Лабораторна робота №3

Тема: Захист інформації засобами операційних систем. Налаштування власного профілю. Поняття батьківського контролю.

Мета: ознайомитися з способами захисту інформації засобами операційної системи; навчитися налаштовувати власний профіль та користуватися функцією батьківського контролю.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Використання надійного паролю є одним з найбільш важливих факторів захисту комп'ютера від несанкціонованого доступу.

Якщо ввійти в систему з правами адміністратора, то можливо встановити пароль для будь-якого облікового запису.

1. ***Пуск, Панель управления, Учетные записи пользователей***
2. Оберіть команду ***Создать пароль.***
3. Введіть пароль в поле ***Новый пароль***, а потім повторіть введення в поле ***Подтверждение пароля.***
4. Щоб скористатися підказкою паролю введіть її в поле ***Подсказка о пароле.***
5. Оберіть команду ***Создать пароль.***

Для того, щоб змінити існуючий пароль облікового запису, оберіть команду ***Изменение своего пароля.***

Захист файлів за допомогою шифрування дисків BitLocker

Шифрування дисків BitLocker використовується для захисту всіх файлів, що зберігаються на диску з встановленою ОС Windows (диск операційної системи) і на незнімних дисках (наприклад, внутрішніх жорстких дисках). Шифрування BitLocker To Go використовується для захисту всіх файлів, що зберігаються на знімних дисках (наприклад, зовнішніх жорстких дисках або USB флеш-пам'яті). На відміну від шифрованого файлової системи (EFS), що дозволяє зашифровувати окремі файли, BitLocker шифрує диск цілком. Користувач може входити в систему і працювати з файлами як звичайно, а BitLocker буде заважати зловмисникам, які намагаються отримати доступ до системних файлів для пошуку паролів, а також до диску шляхом вилучення його з даного комп'ютера та інсталяції в інший.

BitLocker автоматично шифрує всі файли, що додаються на зашифрований диск. Файли будуть зашифровані тільки при зберіганні на зашифрованому диску. При їх копіюванні на інший диск або комп'ютер вони будуть розшифровані. При наданні загального доступу до файлів по мережі вони будуть зашифровані на зашифрованому диску, але авторизовані користувачі зможуть отримувати до них доступ звичайним чином. При шифруванні диска з ОС BitLocker перевіряє комп'ютер при завантаженні на наявність можливих загроз безпеки (наприклад, змін в BIOS або файлах завантаження). При виявленні загрози безпеці BitLocker заблокує диск з ОС. Щоб розблокувати його, потрібно спеціальний ключ відновлення BitLocker. Переконайтеся, що цей ключ створений при першому запуску BitLocker. В іншому випадку доступ до файлів може бути втрачений. Якщо комп'ютер оснащений модуля TPM (TPM), BitLocker використовує його для запечатування ключів розблокування зашифрованого диска з ОС. Призавантаженні комп'ютера BitLocker запитує в модуля TPM ключі для доступу до диска і розблокує його. Зашифровані диски (незнімні або знімні) можна розблокувати за допомогою пароля або смарт-

карти або налаштувати автоматичну розблокування дисків при вході в систему.

BitLocker завжди можна відключити або тимчасово (призупинивши його), або на постійній основі (розшифрувавши диск).

Примітка.

• Можливість шифрувати дані на дисках з використанням шифрування BitLocker доступна не в усіх випусках операційної системи Windows.

Включення BitLocker

1. ***Пуск, Панель управления, Система и безопасность, Шифрование диска BitLocker***
2. Клацніть ***Включить BitLocker***. Відкриється майстер настройки BitLocker. Дотримуйтесь

інструкцій майстра. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

Відключення або тимчасове призупинення BitLocker

1. ***Пуск, Панель управления, Система и безопасность, Шифрование диска BitLocker***
2. Виконайте одну з таких дій.

Щоб тимчасово призупинити BitLocker, клацніть ***Приостановить защиту*** і натисніть кнопку ***Да***.

