УДК 37.014:004
ББК Ч402.684.3 ГРНТИ 14.25.07 Код ВАК 13.00.02

Емельянов Дмитрий Александрович,
кандидат технических наук, доцент кафедры информатики, информационных технологий и методики обучения информатике, Институт математики, физики, информатики и технологий, Уральский государственный педагогический университет; 620075, г. Екатеринбург, ул. К. Либкнехта, 9; e-mail: eda@uspu.me.

ФИЛЬТРАЦИЯ СЕТЕВОГО КОНТЕНТА В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

КЛЮЧЕВЫЕ СЛОВА: защита информации; негативная информация; контент-фильтры; правовые ограничения; сетевые контенты; технические ограничения; нормативно-правовые акты; интернет; информационные технологии; технические методы; сетевые трафики.

АННОТАЦИЯ. В 2006–2008 годах в рамках реализации приоритетного национального проекта «Образование» было осуществлено подключение более 50000 образовательных учреждений Российской Федерации к сети Интернет. Однако наряду с полезной и необходимой информацией, способствующей получению новых знаний и построению эффективного процесса обучения, обучаемые получили доступ к ресурсам, содержащим нежелательное содержание (агрессивное, неэтичное и др.). С целью защиты учащихся образовательных учреждений РФ от противоправного и агрессивного контента в 2006–2007 годах была разработана и внедрена федеральная Система исключения доступа к Интернет-ресурсам, несовместимым с задачами образования обучающихся РФ (СИД). Согласно федеральному закону Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в срок до 1 сентября 2012 г. во всех образовательных учреждениях на территории Российской Федерации обязательным требованием является установка персонального контент-фильтра на каждый компьютер.
Контент-фильтр — устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определенным сайтам или услугам сети Интернет. Средствами контент-фильтрации (СКФ) доступа к сети Интернет являются аппаратно-программные или программные комплексы, обеспечивающие ограничение доступа к Интернет-ресурсам, несовместимым с задачами образования и воспитания обучаемых.
В данной статье рассмотрены основные положения, связанные с фильтрацией сетевого контента: законы, регулирующие сеть Интернет, технические методы фильтрации сетевого трафика, существующие современные контент-фильтры их возможности и недостатки. Предложена система контентной фильтрации «Selecta», которая предназначена для фильтрации интернет-трафика для образовательных учреждений, разработанная на кафедре информатики, информационных технологий и методики обучения информатике Уральского государственного педагогического университета совместно с ООО IDECO SELECTA г. Екатеринбург.

Emelyanov Dmitry Alexandrovich,
Candidate of Technical Sciences, Associate Professor, Department of Informatics, Computer Technology and Methods of Teaching Informatics, Institute of Mathematics, Physics, Informatics and Technology, Ural State Pedagogical University, Ekaterinburg, Russia.

FILTERING THE NETWORK CONTENT IN EDUCATIONAL INSTITUTIONS

KEYWORDS: information protection; negative information; content filter; legal restrictions; net content; technical restrictions; laws and regulations; Internet; information technologies; technical methods; net traffic.

ABSTRACT. In 2006–2008, as part of the priority national project «Education», more than 50,000 educational institutions of the Russian Federation were connected to the Internet. However, along with useful and necessary information that contributes to obtaining new knowledge and building an effective learning process, students have access to resources that contain undesirable content (aggressive, unethical, etc.). In order to protect students of educational institutions of the Russian Federation from illegal and aggressive content in 2006–2007 a Federal system of access exception to Internet resources incompatible with the tasks of education and training of students of the Russian Federation was developed and implemented. According to the Federal law of the Russian Federation of December 29, 2010 № 436-FZ «On protection of children from information harmful to their health and development» by September 1, 2012. it is obligatory to install a personal content filter on each computer in all educational institutions in the territory of the Russian Federation.
Content-filter is a device or software to filter sites by their content, which does not allow access to certain sites or services on the Internet. Means of content filtering of access to the Internet are hardware-software or software systems that provide restriction of access to Internet resources that are incompatible with the objectives of education and upbringing of students.
This article describes the main provisions related to the filtering of network content: laws governing the Internet, technical methods of filtering network traffic, existing modern content filters their capabilities and shortcomings. The system of content filtering «Selecta», which is designed to filter Internet traffic for educational institutions, developed at the Department of Informatics, Information Technologies and Methods of Teaching Informatics of the Ural State Pedagogical University in cooperation with IDECO SELECTA Ekaterinburg, is proposed.

