УДК 004.777
DOI 10.25205/1818-7900-2021-19-1-48-60

Разработка монитора безопасности от деструктивных влияний веб-сайтов и социальных сетей Интернета

А. А. Зеленский, А. И. Григорян, Л. В. Черкесова, Е. А. Ревякина

Донской государственный технический университет
Ростов-на-Дону, Россия

Аннотация

Рассмотрены основные возрастные особенности использования сети «Интернет» детьми и подростками. Всё большее распространение получает подключение к сети по высокоскоростным каналам, что позволяет им проводить в Интернете почти всё свое свободное время. Остро встает проблема обеспечения их безопасности в веб-пространстве. Для этого разработан монитор безопасности, обладающий множеством функций, позволяющих использовать Интернет безопаснее и под контролем родителей. Программное обеспечение написано на языках веб-программирования JavaScript и PHP, что позволяет использовать его практически на всех современных браузерах. Представлены скриншоты функционирования ПО и блок-схема работы монитора безопасности с подробным описанием функций. Приведены сравнения с аналогами и показаны преимущества разработанного ПО в сравнении с ними.

Ключевые слова

деструктивный сайт, кибербуллинг, деструктивный текстовый контент, информационная защищенность детей и подростков, веб-программирование, браузер

Для цитирования

Зеленский А. А., Григорян А. И., Черкесова Л. В., Ревякина Е. А. Разработка монитора безопасности от деструктивных влияний веб-сайтов и социальных сетей Интернета // Вестник НГУ. Серия: Информационные технологии. 2021. Т. 19, № 1. С. 48–60. DOI 10.25205/1818-7900-2021-19-1-48-60

Development of Safety Monitor from Destructive Influences of Web-Sites and Social Networks of Internet

A. A. Zelensky, A. I. Grigoryan, L. V. Cherkesova, E. A. Revyakina

Don State Technical University
Rostov on Don, Russian Federation

Abstract

This article discusses the main age-related features of the Internet use by adolescents and children. Today more and more computers are connected to the Internet. At the same time, connection via high-speed channels is becoming more common, both at work and at home. More and more children get the opportunity to work on the Internet. But at the same time, the problem of ensuring the safety of children on the Internet is becoming more acute. For this, a security monitor was developed, which has many functions that allow you to use the Internet more safely and under parental control. This security monitor is written in the web programming language JavaScript and PHP, which will allow using the system on almost all modern browsers and on any computer. The article also provides screenshots of the program's operation and a flowchart with a detailed description.

Keywords

destructive site, cyberbulling, destructive text content, information security of children and teenagers, web-programming, browser

For citation

Zelensky A. A., Grigoryan A. I., Cherkesova L. V., Revyakina E. A. Development of Safety Monitor from Destructive Influences of Web-Sites and Social Networks of Internet. *Vestnik NSU. Series: Information Technologies*, 2021, vol. 19, no. 1, p. 48–60. (in Russ.) DOI 10.25205/1818-7900-2021-19-1-48-60

Введение

Информационные технологии стремительно внедряются в нашу жизнь. На сегодняшний день Интернет является неотъемлемой частью жизни любого взрослого человека. Мы используем компьютеры на работе, дома, на отдыхе и даже во время поездок на транспорте. В наше время компьютеры стали чаще использоваться в быту, чем в офисных помещениях. Эта тенденция приобретает мировой характер, и Россия не является исключением. Возрастной диапазон пользователей Интернета расширяется, а доля молодых и совсем юных пользователей среди них очень велика. Всё большее количество детей уже в раннем возрасте начинают осваивать Интернет, легко ориентируясь на различных сайтах и в приложениях. Родители не всегда имеют возможность проконтролировать действия своих детей, которые уже с дошкольного возраста проявляют интерес к компьютерным технологиям. В связи с этим возникла проблема обеспечения информационной безопасности детей и несовершеннолетних подростков, получивших доступ к безграничному количеству информации, которая долгое время поступала в сеть без надлежащего контроля.

Информационная безопасность подрастающего поколения – состояние защищенности детей и подростков, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [1].

Дети быстро становятся подростками и с раннего возраста связаны с Интернетом. Это сказывается на их социализации, так как виртуальный мир и реальность для них сливаются воедино [1]. Если раньше формирование личности подростка происходило за счет сопричастности к субкультурным сообществам, то сейчас социализация происходит в различных социальных сетях, играх, блогах и т. д. (рис. 1). Опасностью этого процесса является то, что несовершеннолетние не могут четко разделять реальный и виртуальный мир. Зачастую действия в «онлайне» проецируются на окружающий мир «офлайн» реальной жизни.

