Development of safety monitor from destructive influences of web–sites and social networks of internet

Larisa Cherckesova[1], *Alexandr* Zelensky[1], *Elena* Revyakina[1], *Olga* Safaryan [1*], and *Denis* Korochentsev[1]

[1] Don State Technical University, Gagarin Square, 1, Rostov-on-Don, 344003, Russia

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.

1 Introduction

Ensuring the safety of children and adolescents is a task of increased urgency [1]. To solve it, it is necessary to develop special software - a security monitor that allows you to view, analyze and block a destructive website with malicious content even before it is loaded onto the computer of a young user, and also helps parents control the hobbies of their children [2-4].

The problem of text analysis on Web sites has been considered by many Russian and foreign authors, including I.Ye. Voronina, V. A. Goncharov (in the work "Analysis of the emotional coloring of messages in social networks (on the example of the network" V_Kontakte ") [5], VB Barakhnin, RI Mukhamedyev (in the work" Methods to identify the destructive information ") [6] and many others [7-10].

The aim of the authors' research is to develop software - a security monitor designed for parents of children and teenagers, capable of protecting young users from the destructive influence of Web sites with malicious content that pose a threat to their psychological security.

The object of the research is Internet resources containing destructive text content that threatens the psychological safety of children and teenagers.

*Corresponding author: safari_2006@mail.ru

The subject of the research is the algorithms for analyzing the text content of Web sites and methods of blocking such sites before being downloaded to a computer by a young user.

There are similar programs in the world. Among them, one must first of all name software products: KinderGate, KidShell, Kaspersky and others (Table 1). Let's consider possible analogs [11-14].

Table 1. Existing analogues of the developed software.

	Price	Developer	Interface in Russian language	Age of children	Platform	Hidden mode of work
Kids Place	Free/Paid	Foreign	-	5-7	Android	-
Mspy	Paid	Foreign	-	5-17	Windws	-
SafeKiddo	Paid	Foreign	-	5-17	Windws, Android, Apple	-
KidLogger	Free/Paid	Foreign	+	5-17	Android	+
KidShell	Free/Paid	Foreign	+	5-7	Android	-
PlayPad	Free/Paid	Foreign	+	5-7	Android	-
KinderGate	Paid	Foreign	+	5-17	Windws	-
Norton Family	Paid	Foreign	+	5-17	Windws, Android, Apple	+
Kaspersky	Free/Paid	Russia	+	5-17	Windws, Android, Apple	+
ParentaWatch	Free	Russia	+	5-17	Windws, Android, Apple	+

2 Development of a security monitoring system

The security monitor developed by the authors has its own principles (Fig. 1) and the following differences from analogues:

– monitoring and analysis of the text of the site for the presence of destructive phrases and words is performed by preloading the site (hidden from the young user);
– the detected Web site is automatically added to the database of destructive sites;
– a list of destructive phrases and words is formed, which is constantly updated;
– the developed security monitor is an import substitution, absolutely free, and is designed for a Russian user with any level of computer literacy.

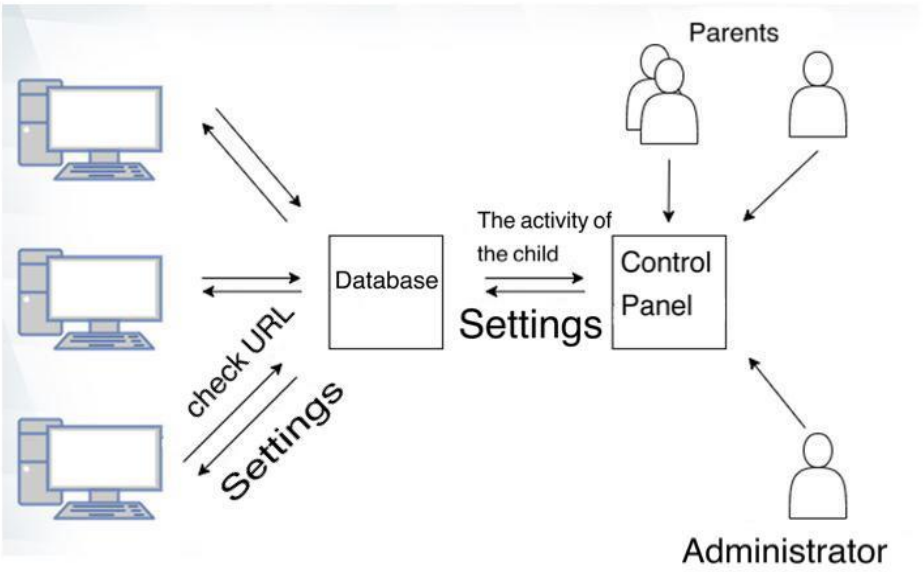


Fig. 1. Principle of the developed software.

