

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Демин В. Экономический шпионаж на пороге XXI века // БДИ. – 1996. – № 5.
2. Ярочкин В.И. Технические каналы утечки информации. – М., 1994. – С. 23-55.
3. Доронин А.И. Бизнес-разведка. – М.: Ось-89, 2002. – С. 33-126.
4. Ромачев Н.Р. Нежданов И.Ю. Конкурентная разведка. Москва Ось-89. – С. 88-141.
5. Ронин Р. Своя разведка способы вербовки агентуры, методы проникновения в психику, форсированное воздействие на личность, технические средства скрытого наблюдения и съема информации. – Минск: Харвест 1998. – С. 45-89.
6. Лемке Г.Э. Конкурентная война нелинейные методы и стратагемы. – М.: Ось-89.
7. Бабец О. Опыт военной разведки на службе в коммерческой фирме. – Минск: Харвест, 2004. – С. 67-87.

**Поздняков Владимир Александрович**

Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.

E-mail: v.pozdnyakov61@mail.ru.

347922, г. Таганрог, ул. Чехова, 2.

Тел.: 88634312016.

**Pozdnyakov Vladimir Alexandrovich**

Taganrog Institute of Technology – Federal State-Owned Educational Autonomy Establishment of Higher Vocational Education “Southern Federal University”.

E-mail: v.pozdnyakov61@mail.ru.

2, Chehova street, Taganrog, 347922, Russia.

Phone: +78634312016.

УДК 004.239.056

**А.Ф. Чипига, В.С. Пелешенко, А.С. Бабанин**

**ПОДХОД К КОНТРОЛЮ РАБОТЫ В СЕТИ ИНТЕРНЕТ С ПОМОЩЬЮ  
ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА ДЛЯ ЗАЩИТЫ ДЕТЕЙ ОТ  
ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ**

*Показан подход к анализу и фильтрации трафика из сети Интернет с помощью технологий контентной фильтрации для защиты детей от информации, причиняющей вред их здоровью и развитию.*

*Защита детей от негативной информации; контентная фильтрация.*

**A.F. Chipiga, V.S. Peleshenko, A.S. Babanin**

**APPROACH TO CONTROL OF THE INTERNET BY NETWORK TRAFFIC  
FILTERING TO PROTECT CHILDREN FROM INFORMATION DAMAGING  
THEIR HEALTH AND DEVELOPMENT**

*Shows the approach to analyze and filter traffic from the Internet with content filtering technologies to protect children from information damaging to their health and development.*

*Protecting children from negative information; content filtering.*

**Постановка задачи.** Самой активной категорией пользователей сети Интернет являются дети, которые быстрее всех учатся пользоваться современными технологиями. Настоящий период характеризуется увеличившимся количеством информационных атак на информационные системы и людей, поэтому актуальной задачей является создание подхода к обнаружению и предотвращению деструк-

тивного воздействия негативной информации и создание средств для защиты детей, работающих в Интернете дома и в учебных заведениях в российском сегменте глобальной сети.

**Решение задачи.** При использовании современных компьютерных технологий несанкционированный доступ к информации становится возможным после удачного осуществления компьютерных сетевых атак [1].

Предлагается использовать известную методологию обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей для контроля работы не только людей разных возрастных категорий, но и детей школьного возраста и студентов в сети Интернет. Для этого необходимо применение системы контентной фильтрации (рис. 1), которая представляет собой программу (агент пользователя), устанавливаемую на персональный компьютер пользователя (или программный маршрутизатор) и центральный сервер, хранящий списки запрещенных URL- и IP-адресов. Агент пользователя, анализируя трафик, осуществляет соединение с центральным сервером для проверки легитимности веб-ресурса, к которому обращается пользователь. Если ресурс является запрещенным, то пользователю в браузер выводится соответствующее сообщение. Механизм проверки ресурсов является полуавтоматическим: если адрес ресурса не содержится в списке запрещенных, производится его контентный анализ агентом пользователя, либо центральным сервером. Ручной анализ выполняется группой специалистов в случае, если контентный анализатор пользователя присвоил флаг «подозрительно». Необходимо предусмотреть также повторные проверки в зависимости от частоты изменения информации на веб-ресурсе. Группой специалистов, помимо разработчиков системы, могут стать ее пользователи или заинтересованные лица. Кроме того, предусмотрено категорирование ресурсов.



Рис. 1. Система контентной фильтрации Интернет-ресурса

Каждому пользователю или группе пользователей предоставляется веб-интерфейс, обладающий следующими возможностями:

- ◆ просмотр посещенных и заблокированных ресурсов;
- ◆ выбор категорий веб-ресурсов, требующих блокирования;
- ◆ собственные белые и черные списки ресурсов, а также правила блокирования.