Можно выделить несколько групп угроз для детей и подростков в Интернете:

- небезопасные знакомства;
- кибербуллинг (кибертрроллинг, травля человека) (рис. 2);
- деструктивные веб-сайты;
- противоправный контент;
- интернет-зависимость.

Каждой группе угроз соответствует определенная целевая аудитория. Так, подростки, юноши и девушки в возрасте 13–14 лет больше подвержены кибербуллингу или сексуальным домогательствам. Дети младшего возраста чаще сталкиваются с различным противоправным контентом, если родители не обеспечивают безопасный доступ в Интернет.

Подобные воздействия сильно влияют на психику детей и подростков, невольно вызывая негативные эмоции и агрессию в сторону сверстников, учителей, родственников и других людей.

[1] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 31.07.2020) «О защите детей от информации, причиняющей вред их здоровью и развитию».

Рис. 1. Статистика использования Интернета детьми и подростками
Fig. 1. Statistics on Internet use by children and adolescents

Рис. 2. Последствия кибербуллинга
Fig. 2. The consequences of cyberbullying

Исходя из опасностей можно выделить следующие риски онлайн-среды. Они разделяются на четыре типа: контентные, коммуникационные, электронные и потребительские.

Контентные риски – это различные материалы (тексты, картинки, аудио- и видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. Столкнуться с ними можно практически везде: социальные сети, блоги, торренты, персональные сайты, видеохостинги и др.

Коммуникационные риски связаны с общением и межличностными отношениями интернет-пользователей. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, груминг), знакомства в сети, встречи с опасными интернет-знакомыми и др.

Электронные риски – это вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ. Вредоносные программы представляют собой различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации.

Потребительские риски – это злоупотребление в Интернете правами потребителя. Они включают в себя риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию, потерю денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества и др.

В наших силах разработать интеллектуальные информационные системы – мониторинги безопасности, которые смогут контролировать деструктивный контент, выкладываемый в сеть.

Разработка программного обеспечения

Обеспечение безопасности детей и подростков является задачей повышенной актуальности. Для ее решения необходимо разработать специальное программное обеспечение, а именно монитор безопасности, позволяющий просматривать, анализировать и блокировать деструктивный веб-сайт с вредоносным контентом еще до его загрузки на компьютер юного пользователя, а также помогающий родителям контролировать увлечения своих детей.

Задачу анализа текста на веб-сайтах рассматривали многие российские и зарубежные авторы, среди которых V. B. Barakhnin, R. I. Mukhamedyev (в работе «Methods to identify the destructive information») [2], И. Е. Воронина, В. А. Гончаров (в работе «Анализ эмоциональной окраски сообщений в социальных сетях (на примере сети «В_Контакте») [3], V. A. Gostyunina, N. V. Davidyuk (в работе «The combined method of textual information analysis for the content of destructive indicators») [4], Д. Р. Байдулова, В. А. Гостюнина, Н. В. Давидюк (в работе «Применение машинного обучения в процессе поиска деструктивной информации в web-контенте») [5], А. А. Браницкий, Е. В. Дойникова, И. В. Котенко (в работе «Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям») [6] и мн. др.

Целью исследования является разработка программного обеспечения – монитора безопасности, предназначенного для родителей детей и несовершеннолетних подростков, способного защитить юных пользователей от деструктивного влияния веб-сайтов с вредоносным контентом, представляющих угрозу их психологической защищенности.

Объектом исследования являются интернет-ресурсы, содержащие деструктивный текстовый контент, угрожающий психологической безопасности детей и несовершеннолетних подростков.

Предметом исследования являются алгоритмы анализа текстового контента веб-сайтов и методы блокирования таких сайтов до загрузки на компьютер юного пользователя.

Подобные программы в мире существуют. Среди них нужно прежде всего назвать программные продукты: KinderGate, KidShell, Kaspersky и др. (рис. 3). Рассмотрим возможные аналоги.

KinderGate. Продукт KinderGate («Родительский контроль») – это фильтр, позволяющий осуществлять многостороннюю политику использования Интернета несовершеннолетними детьми. Для этого он имеет несколько различных инструментов. Главным из них является возможность блокировать сайты по заданной теме. Принцип работы системы фильтрации таков: когда ребенок пытается получить доступ к какому-либо веб-сайту, система запрашивает базу данных с его адресом и получает в ответ категорию, к которой он принадлежит. Если эта категория классифицируется родителями как запрещенная тема, то доступ к сайту будет заблокирован, а вместо него появится страница с предупреждением. В противном случае проект будет открыт в браузере.