Интернет — всемирная система объединенных компьютерных сетей для хранения и передачи информации. Интернет появился в 60-х годах XX века на ос-

нове сетей ARPANET [1]. Основными концепциями сети Интернет являлись:

- *Децентрализованность* сети — все компьютеры сети являются равноправными.
- *Пакетная передача данных* — данные разбиваются на небольшие куски, каждый из которых отправляется по своему маршруту.

Интернет развивался, однако широкую популярность он получил после изобретения в 1991 году британским ученым Т. Бернерс-Ли Всемирной Паутины (World Wide Web) — компьютерной сети на основе Интернет, предоставляющей доступ к связанным между собой документам [2]. Чаще всего документами является гипертекст на языке разметки HTML. Изначально для просмотра документов во всемирной паутине предлагался протокол прикладного уровня Gopher, но потом его быстро заменил протокол HTTP [27].

Всемирная паутина задумывалась как децентрализованная сеть, открытая для расширения и добавления новой информации, связывающая все документы воедино через систему уникальных идентификаторов — URI [3]. Любой человек, владеющий знаниями HTML, а часто и без них, может создать и опубликовать во Всемирной Паутине любую информацию или любой файл. Таким образом, в Интернете может быть опубликована информация любого рода, как положительная (познавательная, учебная, справочная, развлекательная и т. д.), так и негативная (агрессивная, террористическая, неэтическая и пр.).

Интернет — хороший источник знаний для учебного процесса, т. к. предоставляет множество разнообразных ресурсов, начиная от Википедии до онлайн-библиотек и сканов оригиналов документов. Тем не менее, в сети Интернет также много нежелательных или откровенно вредных ресурсов, которые следует отсекать от учебного процесса в образовательных учреждениях.

Таким образом, возникает необходимость решения важной *психолого-педагогической задачи — оградить обучаемых в ходе образовательного процесса от вредных отвлекающих факторов — нежелательного сетевого контента и сервисов*. В настоящее время любому образовательному учреждению при использовании глобальной сети требуется установка контент-фильтра, выбор которого можно осуществить в зависимости от решаемых задач, имеющегося оборудования, установленного программного обеспечения, квалификации обслуживающего персонала и стоимости. Данная статья позволяет обобщить существующие нормативные документы и требования в данной области, существующие методы фильтрации трафика, способы организации контентной защиты в образовательном учреждении, а также предложить свое решение проблемы. Материал, приведенный ниже, может быть полезен при выборе контент-фильтра в любом образовательном учреждении.

Законы, регулирующие работу сети Интернет

Интернет долгое время развивался на принципах саморегулирования. Однако рост популярности и использование всемирной паутины для коммерческих целей потребовало внесение норм права для регулирования правоотношений в сети. В различных странах в зависимости от распространенности Интернета действуют свои собственные законы и системы фильтрации.

Северная Корея (*КНДР*) имеет крайне ограниченный выход в мировой Интернет, однако существует внутренняя изолированная сеть, которая называется Кванмён. Доступ в Интернет имеется только у ограниченного количества учреждений [4]. Кванмён насчитывает порядка 1–1,5 тысяч сайтов, в основном научных и учебных организаций. Доступ к Кванмёну осуществляется по телефонным линиям Dial-Up. Согласно утечки данных в 2016 году, в интернет-сегменте, принадлежащем КНДР, зарегистрировано всего 28 сайтов [5].

Китай. Здесь Интернет доступен для широкого круга людей, однако ограничен и фильтруется в рамках проекта «Золотой щит» [6]. Для всех внутренних веб-сайтов требуется регистрация при создании, а публикация новостей из мирового Интернета запрещена без специального одобрения. Фильтрация страниц происходит на основе «черного списка» сайтов и по ключевым словам в тексте [7]. Для фильтрации между мировым Интернетом и локальным китайским используется «Великий Китайский Фаервол». Через него проходит весь трафик между Китаем и прочими странами. В результате скорость доступа к иностранным сайтам падает на порядок, что подстегивает развитие местных сайтов. В Китае блокируются популярные западные социальные сети, а поисковые системы (Yahoo, Google) ограничивают политически мотивированные результаты. В качестве альтернативы предлагаются внутренние сервисы. Вместо поиска Google популярен местный поисковик Baidu, вместо Amazon предлагается использовать Taobao.com или AliExpress.com [14].

США. Фильтрация сетевого контента запрещена 1-й поправкой к Конституции США. Запрет на распространение материалов в сети может быть связан лишь с нарушением положений законодательства о клевете, детской порнографии, интеллектуальной собственности. Кроме того, некоторые школы и библиотеки блокируют на

своих компьютерах доступ к вредной для детей информации. Фильтрацию Интернет пытаются ввести в рамках борьбы с пиратством — законопроекты SOPA и PIPA приняты в 2011 году [10], но до сегодняшнего дня оба отложены [14].