При контроле работы в сети Интернет с помощью фильтрации сетевого трафика предложено использовать известную технологию автономной и встраиваемой фильтрации с помощью агентов пользователя и центрального сервера.

При такой фильтрации предлагается использовать категоризацию ресурсов, включающую в себя различные методы и их модификации [2]:

- ◆ статистический (подсчет весовых коэффициентов и выбор частотных ключевых слов);
- ◆ вероятностный (на основе теоремы Байеса);
- ◆ векторный (когда текст представляется в виде вектора признаков);
- ◆ лингвистический (лексические портреты документов);
- ◆ скрытое семантическое индексирование (latent semantic indexing);
- ◆ алгоритмы с использованием нейросетей и др.

При использовании категоризации можно рассматривать шаблоны цифровых отпечатков документов-шаблонов, содержащих необходимую информацию для поиска фильтром и при достижении определенного порога схожести ресурсу присваивается категория, к которой относится документ-шаблон.

Для практической реализации, в рамках региона, контентной фильтрации на основе URL, семантического анализа содержимого Web-страниц, анализ графического содержимого страниц; формирование белых, серых и черных списков URL предложено использовать схему контент-фильтрации с учетом увеличения нагрузки на сервер обработки сетевого трафика, вводом балансировки нагрузки и собственных зеркал ресурсов, в разрезе общей схемы вычислительной сети учреждений, показанную на рис. 2.

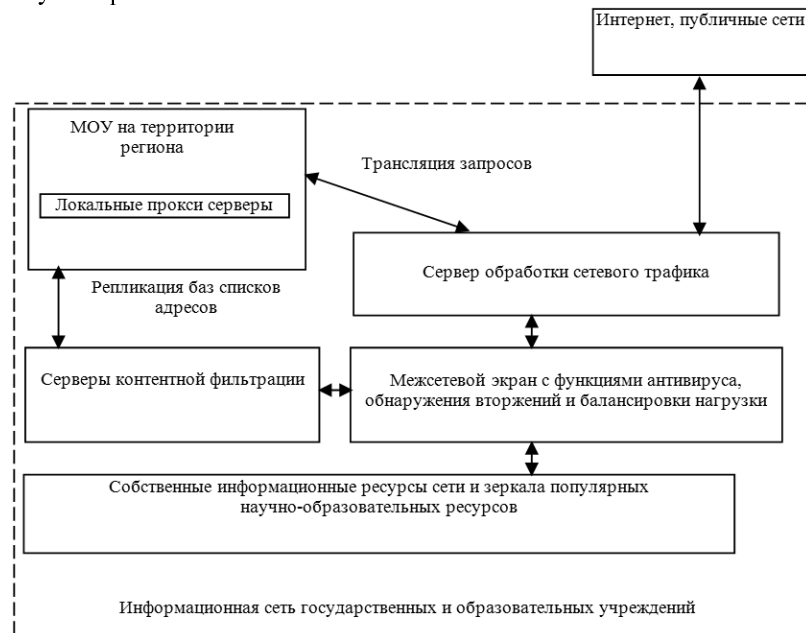


Рис. 2. Схема контент-фильтрации в рамках региона

В основе подхода к контролю работы в сети Интернет с помощью фильтрации сетевого трафика лежит использование дополненной методологии обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей.

В основе методологии лежит использование идентификации пользователей Интернет с помощью известных алгоритмов и алгоритма определения принадлежности пользователя к определенному географическому положению и возрастной категории.

Определение принадлежности пользователя определяется двумя способами. Первый способ заключается в том, что определенному сетевому адресу присваивается идентификатор пользователя (ИП), соответствующий возрастной категории. Второй способ заключается в подписи сетевых пакетов (ПСП) электронной подписью, выдаваемой при регистрации подключения к Интернет, соответствующей, в случае необходимости, географическому положению и возрастной категории пользователя.

Общая, в рамках страны, схема системы фильтрации сетевого трафика, учитывающая вышеописанные способы, представлена на рис. 3.