Elements of the program: browser extension; server; parent's personal account.

Within the framework of the chosen program architecture, the procedure for blocking a site with unsafe content is as follows: when a minor child or teenager opens any site, the browser extension is introduced into the page loading process, stretches the site load while it is being checked, that is, visually stops the page load and loads it in the background. The program checks a Web site for dangerous content, then either deletes the content and displays an error message on the screen, or opens the Web page itself, but sends the information to the server and to the parent's personal account. Parents, in turn, can choose the status of the viewed content and block it [15-17].

Browser extension is implemented using the Java Script programming language and has its own operating principle (Fig. 2) and its own algorithm of work. The expansion works in several stages. At the pre-load stage, code is included that covers the entire page with a white layer to stretch the page load while it is being checked. The next stage is the study of the downloaded, but not yet displayed content. Further, if the website check was passed, then the white layer is removed and the already loaded page opens. Otherwise, the content is deleted and a network error appears on the screen instead.

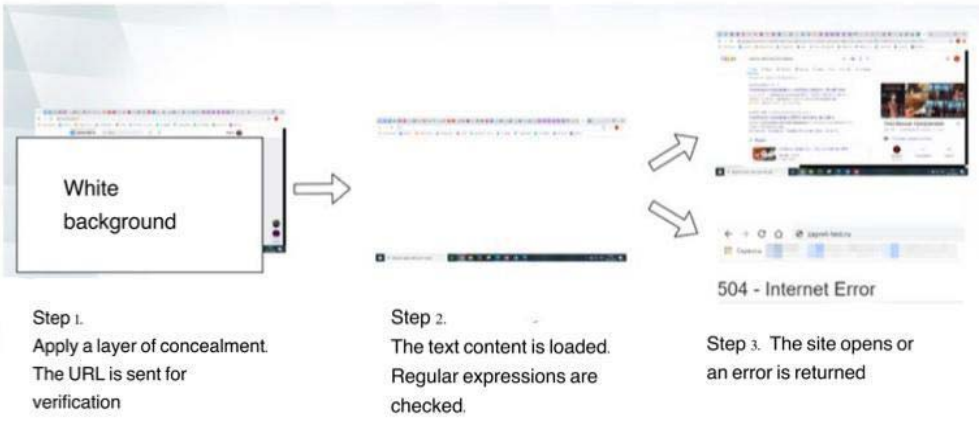


Fig. 2. How the extension works.

To speed up the work of the extension, the server generates a list of forbidden expressions, words and phrases every day, so as not to make a selection constantly. The cache of entries is broken down by types of threats, for example, phrases related to erotica, pornography, pedophilia, murder, suicide, etc. To calculate the site's rating to measure the degree of its destructiveness, formula 1 is used.

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

q_i – site i rating from 0 to 1; i – the serial number of the site in the system; j – the serial number of the visitor; s_i- the number of unique site visitors; t_{ij} – harmfulness coefficient, [0,0.5,1]

The software implementation of the developed safety monitor is divided into two parts. Architecturally, the client-server application scheme is used. The clients are the extension and the control panel of the parents. It should be noted that the control panel performs a presentation role and mainly displays information received from the server, and the main emphasis at the development stage of this panel was placed on visual design.

The server coordinates the work of all extensions and the work of control panels, so its work is provided by two main classes. The essence of these classes boils down to the fact that they transform incoming commands into an understandable SQL database.

Method for generating a request of the update type when updating the page status or the list of allowed or forbidden phrases (Fig. 3).

```
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}'";
}
```

Fig. 3. Method for updating page status or list of allowed or forbidden phrases.

3 Results of research

To test the security monitor software, a conditionally dangerous Web page was created, that is, a page containing keywords, which is located at zapret–test.ru. This page was used as a test bench for extensions.