РОССИЯ. В российском сегменте Интернет (Рунет) документами, ограничивающими контент, являются:

- Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 [22] и ряд поправок;
- Федеральный закон № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 [15];
- Федеральный закон № 139 «О внесении изменений в федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию"» от 28.07.2012 (статьи 6, 55, 119, 140) [16];
- Федеральный закон № 185 «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу законодательные акты (отдельные положения законодательных актов) Российской Федерации в связи с принятием федерального закона "Об образовании в Российской Федерации"» от 02.07.2013 [17];
- статья 29 Федерального закона № 307 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» и отдельные законодательные акты РФ «О признании утратившими силу отдельных положений законодательных актов Российской Федерации в связи с уточнением полномочий государственных и муниципальных органов в части осуществления государственного и муниципального контроля (надзора)» от 14.10.2014 [18].

Контроль над исполнением всех этих документов осуществляет ведомство Роскомнадзор.

Технические методы фильтрации сетевого трафика

Существует несколько способов фильтрации трафика на различных уровнях TCP/IP стека. Каждый TCP/IP-пакет характеризуется 4 параметрами: IP адрес источника, IP-адрес назначения, порты источника и назначения. Зная IP-адрес источника, можно определить, кто из пользователей послал этот пакет, а зная IP-адрес и порт назначения, можно понять, кому предназначен этот пакет и необходимо ли проверять данный пакет и всю TCP/IP сессию. Собирая и проксируя трафик нужных TCP/IP сессий, можно получить дополнительные сведения для фильтрации HTTP(S) запросов, такие как: URL запроса, домен и тело запроса. Для полученных сведений можно использовать различные методы фильтрации.

Блокирование по IP-адресу. При применении данного метода сервер, на котором находится нежелательный материал, становится полностью недоступным для пользователя. Главным преимуществом этого метода является его простота — он может быть реализован с помощью базового сетевого оборудования, используемого интернет-провайдерами. Однако с учетом современных технологий по одному IP-адресу могут находиться тысячи сайтов, а также других сервисов, таких как FTP или электронная почта, поэтому его блокирование приведет к тому, что все они станут недоступны. Из-за низкой точности данного метода страны применяют его с осторожностью. Блокирование по IP-адресу можно достаточно легко обойти при помощи различных технических решений, в частности, прокси-серверов и *VPN (Virtual Private Network)* — это технология, обеспечивающая защищенную (закрытую от внешнего доступа) связь логической сети поверх частной или публичной.

Искажение DNS-записей. При обращении пользователя к любому сайту компьютер посылает запрос к DNS-серверу для того, чтобы преобразовать доменное имя в IP-адрес. В случае применения данного метода DNS сервер возвращает неверный адрес, и сайт оказывается недоступным. Искажение DNS-записи также может быть реализовано без применения дополнительного оборудования. Его преимуществом перед блокированием по IP-адресу является более высокая точность — недоступным становится только один сайт на сервере. При этом все равно происходит чрезмерное блокирование. Например, Китай периодически лишает своих пользователей доступа к CNN International из-за появляющихся там нежелательных новостей. Хотя целью фильтрации ставится блокирование только одной страницы новости, остальные страницы сайта также становятся недоступны. Искажение DNS-записей легко обходится пользователями — в настройках операционной системы достаточно указать альтернативный DNS-сервер или вручную прописать IP-адрес заблокированного сайта.

Блокирование по URL-адресу. В HTTP-протоколе URL-адрес содержит доменное имя сайта, а также параметры запроса. Они могут быть сверены со списком заблокированных ключевых слов, и в случае соответствия связь пользователя с запрошенным ресурсом разрывается, или он перенаправляется на блок-страницу. Данный метод является более эффективным по сравнению с блокированием по IP-адресу и искажением DNS-записи, но требует дополнительного оборудования, так как использует поверхностный анализ пакетов. Его дополнитель-

ным преимуществом является то, что он способен динамически блокировать новые страницы, если в их адресе содержатся запрещенные слова. Например, в Китае блокируются все запросы, содержащие слова «falun» и «gong». Однако при неправильной настройке ключевых слов точность метода резко ухудшается — он может пропускать нежелательный материал или, наоборот, допускать чрезмерное блокирование. Блокирование по URL-адресу нельзя обойти с помощью обычных прокси-серверов — необходимы инструменты, которые шифруют трафик, такие как VPN или TOR.