	Цена	Разработчик	Интерфейс на русском языке	Возраст детей	Платформа	Режим скрытой работы
Kids Place	Бесплатная/платная	Зарубежный	-	5-7	Android	-
Mspy	платная	Зарубежный	-	5-17	Windows	-
SafeKiddo	платная	Зарубежный	-	5-17	Windows, Apple, Android	-
KidLogger	Бесплатная/платная	Зарубежный	+	5-17	Android	+
KidShell	Бесплатная/платная	Зарубежный	+	5-7	Android	-
PlayPad	Бесплатная/платная	Зарубежный	+	5-7	Android	-
KinderGate	платная	Зарубежный	+	5-17	Windows	-
Norton Family	платная	Зарубежный	+	5-17	Windows, Apple, Android	+
Kaspersky	Бесплатная/платная	Россия	+	5-17	Windows, Apple, Android	+
ParentalWatch	**Бесплатная**	**Россия**	+	5-17	Windows, Apple, Android	+

Рис. 3. Существующие аналоги разработанного ПО
Fig. 3. Existing analogues of the developed software

KidShell. Эта программа отличается от предыдущей. Это «песочница» для детей на мобильном устройстве родителей – особая зона, специально предназначенная для безопасного использования программных продуктов. Учетная запись ребенка на родительском телефоне настроена на запуск только разрешенных родителями приложений. Без настроенного доступа ребенок не может звонить, писать SMS, покупать или запускать приложение.

Kaspersky. Родительский контроль данного производителя предоставляется только в рамках других продуктов, например Kaspersky Total Security 2016. Возможности контроля широки: можно ограничить время пребывания ребенка в Интернете, создать список нежелательных сайтов (по всему названию сайта или по его части, по теме, связанной с эротикой, жестокостью, смертью, оружием, убийствами и т. д.). Усилить контроль можно с помощью «белого списка» веб-сайтов. В этом случае ребенок сможет заходить только на те сайты, которые находятся в разрешенном списке.

Хороший подход к фильтрации контента продемонстрирован в работе «Подход к фильтрации запрещенного контента в веб-пространстве» [7], в ней фильтрация контента происходит с помощью:

- лингвистического анализа контента;
- тематической классификации веб-текстов;
- жанровой классификации веб-текстов;
- уточняющей классификации.

Разработанный авторами этой статьи монитор безопасности имеет следующие принципы (рис. 4):

- выполняется мониторинг и анализ текста сайта на наличие деструктивных фраз и слов путем предварительной загрузки сайта (скрытно от юного пользователя);
- происходит автоматическое внесение обнаруженного веб-сайта в базу деструктивных сайтов;
- формируется список деструктивных фраз и слов, который постоянно пополняется;
- разработанный монитор безопасности является импортозамещающим, абсолютно бесплатным, и рассчитан на российского пользователя с любым уровнем компьютерной грамотности.

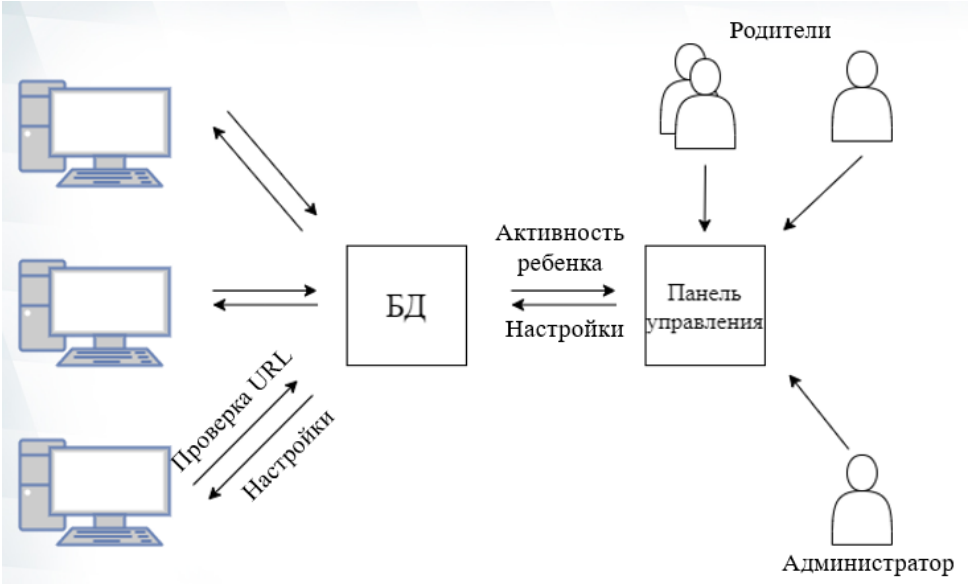

Рис. 4. Принцип работы ПО, разработанного авторами данной статьи
Fig. 4. Principle of the software developed by authors of this paper

Элементы программы: расширение браузера; сервер; личный кабинет родителя.