In the tool, the administrator initially created a list of prohibited expressions. But parents also have the opportunity to make changes to the list, to add prohibited websites there, which, in their opinion, may somehow harm their child (Fig. 4).

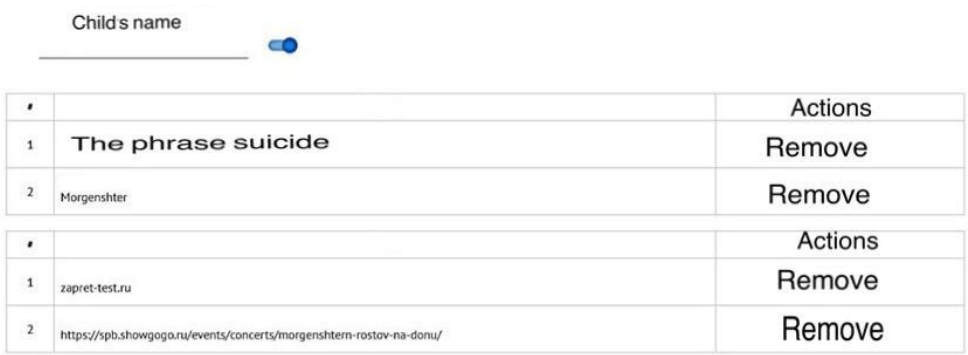


Fig. 4. Banned sites settings tab.

After enabling the extension on the computer, we will go to the secure website. The browser loads it without any blocking. Now let's go to the site that we created for local tests with the address zapret-test.ru, that is, it has dangerous content for a child. After going to this page, the network error 504 appears (Fig. 5).

This means that our extension recognized this page as malicious, and made the child understand that it was impossible to get on it, without showing explicitly that the site was blocked by some extension that the parents installed, passing it off as a simple network error.

Fig. 5. Error window.

Next, we will go to Yandex and check the work of search queries. After entering in the line cartoon "Spirited away", the browser will open all available pages for the child.

In the parent's personal account, you can go to the activity tab and view all the child's activities in the browser with the extension installed, that is, view the history of visits to all sites visited by the child and other functions of the control panel (Fig. 6).

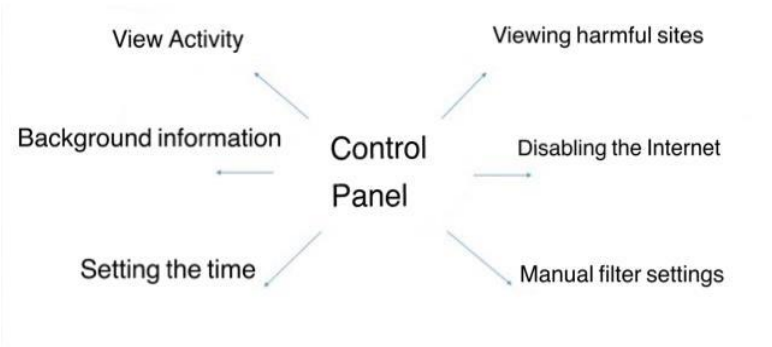
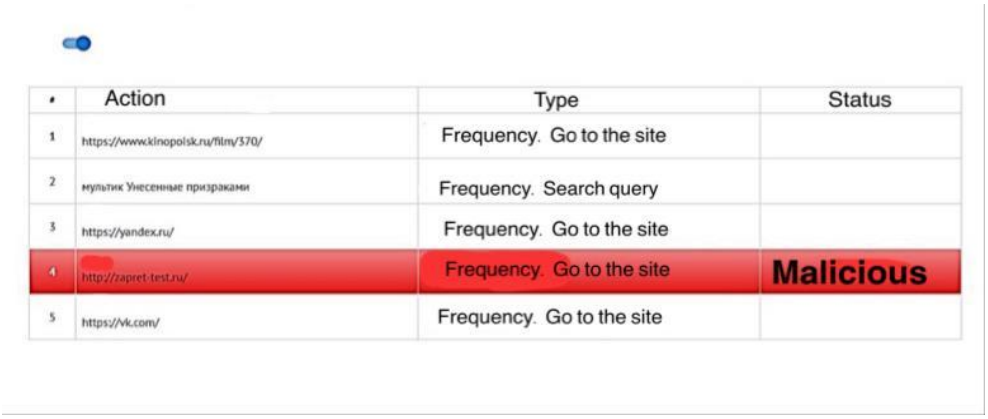


Fig. 6. Control panel functions.