Щоб відключити BitLocker і розшифрувати диск, послідовно клацніть ***Выключить BitLocker*** і ***Расшифровать диск.***

Поняття захисту системи

Захист системи - це компонент, який регулярно створює і зберігає інформацію про системних файлах і параметрах комп'ютера. Захист системи також зберігає попередні версії змінених файлів. Ці файли зберігаються в точках відновлення, які створюються безпосередньо перед значущими системними подіями, такими як установка програми або драйвера пристрою. Вони також створюються автоматично раз на тиждень, якщо за попередній тиждень не було створено інших точок відновлення, проте можна створювати точки відновлення вручну в будь-який час.

Захист системи автоматично включена для диска, на якому встановлена ОС Windows. Захист системи можна включити тільки для дисків, відформатованих з використанням файлової системи NTFS.

Існує два способи скористатися перевагами захисту системи.

• Якщо комп'ютер працює повільно або з помилками, то за допомогою відновлення системи можна відновити стан системних файлів і параметрів комп'ютера на попередній момент часу з використанням точки відновлення.

• Якщо файл або папка були випадково змінені або видалені, можна відновити їх попередню версію, яка зберігається як частина контрольної точки відновлення.

Відновлення системи використовує точки відновлення для повернення системних файлів і параметрів до стану на певний момент часу, не впливаючи на особисті файли. Знімки автоматично створюються щотижня, а також перед значними системними подіями, такими як установка програм або драйверів пристроїв. Точку відновлення також можна створити вручну.

Відновлення системи дозволяє відновити стан системних файлів комп'ютера на попередній моменту часу. Це дозволяє скасувати зміни, внесені в систему комп'ютера, не зачіпаючи особисті файли, такі як електронна пошта, документи або фотографії.

Іноді в результаті установки програми або драйвера виникають несподівані зміни в комп'ютері або спостерігається непередбачувана поведінка ОС Windows. Зазвичай видалення програми або драйвера дозволяє усунути проблему. Але якщо видалення не призвело до усунення проблеми, то можна спробувати відновити стан системи комп'ютера на момент часу в минулому, коли все працювало належним чином.

Зберігаються на жорстких дисках резервні копії образу системи можна використовувати для відновлення системи так само, як і точки відновлення, створені захистом системи.

Відновлення системи не призначене для архівації особистих файлів, тому з його допомогою неможливо відновити видалені або пошкоджені особисті файли. Необхідно регулярно здійснювати архівування своїх особистих файлів і важливих даних за допомогою програми архівування.

Засіб відновлення системи регулярно відстежує зміни в системних файлах комп'ютера і за допомогою функції, званої захист системи, створює точки відновлення. Захист системи включена за замовчуванням на тому диску, де встановлена ОС Windows. Захист системи можна включити і для інших дисків.

Захист системи не можна включити для диска, відформатованого з використанням файлових систем FAT або FAT32.

1. ***Пуск, Панель управления, Система и безопасность, Система.***

2. В області ліворуч виберіть ***Защита системы***. При появі запиту пароля адміністратора або

підтвердження, введіть пароль або надайте підтвердження.

3. В області ***Параметры защиты*** клацніть диск і виберіть ***Настроить***.

4. Виберіть один із зазначених нижче параметрів.

Щоб забезпечити відновлення параметрів системи і попередніх версій файлів, клацніть ***Восстановить параметры системы и предыдущие версии файлов***.

Щоб забезпечити відновлення тільки попередніх версій файлів, клацніть ***Восстановить только предыдущие версии файлов.***

5. Натисніть кнопку ***ОК***, а потім ***ОК*** ще раз.

При відключенні захисту системи для диска всі точки відновлення цього диска видаляються. Системні дані на диску можна буде відновлювати тільки після повторного включення захисту системи і створення нової точки відновлення. Відключення захисту системи також видаляє всі попередні версії файлів, збережених для цього диска.