В рамках выбранной архитектуры программного обеспечения процедура блокирования сайта с небезопасным контентом выглядит следующим образом: при открытии несовершеннолетним ребенком или подростком любого сайта расширение браузера внедряется в процесс загрузки страницы, оно растягивает загрузку сайта на время его проверки, т. е. визуально останавливает загрузку страницы и загружает ее в фоновом режиме. Программа проверяет веб-сайт на наличие опасного контента, затем либо удаляет контент и выводит на экран сообщение об ошибке, либо открывает саму веб-страницу, но при этом отправляет информацию на сервер и в личный кабинет родителя. Родители, в свою очередь, могут выбирать статус просмотренного контента и блокировать его.

Браузерное расширение реализуется с помощью языка программирования Java Script и имеет свой принцип (рис. 5) и алгоритм работы (рис. 6). Работа расширения происходит в несколько этапов. На первоначальном этапе, до загрузки контента, включается код, который покрывает всю страницу белым слоем, чтобы растянуть загрузку страницы на время ее проверки. На следующем этапе происходит исследование загруженного, но еще не выведенного на экран контента. Далее, если проверка веб-сайта была пройдена, то белый слой снимается и открывается уже загруженная страница. В противном случае контент удаляется, и вместо него на экране появляется ошибка сети.

Для ускорения работы расширения, сервер ежедневно формирует список запрещенных выражений, слов и фраз, чтобы не делать выборку постоянно. Кеш записи разбит по видам угроз, например: фразы, связанные с эротикой, порнографией, педофилией, убийствами, суицидом и т. д. Для расчета рейтинга сайта и для измерения степени его деструктивности используется следующая формула:

$$q_i = \sum_{j=0..s_i} \frac{1}{s_i} * t_{ij},$$

где

q_i – рейтинг i сайта от 0 до 1;

i – порядковый номер сайта в системе;

j – порядковый номер посетителя;
s_i – число уникальных посетителей сайта;
t_{ij} – коэффициент вредоносности [0,0.5,1].

Рис. 5. Принцип работы браузерного расширения
Fig. 5. How the browser extension works

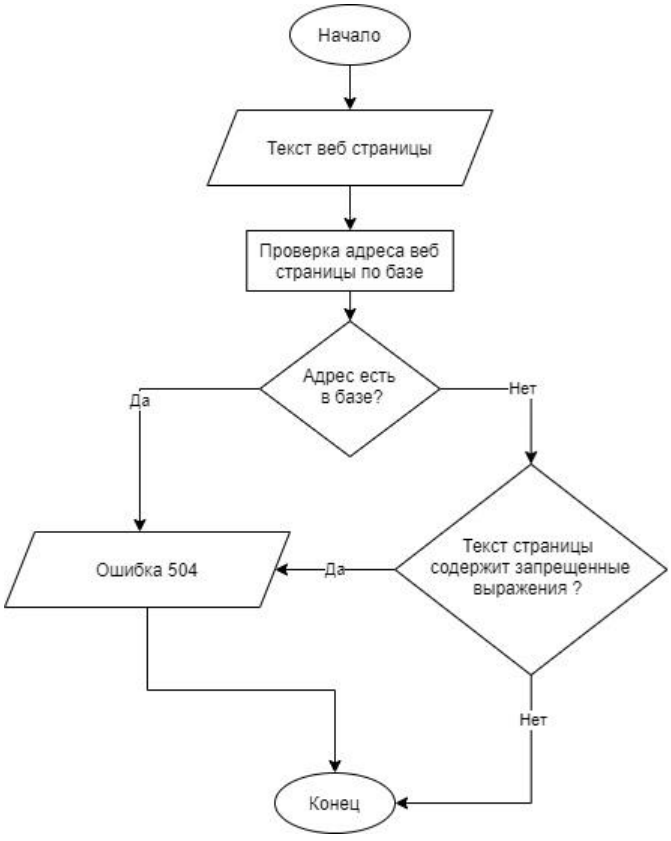

Рис. 6. Алгоритм работы расширения
Fig. 6. Expansion algorithm

Программная реализация разработанного монитора безопасности разделена на две части. Архитектурно используется схема клиент-серверного приложения. В качестве клиентов выступают расширение и панель управления родителей. Стоит отметить, что панель управления выполняет презентационную роль. Ее основной задачей является вывод информации, полученной от сервера. Главный упор на этапе разработки этой панели был сделан на визуальное оформление.