Блокирование по типу файла. В ответе на HTTP-запрос сервер устанавливает заголовок *Content-Type*, в котором описывается тип передаваемого контента. Значением этого заголовка является один из подходящих MIME-типов. MIME — стандарт передачи различных типов данных по электронной почте, а также спецификация для кодирования информации и форматирования сообщения. Сопоставляя значения заголовка Content-Type и запрещенные для пересылки типы файлов, можно фильтровать запросы. Этот метод не является надежным средством для блокировки.

Фильтрация HTTPS-запросов. Заголовки и тело HTTP-запросов передаются в открытом виде, поэтому фильтр может их выделить и использовать для проверки сайта. Однако для страниц HTTPS сайтов невозможно узнать заголовки запросов из-за шифрования трафика. Поэтому для HTTPS-запросов фильтры производят атаку MiTM [9] и подменяют полностью или частично все сертификаты сайтов [21]. Важным расширением протокола TLS является SNI — Server Name Indication. С помощью этого расширения домен доступен в открытом виде. Это расширение используется для организации нескольких HTTPS-сайтов на одном IP-адресе, но также дает возможность фильтру подменять сертификаты только для определенных сайтов [11].

Пакетная фильтрация. Наиболее сложный и дорогостоящий метод, так как он требует применения глубокого анализа пакетов. На данный момент полноценно реализован только в Китае. При использовании пакетной фильтрации изучаются не только заголовки пакетов, содержащих URL адрес, но и все их содержимое. В случае наличия запрещенных слов связь между пользователем и сервером разрывается. Метод позволяет фильтровать нежелательный контент не только в веб-страницах, но и во всех протоколах — электронной почте, сервисах мгновенных сообщений и др. Существенным недостатком данного метода является то, что применение глубокого анализа пакетов может привести к существенному снижению скорости интернет-соединения, что, к примеру, наблюдается при доступе из Китая к зарубежным интернет-серверам. В остальном пакетная фильтрация обладает теми же достоинствами и недостатками, что и блокирование по URL-адресу.

Фильтрация через HTTP прокси-сервер. Данный метод наиболее часто используется организациями для подключения корпоративных сетей к Интернету, но его можно использовать для фильтрации Интернета в рамках всей страны. Гибридный вариант под названием Cleanfeed [26] эффективно применяется в Великобритании и Канаде для борьбы с детской порнографией. Каждый запрос пользователя сверяется со списком IP-адресов, содержащих запрещенные материалы. Если совпадений нет, то запрос пользователя отсылается напрямую. В противном случае, он перенаправляется на прокси-сервер общественной организации Internet Watch Foundation. Прокси-сервер получает запрашиваемую страницу и анализирует ее. Если страница не содержит запрещенных материалов, то пользователь получает к ней доступ, иначе — создается видимость, что ресурс недоступен. Гибридные варианты фильтрации через HTTP прокси-сервер позволяют при низкой стоимости точно блокировать узкие категории контента. При этом, они столь же легко обходятся, как и фильтрация по IP-адресу.

Фильтрация результатов поиска. В ряде стран, таких как Китай, Франция и Германия, работающие там поисковые системы обязаны исключать из результатов поиска ссылки на запрещенные материалы. Так, во французских и германских версиях Google из поисковых результатов исключаются ссылки на неонацистские группы и другие материалы, запрещенные законом. Таким образом, пользователи не могут найти нежелательный контент. Фильтрация результатов поиска — это еще и один из основных методов борьбы с нарушениями авторских прав в Интернете. Метод обходится использованием других поисковых систем — например, международная версия Google не исключает из результатов сайты неонацистских группировок и при этом доступна из Франции и Германии [25].

Существующие современные контент-фильтры

Все фильтры делятся на две категории:

1. личные, т. е. устанавливаются на компьютер пользователя;

2. виды сервера (маршрутизатора), где сетевой трафик от всех пользователей собирается различными методами и фильтруется.

Каждый из способов имеет свои преимущества и недостатки. При установке фильтра на компьютер пользователя не нужен отдельный сервер для фильтрации, но это преиму-

щество нивелируется необходимостью установки и настройки каждого экземпляра приложения отдельно, а также сложностью сбора статистики по запросам пользователей. При установке фильтра на сервер администратор получает простой и единый способ для настройки и управления фильтрацией. В зависимости от сложности требуемых настроек и количества хостов в сети администратором выбирается оптимальный способ организации фильтрации в образовательных учреждениях. Для небольшого количества хостов в сети и малых знаний администратора данной сети оптимально установить личные контент-фильтры на каждый хост в сети, а для средних и крупных сетей необходимо использовать вариант с выделенным сервером для фильтрации трафика.