Попередні версії - це копії файлів і папок, які ОС Windows, автоматично зберігає з точками відновлення.

1. ***Пуск, Панель управления, Система и безопасность, Система.***
2. В області ліворуч виберіть ***Защита системы***. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.
3. В області ***Параметры защиты*** клацніть диск і виберіть ***Настроить***.
4. Клацніть ***Отключить защиту системы***, натисніть кнопку ***ОК***, а потім натисніть кнопку ***ОК*** ще раз.

Захист доступу до мережі (NAP) - це платформа для мережевого адміністратора, що забезпечує безпеку мережі. При підключенні до корпоративної мережі, що використовує NAP, комп'ютер перевіряється на наявність оновлених версій необхідного програмного забезпечення та параметрів. Якщо якийсь з компонентів відсутній або застарілий, він може автоматично оновитися. При цьому доступ до мережі може бути обмежений, але зазвичай це відбувається швидко, після чого повний доступ до мережі поновлюється.

Запобігання виконання даних

DEP - це засіб безпеки, яке допомагає захистити комп'ютер від вірусів та інших загроз безпеці. Компонент DEP призначений для спостереження за програмами, зокрема за тим, як вони використовують системну пам'ять. Якщо програма намагається виконати код, званий виконуваним, з пам'яті невірним способом, засіб DEP закриває програму. Компонент DEP автоматично перевіряє основні програми ОС Windows. При необхідності можна підвищити ступінь захисту, включивши перевірку всіх програм.

Якщо при використанні рекомендованих значень параметрів безпеки антивірусна програма не виявила загрози, комп'ютер, можливо, не піддавався атаці. У цьому випадку програма при включеному засобі DEP може працювати неправильно. Зверніться до виробника програмного забезпечення за версією програми, сумісної з DEP, або виконайте оновлення програми, перш ніж змінювати параметри DEP.

Програми svchost.exe та explorer.exe є частинами операційної системи Windows. Якщо засіб DEP закриває їх або інші служби Windows, причиною можуть бути невеликі програми, такі як розширення, створені іншими видавцями програмного забезпечення та працюють усередині Windows. Якщо програма встановлена недавно і компонент DEP закриває програми під управлінням ОС Windows, зверніться до виробника програмного забезпечення за оновленою версією, сумісної з DEP, або спробуйте видалити програму.

DEP - це програмний засіб Windows. Деякі процесори також надають апаратний засіб DEP під різними назвами. Ці процесори використовують апаратну технологію заборони програмам виконувати код із захищених областей пам'яті. Якщо процесор не підтримує апаратне засіб DEP, Windows буде використовувати для захисту комп'ютера програмний засіб DEP.

Пароль як засіб захисту окремих файлів

В ОС Windows не можна захистити файл або папку з допомогою пароля. Однак у деяких програмах для ОС Windows, підтримується захист окремих файлів за допомогою пароля.

Існують і інші способи захисту файлів і папок у Windows. Можна зашифрувати файли за допомогою шифрувальної файлової системи (EFS), вручну визначити користувачів, що мають права на доступ до файлів і папок за допомогою дозволів, а можна приховати їх. Можна вибрати метод захисту в залежності від необхідного для файлів і папок рівня безпеки. Шифрування є найбільш безпечним методом захисту, а приховування - найменш безпечним.

Шифрована файлова система (EFS)

Шифрована файлова система (EFS) - це компонент Windows, що дозволяє зберігати відомості на жорсткому диску в зашифрованому форматі. ***Шифрування*** - це найсильніший захист, який надає Windows, для захисту даних.

Деякі ключові властивості EFS:

• Шифрування - проста дія, для його включення досить встановити прапорець у властивостях файлу або папки.

• Можна вказати, кому саме дозволяється читати ці файли.

• Файли шифруються, коли вони закриваються, але при відкритті вони автоматично готові до використання.

• Якщо шифрувати файл більше немає необхідності, зніміть прапорець у властивостях файлу.