Malicious sites are highlighted in a special color so that they can be immediately distinguished from the allowed ones (Fig. 7).



•	Action	Type	Status
1	https://www.kinopoisk.ru/film/370/	Frequency. Go to the site	
2	мультик Унесенные призраками	Frequency. Search query	
3	https://yandex.ru/	Frequency. Go to the site	
4	http://zapret-test.ru/	Frequency. Go to the site	Malicious
5	https://vk.com/	Frequency. Go to the site	

Fig. 7. Website visit history.

4 Discussion and conclusions

In the process of development, the authors studied the age characteristics of the use of the Internet by children and underage adolescents, identified the negative impact of social networks on the psyche of children and adolescents, studied the classification of risks and threats that are possible in the absence of parental control, analyzed the protection of children and adolescents on a legal basis. The existing Internet risks can be conditionally divided into content, communication, electronic and user risks. Each of these types of risks can cause irreparable damage to the emotional well-being and psychological health of a child or adolescent, and therefore requires careful analysis and leveling.

Existing programs to ensure the safety of children on the Internet were analyzed. Based on this analysis, software development technologies, basic program modules and algorithms for working with resources were selected. A software application has been created for parental control of children and teenagers against the destructive influences of Web sites that pose a threat to their security.

The use of the existing software is considered and a comparison is made with the security monitor developed by the author. It was revealed that the existing software applications were created abroad and can be used in Russia only if paid versions are connected.

References

1. P.J.C. Adachi, T. Willoughby, Child Development, **87 (6)**, 1877-1892 (2016), 10.1111/cdev.12556
2. P. Razumov, N. Boldyrikhin, L. Cherckesova, et al., E3S Web of Conferences, **224**, 01033 (2020)
3. V.V. Zhilin, I.I. Drozdova, I.A. Sakharov, et al., in Proceedings of IEEE East-West Design and Test Symposium, EWDTS 2019, Institute of Electrical and Electronics Engineers, Inc., 8884375 (2019), DOI: 10.1109/EWDTS.2019.8884375
4. Federal Law of December 29, 2010 N 436-FZ (as revised on July 31, 2020) "On the Protection of Children from Information Harmful to Their Health and Development." (2010)
5. I. Ye. Voronina, V. A. Goncharov, Computational Linguistics and Natural Language Processing, **4**, 151-158 (2015)
6. M. Paciello, C. Tramontano, A. Nocentini, R. Fida, E. Menesini, Computers in Human Behavior, **103**, 190-198 (2020)
7. W. Elsayed, Heliyon, **7(2)**, e06327 (2021)
8. L. Tomczyk, Technology in Society, **58**, 101137 (2019)
9. A. Vale, F. Pereira, M. Gonçalves, M. Matos, Children and Youth Services Review, **93**, 88-99 (2018)
10. A. Wąsińskia, L. Tomczyk, Children and Youth Services Review, **57**, 68-74 (2015)
11. V. Mitchella, D. Petrovicib, B. B. Schlegelmilchc, I. Szőcsd, Electronic Commerce Research and Applications, **14(2)**, 95-103 (2015)
12. A.I. Olugbenga, Heliyon, **6(8)**, e04584 (2020)
13. J.F. Brockmyer, Child and Adolescent Psychiatric Clinics of North America, **24(1)**, 65-77 (2015), https://doi.org/10.1016/j.chc.2014.08.001
14. W. Wang, L. Qiu, Addictive Behaviors, **84**, 171-177 (2018)

15. S.A. Radi, S. Shokouhyar, Sustainable Production and Consumption, **25**, 217-233 (2021), https://doi.org/10.1016/j.spc.2020.08.012
16. S. Shadroo, A.M. Rahmani, Computer Networks, **139**, 19-47 (2018), https://doi.org/10.1016/j.comnet.2018.04.001
17. M.S. Hajar, H.K. Kalutarage, Computers & Security, **104**, 102211 (2021), https://doi.org/10.1016/j.cose.2021.102211