Рис. 3. Загрози Інтернету

- залучення через Інтернет до протизаконної діяльності;
- знайомства через Інтернет з метою пошуку сексуальних відносин.

Порушення безпеки: віруси, небажана пошта (Спам), он-лайн шахрайство тощо.

Діти використовують сучасні комунікаційні пристрої, інформаційні технології і ресурси, зокрема Інтернет, навіть не замислюючись над широтою всіх можливостей, які вони здатні надавати, і загроз, які вони несуть. Оскільки ефективність технологій не в їх існуванні, а в їх використанні, необхідно, щоб діти знали про них і щоб хотіли і мали можливість їх усвідомлено використовувати для досягнення нової якості або нових результатів [2]. Дорослі мають контролювати і скеровувати діяльність дітей з використання інформаційних технологій та інформаційних ресурсів, сприяти формуванню свідомого підходу до використання Інтернету. Завдання дорослих — створити умови і надати можливості використання інформаційно-комунікаційних технологій молодому поколінню для його повноцінного розвитку й освіти. Щодо користування Інтернетом, то пріоритетними завданнями є: формування у дітей інтернет-культури, запобігання інтернет-залежності, забезпечення інтернет-безпеки, використання корисних інтернет-ресурсів.

★ ★ ★

Дудка Т. Н. Дети и Интернет: возможности и угрозы

Аннотация. Учитывая современное состояние и тенденции использования информационных технологий, выделены основные возможности и угрозы использования Интернета детьми, определена роль взрослых в формировании сознательного отношения детей к использованию Интернета.

Ключевые слова: информационные технологии, Интернет, интернет-ресурсы, возможности Интернета, угрозы Интернета.

★ ★ ★

Dudka T. Children and the Internet: opportunities and threats

Abstract. Given the current state and trends in the use of information technology, highlights the main opportunities and threats of the use of the Internet by children, defines the role of adults in the formation of a conscious attitude of children to use the Internet.

Keywords: information technology, internet, online resources of the Internet, Internet threats.

Література

1. Руководство по реализации пилотного проекта ИИТО ЮНЕСКО «Обучение для будущего» (LFF), ИИТО ЮНЕСКО, 2012 [Электронный ресурс]. — Режим доступу: http://iite.unesco.org/capacity_development/lff/files/LLFGuidelines-final-rus-unoffic_transl.pdf.
2. *Манако А. Ф., Синица Е. М.* Инновационные научно-образовательные пространства на базе перспективных информационных технологий // Новые информационные технологии в образовании для всех: монография. — К., 2012. — 269 с.

★ ★ ★

ФІЛЬТРАЦІЯ ІНТЕРНЕТ-КОНТЕНТУ

Балабан Роман Анатолійович,

методист з навчальних дисциплін міського методичного кабінету Департаменту освіти Вінницької міської ради, учитель інформатики ЗШ I–III ступенів №34 ВМР, balaban286@gmail.com.

Використання інформаційно-комунікаційних технологій на уроках, і не лише інформатики, набуло настільки стрімкого темпу, що постало питання захисту від того вмісту, який нам дає глобальна мережа. Більшість педагогів і, на жаль, серед них учителі інформатики, створюють власні інтернет-ресурси, використовуючи безкоштовні сервіси, перевантажені, як мінімум небажаною рекламою, забуваючи, що учень повинен мати доступ до необхідних матеріалів, інформаційних ресурсів, але не повинен мати можливості переглянути або завантажити матеріали, для нього не призначені. Тому постає питання про захист учнів від негативного контенту, що ллється з Всесвітньої мережі.

У наш час є три способи фільтрації Інтернет-контенту:

- серверна фільтрація;
- клієнтська фільтрація;
- он-лайн фільтрація.

У попередніх числах журналу «Комп'ютер у школі та сім'ї» за 2012 рік розглядались способи Онлайн фільтрації, тому зупинимось на розгляді серверної, а особливо на засобах клієнтської фільтрації Інтернет-контенту.