Система «NetPolice Pro». Персональный контентный фильтр NetPolice Pro позволяет установить необходимый уровень доступа к ресурсам сети Интернет в школах, обеспечивая эффективную фильтрацию контента по спискам категорий, рекомендованным Минобрнауки России. При использовании NetPolice Pro обеспечивается высокий уровень безопасности за счет реализации в решении двух технологий: фильтрации URL и динамической фильтрации. Фильтр проверяет, к какой категории (запрещенной или разрешенной) относится запрашиваемый сайт, и анализирует содержимое его веб-страниц. Программа NetPolice Pro позволяет редактировать списки слов, которые будут блокироваться непосредственно в поисковых запросах, а также вести «черный» и «белый» списки ресурсов. Фильтр настраивается только по предварительно установленному паролю, и, даже обладая администраторскими правами на компьютере, пользователь не сможет отключить защиту NetPolice Pro. Поддерживается 9 категорий с потенциально опасным содержанием, по 7 категорий для сайтов, несовместимых с задачами образования, и ресурсов с неконтролируемым содержанием и 50 профессиональных категорий [23; 29].

Достоинства:

- не требует отдельного мощного сервера для анализа;
- находится в Едином реестре российских программ для электронных вычислительных машин и баз данных.

Недостатки:

1. фильтрует браузеры и мессенджеры;
2. фильтрация происходит только по протоколу HTTP (отсутствует поддержка HTTPS);
3. предназначен только для операционных систем семейства Windows (хотя есть отдельная версия под некоторые дистрибутивы Linux).

Система «Интернет-цензор». Бесплатный интернет-фильтр для детей под ОС Windows. Программа ставится на личный компьютер пользователя администратором, единого интерфейса настройки нескольких пользователей нет. Фильтрация происходит по принципу «белых списков». База «белых списков» сайтов включает в себя порядка миллиона вручную проверенных сайтов из безопасных сайтов Рунета и основных иностранных ресурсов. Программа защищена от взлома и обхода фильтрации паролем. Основной сайт программы почему-то часто бывает недоступен, однако саму программу можно найти и скачать в сети Интернет [12; 13].

Достоинства:

- бесплатный;
- не требует отдельного мощного сервера для анализа;
- простая установка.

Недостатки:

- анализ трафика основан на списке вручную проверенных сайтов;
- фильтрует браузеры и мессенджеры;
- поддерживается только ОС семейства Windows;
- отсутствует фильтрация по категориям;
- низкое качество фильтрации.

Traffic Inspector для школ. Система от российской компании Smart-Soft — Traffic Inspector — устанавливается на шлюз школы. Программа рассчитана на использование в среде операционных систем Microsoft Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2 x64, Windows Server 2012, Windows Server 2012 R2. Начиная с версии 3.0.1 (2013 год) поддерживается не только 32-х битные системы, но и 64-битные. Traffic Inspector имеет лицензию и сертификат ФСТЭК по 3-му классу защищенности. Поддерживает фильтрацию по URL («черные» и «белые» списки), по категориям. Ведется статистика, учет и расчет (биллинг) трафика пользователей и статистика посещений. Поддерживаются различные виды авторизации пользователя, в том числе интеграция с AD. В дополнение к основному продукту имеются модули расширения для фильтрации рекламы, фишинга, проверка трафика через антивирус, контентная фильтрация. Администрирование программы осуществляется в графическом режиме, через оснастку Microsoft Management Console [24; 28].

Достоинства:

- находится в едином реестре программного обеспечения;
- имеет аппаратное решение;
- ведется статистика запросов;
- имеется множество вариантов аутентификации пользователей.

Недостатки:

- как правило, Windows не слишком хорошо подходит для создания файерволла;
- для настройки требуются знания по администрированию Windows систем.

SquidGuard — открытая (open-source) программа, дополняющая прокси-сервер Squid. В файл с настройками Squid [20] администратор добавляет вызов сторонней программы — редиректора URL. SquidGuard может фильтровать сайты по доменам, по определенному времени суток, IP пользователя или IP цели. Заблокированные страницы логируются. Минусы: отсутствует контентная фильтрация, настройка требует от администратора кроме знаний по настройке Squid также знаний синтаксиса правил по настройке SquidGuard, версия 1.5 2010 года является последней [8].

Достоинства:

1. бесплатная;
2. имеется логирование пользовательских запросов.

Недостатки:

- уже не поддерживается;
- сложная в настройке;
- требует знаний по администрированию прокси-сервера Squid и Linux-систем.

