobennosti-i-otlichiya-sorm/, свободный. – Яз. рус.

4 Пискунов, И. Перехват и расшифровка HTTPS трафика [Электронный ресурс]. – 2016. – Режим доступа: https://ipiskunov.blogspot.com/2016/06/https.html, свободный. – Яз. рус.

5 Масюк, А.А, Сараджишвили, С.Э. Тематическая категоризация ресурсов в системах контентной фильтрации [Текст] / А.А. Масюк, С.Э. Сараджишвили // Научно-технические ведомости СПбГПУ. Сер. Информатика. Телекоммуникации. Управление. –2013. –№ 1.

# СПИСОК СОКРАЩЕННЫХ ОБОЗНАЧЕНИЙ

*IP*-адрес (*Internet Protool*) – уникальный сетевой адрес узла в компьютерной сети

*IDS* (*Intrusion Detection System*) – система обнаружения вторжений

*VoIP* (*Voice over IP*) – технология передачи звукового сигнала в *IP*-сетях

*HTTP* (*HyperText Transfer Protocol*) – протокол передачи гипертекста. Широко используется в сети интернет

*HTTPS* (*HyperText Transfer Protocol Secure*) – расширение протокола *HTTP* с поддержкой шифрования передаваемой информации

*Trusted MITM* (*Man-In-The-Middle*) – технология перехвата *HTTPS*-трафика, путем подмены сертификата доверенным «лицом» (программой)

*URL* (*Uniform Resource Locator*) – единообразный определитель ресурса в сети интернет

БД – база данных

СОРМ – система оперативно-розыскных мероприятий