Сервер координирует работу всех расширений и панелей управления, поэтому его работа обеспечивается двумя основными классами. Суть этих классов сводится к тому, что они преобразуют поступающие команды в понятные базе данных SQL-запросы.

Метод формирования запроса типа update при обновлении статуса страницы или списка разрешенных или запрещенных фраз:

```
public static function getUpdateQuery($table,$params,$entity = "",$id = ""){

if($entity != ""){
$params = self::getParams($params,$entity);
}
global $entity_key;

if(isset($entity_key[$entity])){
$id = $entity_key[$entity];
}

$id_value = $params[$id];

unset($params[$id]);
$set_array = array();
foreach($params as $key => $val){
$set_array[] = "`{$key}` = '{$val}'";
}



return "UPDATE `".$table."` SET ".implode(",",$set_array)." WHERE {$id} = '{$id_value}'";
}
```

Для тестирования программного средства монитора безопасности была создана условно опасная веб-страница, т. е. страница с содержанием запрещенных ключевых слов, которая находится по адресу zapret-test.ru. Эта страница использовалась как стенд для тестирования браузерного расширения.

В программном средстве изначально администратором создан список запрещенных выражений, но и у родителей ребенка также есть возможность вносить в список изменения, добавлять туда запрещенные веб-сайты, которые, по их мнению, могут как-то навредить безопасности ребенка (рис. 7).

Для тестирования после включения браузерного расширения на компьютере вначале нужно перейти на безопасный веб-сайт, который браузер загружает без каких-либо блокировок. После этого переходим на сайт, который был нами создан для локальных тестов, с адресом zapret-test.ru, т. е. имеющий опасный для ребенка контент. После перехода на эту страницу появляется сетевая ошибка 504 (рис. 8). Это означает, что наше расширение распознало данную страницу как вредоносную и дало ребенку понять, что попасть на нее невозможно, при этом не показав ему явно, что сайт заблокирован каким-либо расширением, которое установили его родители, выдав это за простую сетевую ошибку.

Далее переходим в Яндекс и проверяем работу поисковых запросов. После ввода в строке «мультик “Унесенные призраками”» браузер открывает для ребенка все доступные страницы. В личном кабинете родителя можно перейти во вкладку активности и просмотреть все посещения ребенка в браузере с установленным расширением, т. е. просмотреть историю, сайты, на которые заходил их ребенок, а также другие функции панели управления (рис. 9).

