

**УДК 004.492 : 004.453 : 004.031.43**

**О.О. Горбенко, О.О. Супруненко, к.т.н, доц.**

Черкаський національний університет імені Богдана Хмельницького, Україна

## **РЕАЛІЗАЦІЯ БАР'ЄРНОГО ЗАХИСТУ У СИСТЕМАХ БАТЬКІВСЬКОГО КОНТРОЛЮ**

**O.O. Gorbenko, O.O. Suprunenko, Ph.D., Assoc. Prof.**

## **REALIZATION THE BARRIER PROTECTION OF SYSTEMS PARENTAL CONTROL**

Враховуючи широке розповсюдження комп'ютерів та стрімкий розвиток глобальної мережі Internet, зростає потреба у створенні програм батьківського контролю.

Сучасний Internet – не тільки джерело корисної інформації, а й великий концентратор ресурсів, ознайомлення з якими дуже небажано для дітей як молодшого, так і старшого шкільного віку. Будь-які нормальні батьки хочуть захистити своїх дітей від перегляду ресурсів небажаного змісту. Зробити це можна, встановивши на комп'ютери спеціальні додатки-фільтри, які називають програмами батьківського контролю. Основні функції програм батьківського контролю наступні:

- обмеження часу, проведеного дитиною за комп'ютером. Якщо в момент закінчення дозволеного періоду часу діти працюють за комп'ютером, відбувається автоматичний вихід із системи чи блокування;
- встановлення заборони на доступ до окремих ігор. Можна контролювати доступ до ігор, вибирати допустиму вікову категорію, вибирати типи вмісту, які слід блокувати, і встановлювати дозвіл або заборону на доступ до окремих ігор;
- встановлення заборон на використання дітьми окремих програм;
- обмеження доступу дитини інформації, яка може чинити негативний вплив;
- спостереження за діями дитини за комп'ютером.

Функції батьківського контролю виконують у операційній системі одночасно два завдання. З одного боку, вони дозволяють вберегти операційну систему від пошкодження недосвідченим користувачем – дитиною, студентом або просто людиною, яка тільки починає освоєння роботи за комп'ютером. З іншого боку, функції батьківського контролю дозволяють вберегти дітей та вразливих дорослих від можливого негативно-го впливу комп'ютера.

Програмний засіб батьківського контролю є продуктом для контролю доступу дітей до програм у системі та до ресурсів у мережі Internet. Продукт має поєднувати в собі можливості обмеження доступу до файлів у операційній системі комп'ютера, URL-фільтрації, фільтрації по категоріях сайтів, а також надавати можливість завдання розкладу для доступу в мережу Інтернет та можливості легування всіх дій, які виконує людина, що контролюється.

Існує два способи блокування комп'ютера від небажаного користування: апаратний та програмний. Найявні засоби апаратного блокування ефективні, проте досить радикальні, оскільки повністю обмежують роботу з комп'ютером [1]. Вони блокують доступ до інформації, не даючи можливості стежити за роботою дитини, тому в наш час набув популярності принцип роботи: «довіряй, але перевіряй» [2, 3], за яким розробляються захисні програмні додатки.

У даній роботі ставиться завдання розробки програмного продукту, який дає змогу забороняти виконувати деякі операції: користування комп'ютером більше зазначеного часу, вхід на небажані інтернет-ресурси, доступ до файлів певних форматів, обхід функціонування додатку. Також потрібно контролювати всі дії за комп'ютером та перегля-

дати звітність по роботі наступних модулів: модуль контролю часу, модуль моніторингу клавіатури, модуль безпеки, модуль знімків екрану, модуль контролю веб-сайтів.

Архітектура програмного продукту побудована на основі принципу бар'єрного захисту конфіденційної інформації. Тобто у системі батьківського контролю відкритою вважається вся інформація, яка може бути доступна дитині, а закритою – вся інформація, яку потрібно захистити від перегляду чи змінення дитиною, а також небезпечна для дитини інформація, в тому числі й специфічні програмні продукти типу riskware, adware, pornware, програми дозвону в Internet та подібні небезпечні програми.

Для забезпечення захисних функцій розроблювана програма батьківського контролю має список, у який заносяться дозволені для запуску додатки, інші ж вважаються закритими. При виході в мережу Internet важливо не тільки відфільтрувати сайти, а й блокувати приховані кнопки, спливаючі меню та інші елементи, які можуть нести як шкідливу інформацію, так і служити джерелом вірусних загроз. Тому структура системи батьківського контролю реалізована за принципом бар'єрного захисту, що має тривірневу будову (рис. 1).

На рівні браузера відбувається блокування спроб доступу до інформації у внутрішньому просторі браузера, що унеможливує впровадження шкідливого коду. Також перевіряється автентичність веб-сервера для запобігання переходу на фішингові сайти. Ці функції покладаються на мережевий екран, сервісами якого користується програма батьківського контролю.

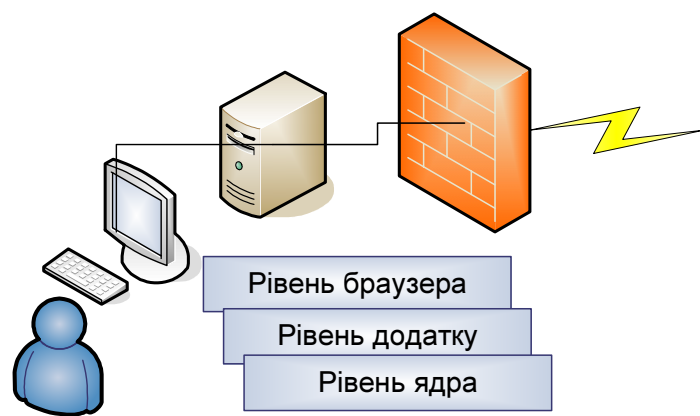


Рис.1. Структура бар'єрного захисту в системах БК

На рівні додатку визначається перелік програм, які можуть запускатися у захищеному просторі, та перелік функцій, що допустимі для користувача, який захищається. На рівні ядра відбувається шифрування натискань для унеможливлення перехвату керування віддаленими об'єктами. Таким чином, дана будова дозволяє забезпечити надійний захист дитини, яка знаходиться за комп'ютером, що підключений до мережі.

Програма батьківського контролю призначена для використання на операційних системах Windows XP, Windows Vista, Windows 7. Мінімальні апаратні вимоги для її ефективної роботи: процесор Intel Pentium 4 1,8 ГГц або аналогічний AMD; об'єм оперативної пам'яті 256 MB DDR; графічний процесор – інтегрований, 256 MB. Програмі потрібно дозволити активність в брандмауері, що встановлений у операційній системі.

### **Література**

1. Рунет сегодня: исследование российского интернета [Электронный документ]. Режим доступа: <http://civilfund.ru/mat/view/1>. Проверен 3.11.2013.
2. Родительский контроль // Журнал СНІР. – 2011. – № 11. – С. 104-105.
3. Родительский контроль // Журнал СНІР. – 2012. – № 64. – С. 99-110.