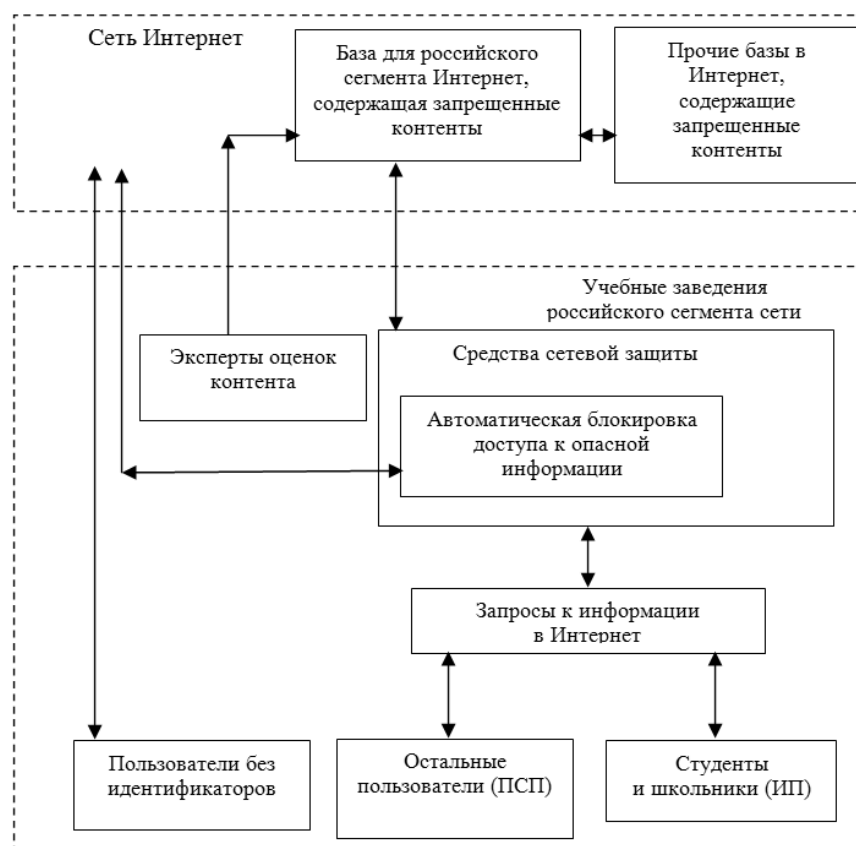


Рис. 3. Система контентной фильтрации сетевого трафика

На рис. 3 к пользователям без идентификаторов относятся сотрудники учебных заведений, работающие в режиме онлайн, не относящиеся к экспертам оценок контента.

Задача системы автоматической блокировки доступа к опасной информации сводится к классификации и блокировке информации тематических категорий, приведенных в наиболее полном виде в табл. 1 [3].

Таблица 1

Тематические категории блокируемой информации

№ п/п	Тематическая категория
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения
2	Злоупотребление свободой СМИ — экстремизм
3	Злоупотребление свободой СМИ — наркотические средства
4	Злоупотребление свободой СМИ — информация с ограниченным доступом
5	Злоупотребление свободой СМИ — скрытое воздействие
6	Экстремистские материалы или экстремистская деятельность (экстремизм)
7	Вредоносные программы
8	Преступления
9	Ненадлежащая реклама
10	Информация с ограниченным доступом
11	Алкоголь
12	Баннеры и рекламные программы
13	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)
14	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)
15	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)
16	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)
17	Корпоративные сайты, интернет-представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)
18	Личная и немодерируемая информация
19	Отправка SMS с использованием интернет-ресурсов
20	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)
21	Нелегальная помощь школьникам и студентам
22	Неприличный и грубый юмор
23	Нижнее белье, купальники
24	Обеспечение анонимности пользователя, обход контентных фильтров
25	Онлайн-казино и тотализаторы
26	Платные сайты
27	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)
28	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)
29	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)
30	Системы поиска изображений

Окончание табл. 1

31	СМИ (ресурсы данной категории, не имеющие отношения к образовательному процессу)
32	Табак, реклама табака, пропаганда потребления табака
33	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)
34	Убийства, насилие
35	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)

Каждой тематической категории соответствует содержание, приведенное в табл. 2.

Таблица 2

## Содержание блокируемых тематических категорий

№ п/п	Содержание
1	Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
2	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	а) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистической рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы; б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: – насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; – подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований;

Продолжение табл. 2

	<ul style="list-style-type: none"> <li>– осуществление террористической деятельности либо публичное оправдание терроризма;</li> <li>– возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию;</li> <li>– унижение национального достоинства;</li> <li>– осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы;</li> <li>– пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;</li> <li>– воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения;</li> <li>– публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;</li> <li>– применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей;</li> <li>– посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность;</li> <li>– нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением</li> </ul>
7	<p>Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети</p>
8	<p>Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию);  Оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме)  Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма  Склонение к потреблению наркотических средств и психотропных веществ.  Незаконное распространение или рекламирование порнографических материалов  Публичные призывы к осуществлению экстремистской деятельности  Информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства  Публичные призывы к развязыванию агрессивной войны</p>