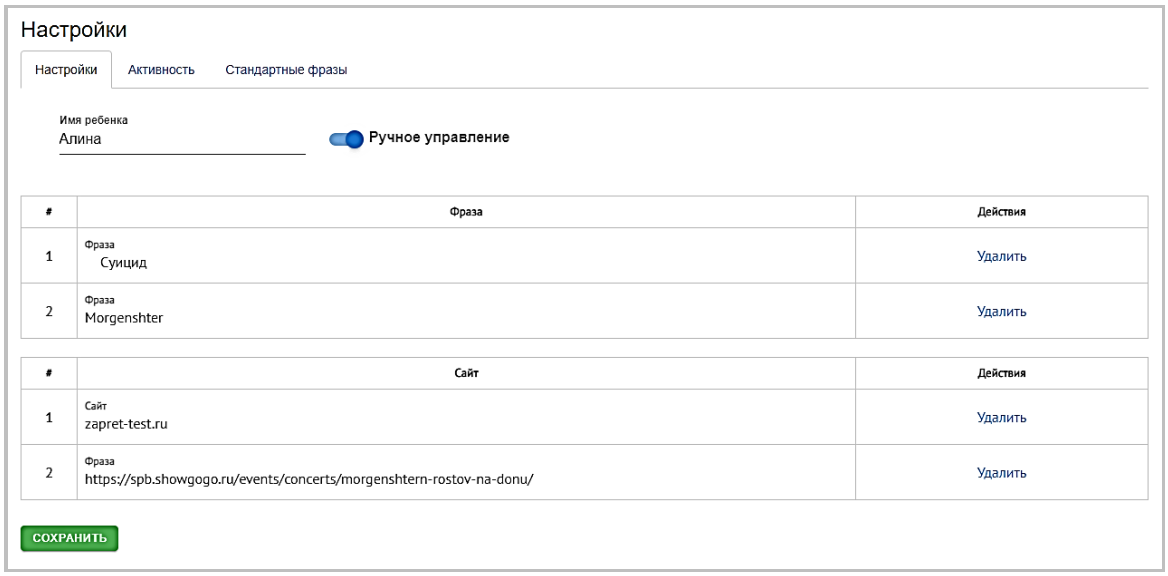

Рис. 7. Вкладка настройки запрещенных сайтов
Fig. 8. Banned sites settings tab

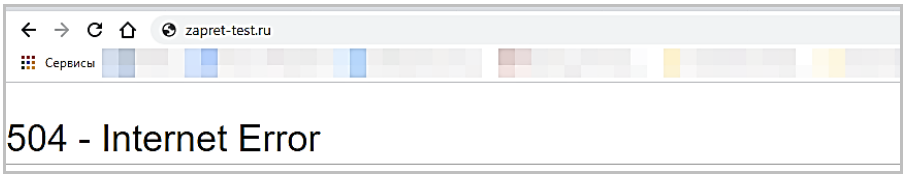

Рис. 8. Окно ошибки
Fig. 8. Error window

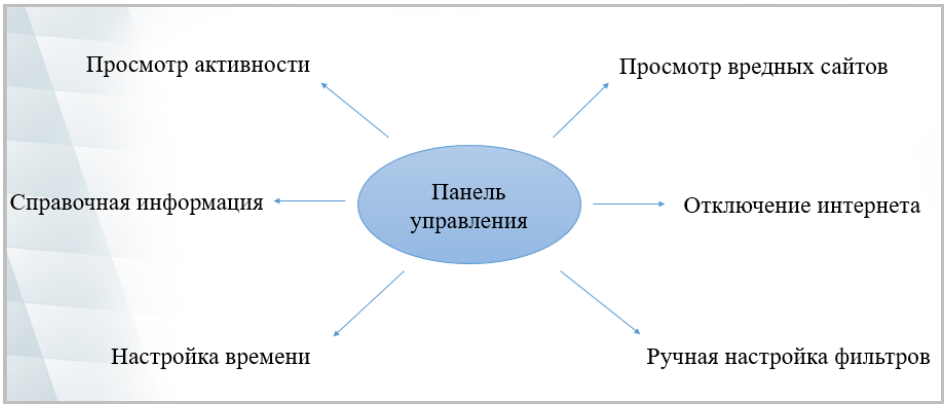

Рис. 9. Функции панели управления
Fig. 9. Control panel functions

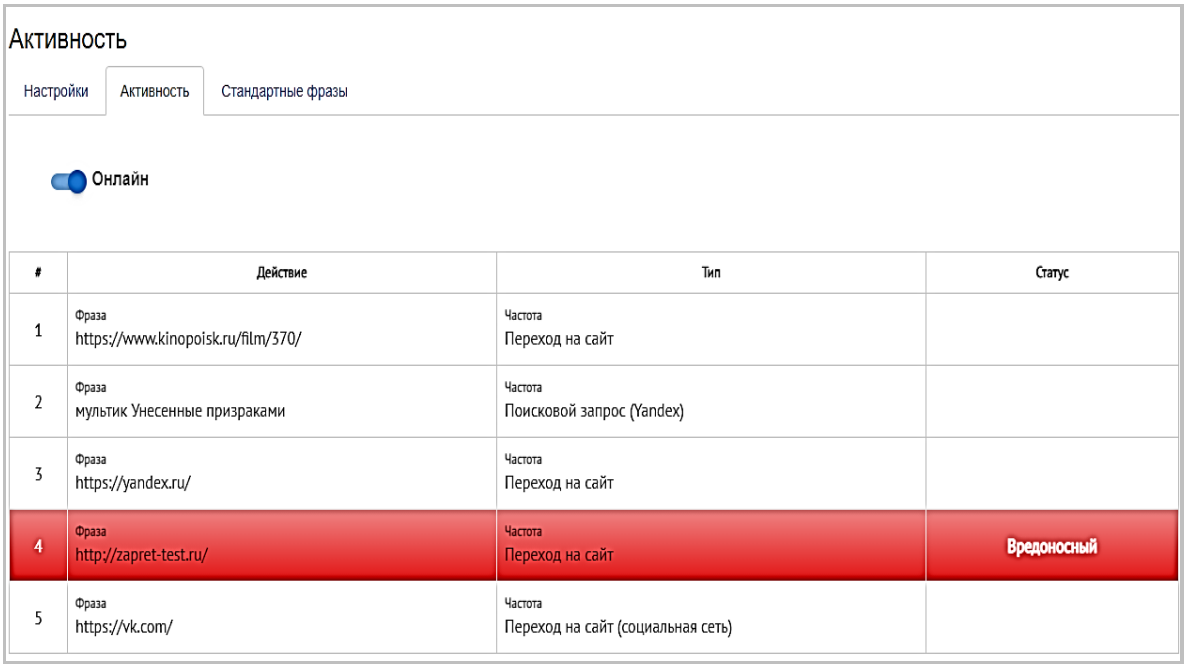

Рис. 10. История посещения сайтов
Fig. 10. Website visit history

Вредоносные опасные сайты выделяются специальным цветом, чтобы их можно было сразу отличить от разрешенных для просмотра ребенка сайтов (рис. 10).

Заключение

В процессе разработки авторами этой статьи были изучены возрастные особенности использования Интернета детьми и несовершеннолетними подростками, выявлено негативное влияние социальных сетей на психику детей и подростков, исследована классификация рисков и угроз, возможных при отсутствии родительского контроля, проведен анализ защиты детей и подростков на правовой основе. Существующие интернет-риски способны нанести непоправимый ущерб эмоциональному благополучию и психологическому здоровью ребенка или несовершеннолетнего подростка и поэтому требуют со стороны родителей тщательного анализа и нивелирования.

Были проанализированы существующие программные приложения, созданные с целью обеспечения информационной безопасности детей и несовершеннолетних подростков в сети «Интернет». На основе этого анализа была выбрана технология разработки программного средства в виде браузерного расширения, разработаны основные модули и алгоритмы для работы с сетевыми ресурсами, и создано ПО для осуществления родительского контроля за поведением детей и несовершеннолетних подростков в Интернете с целью их защиты от деструктивного и опасного влияния веб-сайтов, представляющих угрозу их психологической, нравственной и моральной защищенности.

Рассмотрено использование уже существующего в мире ПО и проведено его сравнение с разработанным авторами этой статьи монитором безопасности. Выяснено, что существующие программные приложения в основном созданы за рубежом и могут использоваться в России только при подключении платных версий. Кроме того, они, как правило, имеют англоязычный интерфейс и трудный в настройке функционал, непонятный многим российским родителям, особенно не связанным по своей профессии с информационными техноло-