Система фильтрации Selecta

В Уральском государственном педагогическом университете на кафедре информатики, информационных технологий и методики обучения информатике совместно с обществом с ограниченной ответственностью IDECO SELECTA (ООО «Айдеко», г. Екатеринбург) разработана система контентной фильтрации «Selecta» с простым понятным интерфейсом и возможностью индивидуальной политики фильтрации для разных сетей и IP-адресов [19]. Она предназначена для фильтрации интернет-трафика образовательных учреждений с категоризацией интернет-трафика по URL и глубокой фильтрацией по содержимому контента. Программный продукт «Selecta» основан на операционной системе Ubuntu/Debian (Debian-8, дистрибутив Linux), являющийся стабильной платформой для создания программ и предоставляет большое множество системных утилит и систем для инициализации и управления правилами фильтрации пакетов. Средствами разработки проекта являются языки программирования: Node.js, Python 3.5, C/C++, виртуальная машина на платформе Linux: KVM (Kernel-based Virtual Machine), Virtual Box. Общая схема проекта представлена на рис.

Особенности реализации системы:

- система работает на отдельном выделенном сервере;
- весь трафик пользователей проходит через систему контентной фильтрации;
- для настройки параметров фильтрации используется обычный веб-интерфейс (не требуется специального обучения персонала);
- высокоскоростная контентная фильтрация HTTP и HTTPS-трафика;
- DNS и URL-фильтрация;
- морфологический анализ web-страниц;
- фильтрация поисковых запросов.

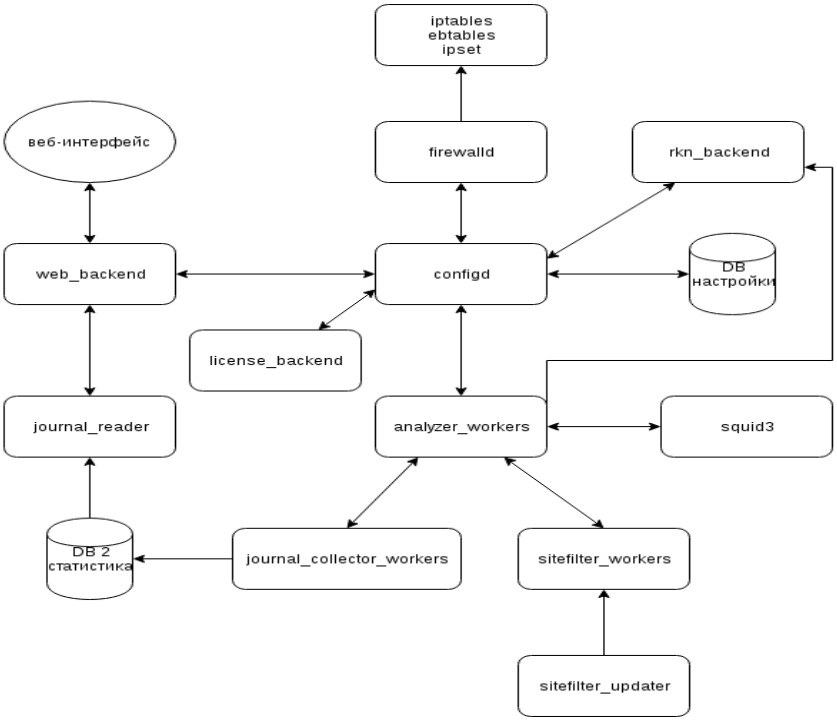

Рис. Общая схема проекта «Selecta»

Разработано руководство по эксплуатации системы «Selecta» для администраторов и методические рекомендации по ее использованию в образовательных учреждениях. Данная система уже внедрена в ряд общеобразовательных школ республики Бурятия.