Розглянемо коротко принцип роботи серверної фільтрації. Є виділений комп'ютер, на ньому налаштовано Інтернет для роздачі на інші комп'ютери через локальну мережу. Фільтрація відбувається на даному виділеному комп'ютері через використання програм для організації серверної фільтрації.

Найпоширенішими є:

- МКФ (Windows);
- UserGate (Windows);
- ISA Server (Windows);
- DansGuardian (Linux);
- Mindwebfilter (Linux).

Але в цьому способі фільтрації є два найбільших недоліки: *наявність досить потужного і недешевого комп'ютера; придбання недешевих ліцензій для програмного забезпечення цього комп'ютера*.

Для того щоб здешевити використання серверної фільтрації в частині програмного забезпечення, можна скористатись дистрибутивом ОС Linux **Ipfire 2.9.** Завантажити дистрибутив і повну інструкцію з його встановлення і налаштування можна з ftp-сервера лабораторії інформаційних та комунікаційних технологій ФМГ №17 м. Вінниці за посиланням: ftp://ftp.pmg17.vn.ua/pub/SchoolNet/.

Розглянемо більш трудоємкий, але безкоштовний, а також такий, що не потребує значних ресурсів у комп'ютерній техніці спосіб фільтрації Інтернет-контенту — клієнтський.

Одним із найрозповсюдженіших Інтернет-фільтрів є **«Інтернет цензор»**.

Програма встановлюється локально на один комп'ютер. В основі роботи програми лежить технологія «білих списків». Основною функцією програми є блокування доступу до Інтернет-сайтів, які не входять до дозволеної бази сайтів («білий список») або блокування сайтів, що знаходяться в базі заборонених сайтів («чорний список») (рис. 1). Списки сайтів заповнюються вручну, хоча є можливість завантажити списки, створені компанією-розробником.

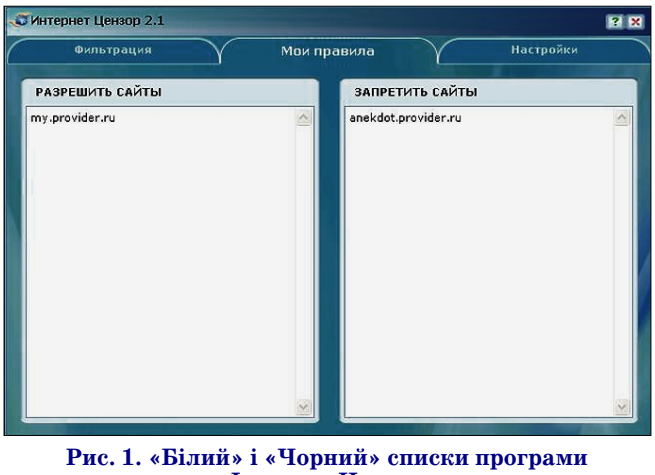

Рис. 1. «Білий» і «Чорний» списки програми Інтернет Цензор

У разі включення режиму фільтрації замість заборонених сайтів браузер буде показувати сторінку-замінник. Якщо на дозволеному ресурсі є небажані елементи, то заміниться тільки та частина сторінки, де знаходяться заборонені до перегляду елементи.

Використовуючи спеціальні налаштування, можна заборонити запуск на ПК Інтернет-пейджерів, файлообмінники, а також ftp-доступ (рис. 2).

Завдяки використанню електронної адреси й паролю під час встановлення обійти програму досить складно.

Також для захисту від небезпек в Інтернеті можна скористатись українською безкоштовною програмою «Центр сімейної безпеки Київстар», яка дозволяє користувачам фіксованого Інтернету захистити дітей від небажаного контенту, захистити комп'ютер від вірусів, злому хакерів та шпигунських і шкідливих програм.

Рис. 2. Спеціальні налаштування

Можливість встановити «Центр сімейної безпеки Київстар» надається всім користувачам фіксованого Інтернету, які користуються операційними системами Windows XP, Windows Vista, Windows 7, Windows 8.