гиями. В то же время импортозамещающий монитор безопасности, разработанный авторами этой статьи, является бесплатным и очень простым в использовании. Разработка внедрена в эксплуатацию в детском клубе ООО «Кибер Арена» (Ростов-на-Дону), и показала хорошие результаты, вызвав благодарность руководства клуба.

Список литературы

1. **Атагимова Э. И.** Проблемы отрицательного влияния Интернета на нравственное воспитание подростков в информационном пространстве и пути решения // Правовая информатика. 2013. № 1. С. 21–24.
2. **Barakhnin V., Mukhamedyev R., Mussabaev R., Kozhemyakina O., Issayeva A. et al.** Methods to identify the destructive information. *Journal of Physics: Conference Series*, 2019, no. 1405, p. 2–10.
3. **Воронина И. Е., Гончаров В. А.** Анализ эмоциональной окраски сообщений в социальных сетях (на примере сети «В_Контакте») // Компьютерная лингвистика и обработка естественного языка. 2015. № 4. С. 151–158.
4. **Gostyunina V. A., Davidyuk N. V.** The combined method of textual information analysis for the content of destructive indicators. *Journal of Physics: Conference Series*, 2019. no. 1399, p. 2–8. DOI 10.1088/1742-6596/1399/3/033109
5. **Байдулова Д. Р., Гостюнина В. А., Давидюк Н. В.** Применение машинного обучения в процессе поиска деструктивной информации в web-контенте // Вопросы информационной безопасности. 2019. № 1. С. 62–68.
6. **Браницкий А. А., Дойникова Е. В., Котенко И. В.** Использование нейросетей для прогнозирования подверженности пользователей социальных сетей деструктивным воздействиям // Информационно-управляющие системы. 2020. № 104. С. 24–33. DOI 10.31799/1684-8853-2020-1-24-33.
7. **Сидорова Е. А., Кононенко И. С., Загорулько Ю. А.** Подход к фильтрации запрещенного контента в веб-пространстве // Аналитика и управление данными в областях с интенсивным использованием данных: Сб. науч. тр. XIX Междунар. конф. DAMDID / RCDL’2017. М., 2017. С. 94–101.