Опис захисту, забезпечуваного Захисником Windows, в реальному часі

Функція захисту в реальному часі повідомляє користувача, якщо шпигунська або інша небажана програма намагається встановити або запустити на комп'ютері. В залежності від рівня оповіщення, користувач може застосувати до цієї програми одну з наступних дій.

• *Помістити в карантин.* Переміщує відповідну програму в інше місце на комп'ютері і перешкоджає її запуску, доки вона не буде відновлена або видалена.

• *Видалити.* Остаточно видаляє програму з комп'ютера.

• *Дозволити.* Додає програму в список дозволених програм Захисника Windows, і дозволяє її запуск. Захисник Windows, не буде оповіщати про потенційну загрозу конфіденційності або безпеці комп'ютера, яку може представляти ця програма. Додавайте програму до списку дозволених тільки в тому випадку, якщо довіряєте цій програмі і її видавцеві.

Ви можете вибрати програми і параметри, за якими повинен спостерігати Захисник Windows, проте рекомендується використовувати всі варіанти захисту в реальному часі, які називаються агентами. Призначення кожного з агентів наведено нижче.

Завантажені файли та вкладення. Відстежує файли і програми, призначені для роботи з веб-браузерами. Дані файли можуть завантажуватися, встановлюватися або запускатися самим браузером. До складу цих файлів можуть входити шпигунські та інші небажані програми і встановлюватися без відома користувача.

Програми, що працюють на комп'ютері. Контролює запуск програм і всі виконувані ними операції протягом їх роботи. Шпигунські та інші небажані програми можуть використовувати уразливості встановлених програм для запуску шкідливих та інших небажаних програм без відома користувача. Наприклад, шпигунські програми можуть запускатися у фоновому режимі при відкритті часто використовуваної програми. Захисник Windows, спостерігає за програмами і оповіщає користувача у разі виявлення будь-яких підозрілих дій.

Захист певних файлів і папок від загального доступу в домашній групі

Користувач, який створює домашню групу або приєднується до неї, вибирає бібліотеки, які будуть доступні іншим членам домашньої групи. Загальний доступ до бібліотек спочатку надається з правом доступу ***Чтение***, яке дозволяє переглядати або прослуховувати вміст бібліотеки, але не дозволяє вносити зміни у файли. Рівень доступу пізніше можна налаштувати, а також виключити певні файли і папки із загального доступу.

Виключення бібліотеки із загального доступу (при створенні домашньої групи або

приєднання до неї)

1. ***Пуск, Панель управления, Сеть и Интернет, Домашняя группа***

2. Виконайте одну з таких дій.

- Щоб створити нову домашню групу, клацніть ***Создать домашнюю группу.***
- Щоб приєднатися до існуючої домашньої групи, клацніть ***Присоединиться.***

3. На наступній сторінці майстра зніміть прапорці для всіх бібліотек, які потрібно виключити з загального доступу.

4. Натисніть кнопку ***Далее***, а потім кнопку ***Готово***.

Виключення бібліотеки із загального доступу (після створення домашньої групи або приєднання до неї)

1. ***Пуск, Панель управления, Сеть и Интернет, Домашняя групп.***

2. Зніміть прапорці для всіх бібліотек, які потрібно виключити із загального доступу, і натисніть кнопку ***Сохранить изменения.***

Виключення певних файлів і папок із загального доступу (після створення домашньої групи або приєднання до неї)

1. Натисніть кнопку ***Пуск***, виберіть ім'я користувача.

2. Перейдіть до файлу або папки, які потрібно виключити із загального доступу, і виберіть файл або папку.

3. Виконайте одну з таких дій.

Щоб виключити файл або папку із загального доступу для всіх, на панелі інструментів натисніть кнопку ***Общий доступ*** для та виберіть пункт ***Никто из пользователей***.