Центр сімейної безпеки «Київстар» включає набір рішень для безпеки Вашого комп'ютера (рис. 3).

Рис. 3. Центр сімейної безпеки «Київстар»

1. «Батьківський контроль» — рішення для онлайн-безпеки дітей (рис. 4).

Програма дозволяє встановити фільтри для перегляду сайтів тільки з «білого списку», сайтів для ді-

Рис. 4. Програма «Батьківський контроль»

тей, сайтів для всіх (крім сайтів для дорослих), на спілкування в мережі. Включає попередження про контент для дорослих.

Також програма дозволяє створювати звіти і контролювати дії дитини в Інтернеті та на комп'ютері.

2. «Антивірус» — для знаходження і «лікування» заражених вірусом програм.

3. «Брандмауер» — для запобігання злому Вашого комп'ютера хакерами або проникненню зловмисних програм.

4. «Сканер безпеки» — для знаходження і знешкодження шкідливих і шпигунських програм (рис. 5).

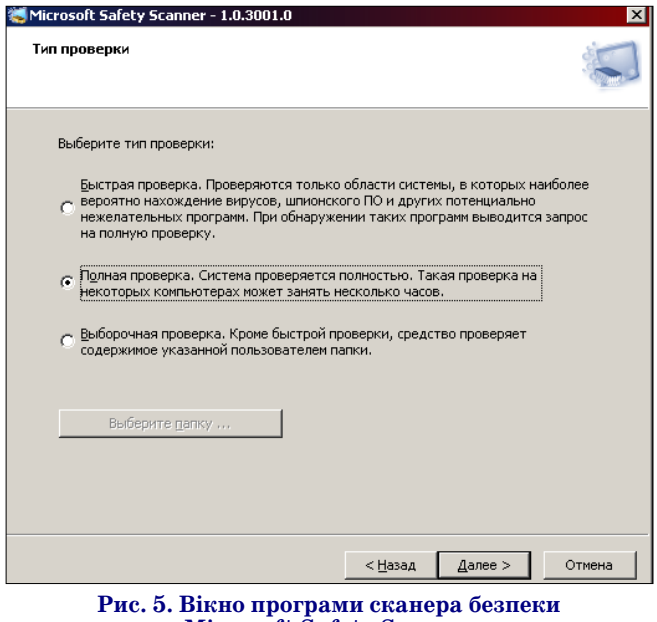

Рис. 5. Вікно програми сканера безпеки Microsoft Safety Scanner

Іншою безкоштовною програмою є **«КіберПапа»**.

КіберПапа — це дитячий Інтернет-фільтр, який працює у всіх браузерах, що блокує неперевірені сайти, не допускаючи до них дітей. За своєю сутністю КіберПапа є Інтернет-фільтром, орієнтованим на дітей від 6 до 14 років. Після активації він перенаправляє весь трафік через свої проксі-сервери і видає дитині безпечний веб-інтерфейс із власним пошуковим сервісом (рис. 6), заснованим на технології білого списку.

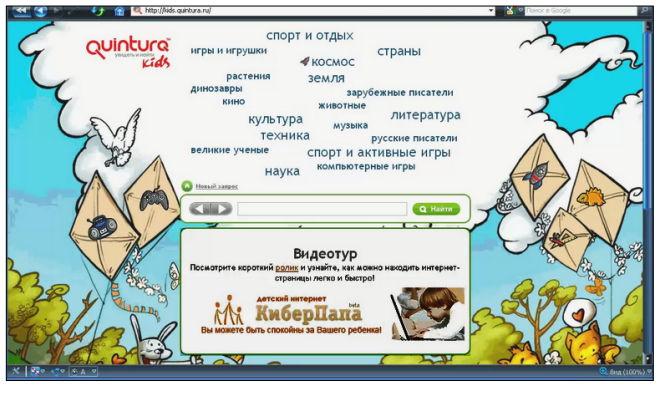

Рис. 6. Веб-інтерфейс Інтернет-фільтру КіберПапа

Як і в Інтернет цензорі завдяки використанню електронної адреси і паролю під час реєстрації програми обійти її захист достатньо складно.