ЛИТЕРАТУРА

1. Википедия. ARPANET [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/ARPANET (дата обращения: 15.05.2018).
2. Википедия. Всемирная паутина [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Всемирная_паутина (дата обращения: 15.05.2018).
3. Википедия. URI [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/URI (дата обращения: 15.05.2018).
4. Википедия. Интернет в КНДР [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Интернет_в_КНДР (дата обращения: 15.05.2018).
5. Википедия. Кванмён [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Кванмён_(сеть) (дата обращения: 15.05.2018).
6. Википедия. Great Firewall [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/Great_Firewall (дата обращения: 15.05.2018).
7. Википедия. Internet censorship in China [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/Internet_censorship_in_China (дата обращения: 15.05.2018).
8. Википедия. SquidGuard [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/SquidGuard (дата обращения: 22.05.2018).
9. Википедия. Атака посредника [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Атака_посредника SquidGuard (дата обращения: 22.05.2018).
10. Википедия. PIPA [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/PROTECT_IP_Act (дата обращения: 15.05.2018).
11. Википедия. Server_Name_Indication [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Server_Name_Indication (дата обращения: 15.05.2018).
12. Живой Журнал. Интернет Цензор [Электронный ресурс]. — Режим доступа: http://icensor.livejournal.com/ (дата обращения: 22.05.2018).
13. Интернет Цензор — эффективный родительский контроль [Электронный ресурс]. — Режим доступа: https://vellisa.ru/internet-tsenzor (дата обращения: 22.05.2018).
14. Как ограничивают Интернет в разных странах [Электронный ресурс]. — Режим доступа: http://politmix.ru/content/kak-ogranichivayut-internet-v-raznykh-stranakh (дата обращения: 15.05.2018).
15. КонсультантПлюс. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ (последняя редакция) [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 15.05.2018).
16. КонсультантПлюс. Федеральный закон № 139 «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 28.07.12 [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_133282/ (дата обращения: 15.05.2018).
17. КонсультантПлюс. Федеральный закон № 185 от 02.07.2013 [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_148576/ (дата обращения: 15.05.2018).
18. КонсультантПлюс. Федеральный закона № 307 от 14.10.2014 [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_169745/ (дата обращения: 15.05.2018).
19. ООО «Айдеко» [Электронный ресурс]. — Режим доступа: http://www.ideco.ru.
20. Официальный сайт Squid [Электронный ресурс]. — Режим доступа: http://www.squid-cache.org/ (дата обращения: 22.05.2018).
21. «Прозрачный» Squid с фильтрацией HTTPS ресурсов без подмены сертификатов (x86) [Электронный ресурс]. — Режим доступа: https://habrahabr.ru/post/267851/ / (дата обращения: 22.05.2018).
22. Российская Газета. Федеральный закон от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации [Электронный ресурс]. — Режим доступа: https://rg.ru/2006/07/29/informacia-dok.html (дата обращения: 22.05.2018).
23. Сайт NetPolice Pro [Электронный ресурс]. — Режим доступа: http://www.netpolice.ru/ (дата обращения: 22.05.2018).
24. Сайт Traffic Inspector [Электронный ресурс]. — Режим доступа: http://www.smart-soft.ru/products/traffic-inspector/ (дата обращения: 22.05.2018).
25. Средства и методы фильтрации контента в интернете [Электронный ресурс]. — Режим доступа: https://sites.google.com/site/metodyblokirovkinezelanojinfor/sredstva-i-metody-filtracii-kontenta-v-internete / (дата обращения: 22.05.2018).
26. Cleanfeed [Электронный ресурс]. — Режим доступа: https://www.cybertip.ca/app/en/projects-cleanfeed (дата обращения: 22.05.2018).
27. FAQ по Gopher [Электронный ресурс]. — Режим доступа: https://gopherproxy.meulie.net/gopher.viste-family.net/0/gopher-faq/gopher-faq-2009-02-07.txt (дата обращения: 15.05.2018).
28. Habrahabr. Что такое Traffic Inspector и с чем его едят [Электронный ресурс]. — Режим доступа: https://habrahabr.ru/company/smart_soft/blog/225427/ (дата обращения: 22.05.2018).
29. NetPolice Pro [Электронный ресурс]. — Режим доступа: http://www.netpolice.ru/collection/dlya-ofisa/product/netpolice-pro-litsenziya-na-1-god (дата обращения: 22.05.2018).