Щоб надати спільний доступ до файлу або папці деяким (але не всім) користувачам, на панелі інструментів натисніть кнопку ***Общий доступ для***, виберіть пункт ***Конкретные пользователи***, виберіть тих користувачів, яким потрібно надати доступ, і натисніть кнопку ***Добавить***. По завершенні натисніть кнопку ***Доступ***.

Щоб змінити рівень доступу до файлу або папки, на панелі інструментів натисніть кнопку ***Общий доступ для*** та виберіть пункт ***Домашняя группа (чтение)*** або ***Домашняя группа (чтение и запись).***

Пристрій читання відбитків пальців в Windows

Замість пароля для входу в цю версію Windows, можна використовувати пристрій читання відбитків пальців.

Пристрій читання відбитків пальців - це пристрій, призначений для ідентифікації користувачів по відбитках пальців. Це пристрій сканує зображення відбитка пальця користувача та зберігає його копію. Потім для ідентифікації користувача, наприклад, при вході на веб-сайт або в систему для Windows, виконується сканування відбитку пальця і його порівняння із збереженою версією.

Можна використовувати вбудований пристрій читання відбитків пальців, встановлений в деяких моделях ноутбуків, або придбати окремий пристрій і підключити його до комп'ютера.

Якщо у вас кілька пристроїв читання відбитків пальців або потрібно замінити один на інший, то може знадобитися зчитати і зберегти (це часто називається записати) відбитки пальців перед початком використання пристрою читання з Windows. Це необхідно, тому деякі пристрої читання відбитків пальців зберігають відбитки пальців у різних форматах і вони не можуть бути прочитані іншими сканерами.

Безпека і безпечна робота на комп'ютері

Існують різні способи захисту комп'ютера від можливих загроз безпеки.

• Брандмауер. Брандмауер захищає комп'ютер, запобігаючи доступ до нього хакерів і шкідливих програм.

• Центр оновлення Windows. ОС Windows може регулярно перевіряти наявність оновлень для комп'ютера і автоматично їх встановлювати.

• Захист від вірусів. Антивірусне програмне забезпечення допомагає захистити комп'ютер від вірусів, черв'яків і інших погроз безпеці.

• Захист від шпигунських та інших шкідливих програм. Антишпигунське програмне забезпечення допомагає захистити комп'ютер від шпигунських програм та іншого небажаного програмного забезпечення.

Брандмауер. Брандмауер - це програма або пристрій, який перевіряє дані, що надходять з локальної мережі або Інтернету, а потім або відхиляє її, або пропускає в комп'ютер, в залежності від параметрів брандмауера. Таким чином, брандмауер допомагає запобігти доступ хакерів і шкідливих програм до комп'ютера.

Брандмауер Windows, вбудований в Windows, і включається автоматично.

Якщо на комп'ютері використовуються такі програми, як програма передачі миттєвих повідомлень або мережеві ігри, якій потрібно отримувати дані з Інтернету або локальної мережі, брандмауер запитує про блокування або дозволі підключення. Якщо користувач дозволяє підключення, брандмауер Windows, створює виняток, щоб не турбувати користувача запитами, коли в майбутньому цій програмі знадобляться дані.

Захист від вірусів. Віруси, хробаки та троянські коні - це програми, створені хакерами, які використовують Інтернет для зараження комп'ютерів. Віруси та хробаки можуть розмножуватися від комп'ютера до комп'ютера, а троянський кінь потрапляє до комп'ютера, сховавшись у легальних програмах. Деструктивні віруси, хробаки та троянські програми можуть стерти інформацію з жорсткого диска або повністю вивести з ладу. Інші не завдають прямої шкоди, але знижують продуктивність і стабільність комп'ютера.

Антивірусні програми перевіряють електронну пошту та інші файли комп'ютера на наявність вірусів, хробаків і троянських програм. При виявленні антивірусна програма або у карантин (ізолює) або повністю видаляє до нанесення шкоди комп'ютеру та файлам.