Наступною є програма **ChildWebGuardian Lite**. Це також програма-фільтр.

У цій програмі реалізовані такі функції, як: блокування доступу до мережі Інтернет за часом, заборона доступу на сайт «ВКантекте», функція заборони Однокласників і функція, що обмежує за часом спілкування в ICQ (рис. 7).

Функція «блокувати доступ до Інтернету» дозволяє повністю відключити доступ до всесвітньої мережі у визначений час (рис. 8).

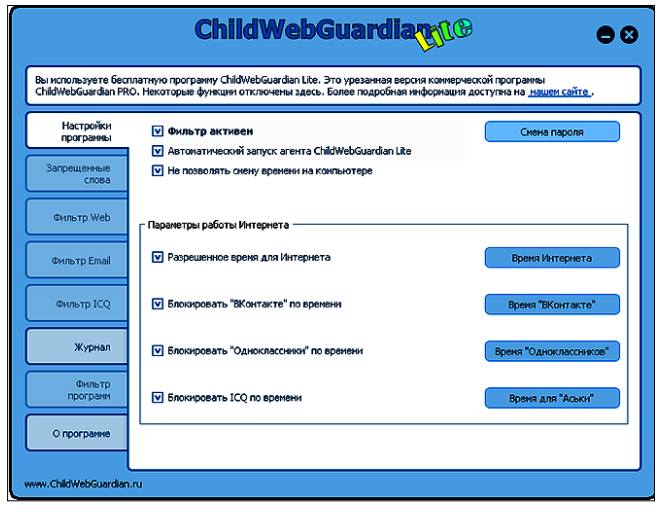

Рис. 7. Вікно налаштувань ChildWebGuardian Lite

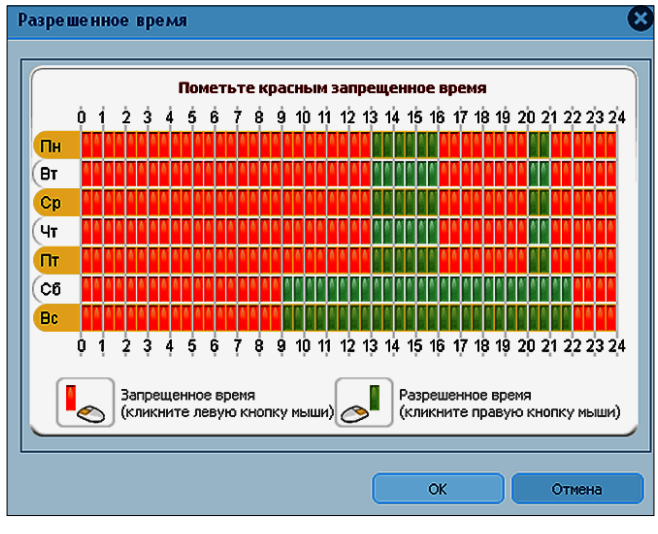

Рис. 8. Вікно налаштувань часу доступу до мережі Інтернет у програмі ChildWebGuardian Lite

Зазвичай, переглянутий список засобів клієнтської фільтрації Інтернет-контенту не є повним і кожен із користувачів воліє обирати свій спосіб і програмний продукт для захисту від небажаного вмісту веб-ресурсів. Попри це, описані наявні засоби клієнтської безпеки дають змогу на безкоштовних засадах реалізувати засоби захисту учнів від небажаного контенту під час навчання у школі, а також у домашніх умовах без спеціального і дороговартісного обладнання і програмного забезпечення.

Список використаних джерел

1. http://habrahabr.ru/.
2. ftp://ftp.pmg17.vn.ua/pub/SchoolNet/.
3. http://www.kyivstar.ua/press_center_new/news/?id=29664.
4. http://www.bestfree.ru/soft/inet/children-online.php.
5. http://www.childwebguardian.ru/lite/.