References

1. **Atagimova E. I.** Problems of the negative influence of the Internet on the moral education of adolescents in the information space and solutions. *Legal Informatics*, 2013, no. 1, p. 21–24. (in Russ.)
2. **Barakhnin V., Mukhamedyev R., Mussabaev R., Kozhemyakina O., Issayeva A. et al.** Methods to identify the destructive information. *Journal of Physics: Conference Series*, 2019, no. 1405, p. 2–10.
3. **Voronina I. E, Goncharov V. A.** Analysis of the emotional coloring of messages in social networks (on the example of the “V_Kontakte” network). *Computational linguistics and natural language processing*, 2015. no. 4, p. 151–158. (in Russ.)
4. **Gostyunina V. A., Davidyuk N. V.** The combined method of textual information analysis for the content of destructive indicators. *Journal of Physics: Conference Series*, 2019. no. 1399, p. 2–8. DOI 10.1088/1742-6596/1399/3/033109
5. **Baidulova D. R., Gostyunina V. A., Davidyuk N. V.** Application of machine learning in the process of searching for destructive information in web-content. *Issues of information security*, 2019, no. 1, p. 62–68. (in Russ.)
6. **Branitskiy A. A., Doinikova E. V., Kotenko I. V.** Using neural networks to predict the susceptibility of social network users to destructive influences. *Information and control systems*, 2020, no. 104, p. 24–33. (in Russ.) DOI 10.31799/1684-8853-2020-1-24-33

7. **Sidorova E. A., Kononenko I. S., Zagorulko Yu. A.** An approach to filtering prohibited content in the web space. In: Analytics and data management in data-intensive areas: collection of scientific papers of the XIX International Conference DAMDID / RCDL'2017. Moscow, 2017, p. 94–101. (in Russ.)

Материал поступил в редколлегию
Received
29.12.2020

Сведения об авторах

Зеленский Александр Андреевич, аспирант первого года обучения профиля «Информационные системы и процессы», кафедра кибербезопасности информационных систем, факультет информатики и вычислительной техники, Донской государственный технический университет (ДГТУ) (Ростов-на-Дону, Россия)

sashaz1696@yandex.ru
ORCID 0000-0002-3452-9880

Григорян Анна Игоревна, студентка 6 курса профиля «Компьютерная безопасность», кафедра кибербезопасности информационных систем, факультет информатики и вычислительной техники, Донской государственный технический университет (ДГТУ) (Ростов-на-Дону, Россия)

Черкесова Лариса Владимировна, доктор физико-математических наук, профессор кафедры кибербезопасности информационных систем, факультет информатики и вычислительной техники, академик Российской Академии Естествознания, член-корреспондент Международной академии наук прикладной радиоэлектроники, член-корреспондент Российской академии изучения проблем национальной безопасности, Донской государственный технический университет (ДГТУ) (Ростов-на-Дону, Россия)

chia2002@inbox.ru

Ревякина Елена Александровна, кандидат технических наук, доцент, кафедра кибербезопасности информационных систем, факультет информатики и вычислительной техники, Донской государственный технический университет (ДГТУ) (Ростов-на-Дону, Россия)

revyelena@yandex.ru

Information about the Authors

Alexander A. Zelensky, 1st year postgraduate student, «profile Information Systems and Processes», Department of Cybersecurity of Information Systems, Faculty of Informatics and Computer Sciences, Don State Technical University (DSTU) (Rostov on Don, Russian Federation)

sashaz1696@yandex.ru
ORCID 0000-0002-3452-9880

Anna I. Grigoryan, 6th year student, «profile computer security», Department of Cybersecurity of Information Systems, Faculty of Informatics and Computer Sciences, Don State Technical University (DSTU) (Rostov on Don, Russian Federation)

Larisa V. Cherkesova, Doctor of Physical and Mathematical Sciences, Professor of the Cybersecurity of information systems Department, Informatics and Computer engineering Faculty, Acad. of Russian Academy of Natural Sciences, Corresponding Member of International Academy of Applied Radioelectronics Sciences, Corresponding Member of Russian Academy of National Security Problems Investigations, Don State Technical University (DSTU) (Rostov on Don, Russian Federation)

chia2002@inbox.ru

Elena A. Revyakina, Candidate of Technical Sciences, Associate Professor, Department of Cybersecurity of Information Systems, Faculty of Informatics and Computer Sciences, Don State Technical University (DSTU) (Rostov on Don, Russian Federation)

revyelena@yandex.ru