Продолжение табл. 2

9	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну
11	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
12	Баннерные сети, всплывающая реклама, рекламные программы
13	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
14	Не имеющая отношения к образовательному процессу информация: <ul style="list-style-type: none"> <li>– фотоальбомы и фотоконкурсы;</li> <li>– рейтинги открыток, гороскопов, сонников;</li> <li>– гадания, магия и астрология;</li> <li>– ТВ-программы;</li> <li>– прогнозы погоды;</li> <li>– тесты, конкурсы онлайн;</li> <li>– туризм, путешествия;</li> <li>– тосты, поздравления;</li> <li>– кроссворды, сканворды, ответы к ним;</li> <li>– фантастика;</li> <li>– кулинария, рецепты, диеты;</li> <li>– мода, одежда, обувь, модные аксессуары, показы мод;</li> <li>– тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.;</li> <li>– о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними;</li> <li>– о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании;</li> <li>– о службах знакомств, размещении объявлений онлайн;</li> <li>– анекдоты, «приколы», слухи;</li> <li>– о сайтах и журналах для женщин и для мужчин;</li> <li>– желтая пресса, онлайн-ТВ, онлайн-радио;</li> <li>– о знаменитостях;</li> <li>– о косметике, парфюмерии, прическах, ювелирных украшениях.</li> </ul>
15	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
16	Не имеющие отношения к образовательному процессу компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
17	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
18	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги



Окончание табл. 2

19	Сайты, предлагающие услуги по отправке SMS-сообщений
20	Содержащие информацию, не имеющую отношения к образовательному процессу, модерлируемые доски сообщений/объявлений, а также модерлируемые чаты
21	Банки готовых рефератов, эссе, дипломных работ и пр.
22	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
23	Сайты, на которых рекламируется и изображается нижнее белье и купальники
24	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
25	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
26	Сайты, на которых вывешено объявление о платности посещения веб-страниц
27	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
28	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете
29	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности
30	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
31	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу
32	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
33	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
34	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
35	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.

**Анализ полученных результатов.** При использовании предложенного подхода к контролю работы в сети Интернет с помощью фильтрации сетевого трафика становится возможным защитить детей от информации, причиняющей вред их здоровью и развитию в учебных заведениях, дома и в других местах, имеющих выход в Интернет, в которых есть необходимость контроля Интернет-контента.

**Выводы.** Применение предлагаемой системы контентной фильтрации позволит повысить уровень защиты как информационных систем в целом, так и людей от информации, причиняющей вред их здоровью и развитию.

#### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Чипига А.Ф.* Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Материалы XI Международной научно-практической конференции «Информационная безопасность», – Ч.2. – Таганрог: Изд-во ТТИ ЮФУ, 2010.
2. *Ефременко Н.* «Онтологии в DLP-системах третьего поколения» [www.itsec.ru/articles2/Oborandteh/ontologii-v-dlp-sistemah-tretyego-pokolenia](http://www.itsec.ru/articles2/Oborandteh/ontologii-v-dlp-sistemah-tretyego-pokolenia).
3. «Система классификации информации, не имеющей отношения к образовательному процессу», Приложение № 7 к приказу по МОУ «Сосновская ООШ» Моргаушского района от 8 декабря 2008 № 111. [www.21411s24.edusite.ru/DswMedia/prilozhenie7\\_sistemaklassifikaciiinformacii.doc](http://www.21411s24.edusite.ru/DswMedia/prilozhenie7_sistemaklassifikaciiinformacii.doc).

**Чипига Александр Федорович**

Северо-Кавказский государственный технический университет.

E-mail: zik@ncstu.ru.

355003, г. Ставрополь, ул. Морозова, 105, кв. 15.

Тел.: 89624441070.

**Пелешенко Виктор Сергеевич**

E-mail: zik@ncstu.ru.

355029, г. Ставрополь, проспект Кулакова, 2.

Тел.: +79188657032.

**Бабанин Андрей Сергеевич**

E-mail: zik@ncstu.ru.

355044, г. Ставрополь, ул. Васильева, 17, кв. 108.

Тел.: +79187470178.

**Chipiga Alexander Fedorovich**

North Caucasus State Technical University.

E-mail: zik@ncstu.ru.

App. 15, 105, Morozova street, Stavropol, 355003, Russia.

Phone: +79624 441070.

**Peleshenko Viktor Sergeevich**

E-mail: zik@ncstu.ru.

2, Kulakova avenue, Stavropol, 355029, Russia.

Phone: +79188657032.

**Babanin Andrey Sergeevich**

E-mail: zik@ncstu.ru.

App. 108, 17, Vasileva street, Stavropol, 355044, Russia.

Phone: +79187470178.