R E F E R E N C E S

1. Vikipediya. ARPANET [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/ARPANET (data obrashcheniya: 15.05.2018).
2. Vikipediya. Vsemirnaya pautina [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/Vsemirnaya_pautina (data obrashcheniya: 15.05.2018).
3. Vikipediya. URI [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/URI (data obrashcheniya: 15.05.2018).
4. Vikipediya. Internet v KNDR [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/Internet_v_KNDR (data obrashcheniya: 15.05.2018).
5. Vikipediya. Kvanmen [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/Kvanmen_(set') (data obrashcheniya: 15.05.2018).
6. Vikipediya. Great Firewall [Elektronnyy resurs]. — Rezhim dostupa: https://en.wikipedia.org/wiki/Great_Firewall (data obrashcheniya: 15.05.2018).
7. Vikipediya. Internet censorship in China [Elektronnyy resurs]. — Rezhim dostupa: https://en.wikipedia.org/wiki/Internet_censorship_in_China (data obrashcheniya: 15.05.2018).
8. Vikipediya. SquidGuard [Elektronnyy resurs]. — Rezhim dostupa: https://en.wikipedia.org/wiki/SquidGuard (data obrashcheniya: 22.05.2018).
9. Vikipediya. Ataka posrednika [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/Ataka_posrednika SquidGuard (data obrashcheniya: 22.05.2018).
10. Vikipediya. PIPA [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/PROTECT_IP_Act (data obrashcheniya: 15.05.2018).
11. Vikipediya. Server_Name_Indication [Elektronnyy resurs]. — Rezhim dostupa: https://ru.wikipedia.org/wiki/Server_Name_Indication (data obrashcheniya: 15.05.2018).
12. Zhivoy Zhurnal. Internet Tsenzor [Elektronnyy resurs]. — Rezhim dostupa: http://icensor.livejournal.com/ (data obrashcheniya: 22.05.2018).
13. Internet Tsenzor — effektivnyy roditel'skiy kontrol' [Elektronnyy resurs]. — Rezhim dostupa: https://vellisa.ru/internet-tsenzor (data obrashcheniya: 22.05.2018).
14. Kak ogranichivayut Internet v raznykh stranakh [Elektronnyy resurs]. — Rezhim dostupa: http://politmix.ru/content/kak-ogranichivayut-internet-v-raznykh-stranakh (data obrashcheniya: 15.05.2018).
15. Konsul'tantPlyus. Federal'nyy zakon «O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorov'yu i razvitiyu» ot 29.12.2010 № 436-FZ (poslednyaya redaktsiya) [Elektronnyy resurs]. — Rezhim dostupa: http://www.consultant.ru/document/cons_doc_LAW_108808/ (data obrashcheniya: 15.05.2018).
16. Konsul'tantPlyus. Federal'nyy zakon № 139 «O vnesenii izmeneniy v federal'nyy zakon «O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorov'yu i razvitiyu» ot 28.07.12 [Elektronnyy resurs]. — Rezhim dostupa: http://www.consultant.ru/document/cons_doc_LAW_133282/ (data obrashcheniya: 15.05.2018).
17. Konsul'tantPlyus. Federal'nyy zakon № 185 ot 02.07.2013 [Elektronnyy resurs]. — Rezhim dostupa: http://www.consultant.ru/document/cons_doc_LAW_148576/ (data obrashcheniya: 15.05.2018).
18. Konsul'tantPlyus. Federal'nyy zakona № 307 ot 14.10.2014 [Elektronnyy resurs]. — Rezhim dostupa: http://www.consultant.ru/document/cons_doc_LAW_169745/ (data obrashcheniya: 15.05.2018).
19. OOO «Aydeko» [Elektronnyy resurs]. — Rezhim dostupa: http://www.ideco.ru.
20. Ofitsial'nyy sayt Squid [Elektronnyy resurs]. — Rezhim dostupa: http://www.squid-cache.org/ (data obrashcheniya: 22.05.2018).
21. «Prozrachnyy» Squid s fil'tratsiey HTTPS resursov bez podmeny sertifikatov (x86) [Elektronnyy resurs]. — Rezhim dostupa: https://habrahabr.ru/post/267851/ / (data obrashcheniya: 22.05.2018).
22. Rossiyskaya Gazeta. Federal'nyy zakon ot 27 iyulya 2006 g. № 149-FZ Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii [Elektronnyy resurs]. — Rezhim dostupa: https://rg.ru/2006/07/29/informacia-dok.html (data obrashcheniya: 22.05.2018).
23. Sayt NetPolice Pro [Elektronnyy resurs]. — Rezhim dostupa: http://www.netpolice.ru/ (data obrashcheniya: 22.05.2018).
24. Sayt Traffic Inspector [Elektronnyy resurs]. — Rezhim dostupa: http://www.smart-soft.ru/products/traffic-inspector/ (data obrashcheniya: 22.05.2018).
25. Sredstva i metody fil'tratsii kontenta v internete [Elektronnyy resurs]. — Rezhim dostupa: https://sites.google.com/site/metodyblokirovkinezelanojinfor/sredstva-i-metody-filtracii-kontenta-v-internete / (data obrashcheniya: 22.05.2018).
26. Cleanfeed [Elektronnyy resurs]. — Rezhim dostupa: https://www.cybertip.ca/app/en/projects-cleanfeed (data obrashcheniya: 22.05.2018).
27. FAQ po Gopher [Elektronnyy resurs]. — Rezhim dostupa: https://gopherproxy.meulie.net/gopher.viste-family.net/0/gopher-faq/gopher-faq-2009-02-07.txt (data obrashcheniya: 15.05.2018).
28. Habrahabr. Chto takoe Traffic Inspector i s chem ego edyat [Elektronnyy resurs]. — Rezhim dostupa: https://habrahabr.ru/company/smart_soft/blog/225427/ (data obrashcheniya: 22.05.2018).
29. NetPolice Pro [Elektronnyy resurs]. — Rezhim dostupa: http://www.netpolice.ru/collection/dlya-ofisa/product/netpolice-pro-litsenziya-na-1-god (data obrashcheniya: 22.05.2018).