ОС Windows не має вбудованої антивірусної програми, але виробник комп'ютера може встановити інші. Якщо антивірусна програма відсутня, відвідайте веб-сайт постачальників програм по забезпеченню безпеки Windows для пошуку антивірусної програми.

Так як нові віруси з'являються щодня, дуже важливо вибрати антивірусну програму з можливістю автоматичного оновлення. При оновленні антивірусне програмне забезпечення додає нові віруси в список перевірки, захищаючи комп'ютер від нових атак. Застарілий комп'ютер стане вразливим до нових загроз. Оновлення зазвичай вимагають щорічної підписки. Підтримуйте підписку для регулярного отримання оновлень.

• Якщо антивірусне програмне забезпечення не використовується, комп'ютер схильний пошкодження шкідливими програмами. Є також ризик заразити вірусами інші комп'ютери.

Захист від шпигунських програм. Шпигунські програми можуть відображати рекламу, збирати особисті відомості та змінювати параметри комп'ютера, зазвичай без отримання на те дозволу.

Наприклад, шпигунські програми можуть встановлювати небажані панелі інструментів, посилання або уподобання в браузер, змінювати домашню сторінку або часто відображати спливаючу рекламу. Деякі шпигунські програми не проявляють видимих симптомів, але таємно збирають важливі відомості, такіяк відвідувані сайти або набраний текст. Більшість шпигунських програм інсталюються разом із безплатним програмним забезпеченням, але в деяких випадках спричиняє зараження звичайне відвідування веб-сайту.

Для захисту комп'ютера від шпигунських програм, користуйтеся анти шпигунське програмне забезпечення. Дана версія ОС Windows має вбудовану анти шпигунську програму «Захисник Windows», включену за умовчанням. Захисник Windows, попереджає про шпигунська програма намагається інсталювати себе на комп'ютер. Захисник також може шукати на комп'ютері шпигунські програми та видаляти їх.

Оскільки з'являються нові шпигунські програми кожен день, Windows Defender, повинен регулярно оновлювати, щоб виявляти і захищати комп'ютер від найновіших загроз. Захисник Windows,

оновлюється по мірі необхідності разом з оновленням Windows. Для досягнення найвищого рівня захисту увімкніть автоматичне оновлення Windows.

Автоматичне оновлення для Windows. Корпорація Майкрософт регулярно пропонує важливі оновлення Windows, для захисту комп'ютера від нових вірусів та інших загроз безпеці. Для якнайшвидшого отримання оновлень, увімкніть автоматичне оновлення. У цьому випадку не потрібно хвилюватися, що критичні оновлення для Windows можуть бути пропущені.

Оновлення завантажуються у фоновому режимі при підключенні до Інтернету. Оновлення встановлюються в 03:00, якщо не задано інший час. Якщо ви вимикаєте комп'ютер, можна інсталювати перед вимкненням. В іншому випадку ОС Windows інсталює наступного разу при запуску комп'ютера.

Включення автоматичного оновлення

1. ***Пуск, Панель управления, Система и безопасность, «Центр обновления Windows».***
2. Клацніть ***Изменить параметры.***
3. Переконайтеся, що вибрано інсталяція оновлень (рекомендується). ОС Windows буде встановлювати на комп'ютері важливі оновлення по мірі їх появи. Важливі оновлення забезпечують суттєві переваги, наприклад підвищення безпеки і надійності.
4. У групі ***Рекомендуемые обновления*** встановіть прапорець ***Получать рекомендуемые обновления таким же образом, как и важные обновления*** та натисніть кнопку ***ОК***. Рекомендовані оновлення можуть усувати менш істотні проблеми і робити використання комп'ютера більш зручним. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

Стандартна обліковий запис

При вході в систему Windows, призначає користувачеві певний рівень прав, що залежить від типу облікового запису. Є три типи облікових записів користувачів: «стандартна», «адміністратор» та «гість».

Хоча обліковий запис адміністратора надає повний контроль над комп'ютером, використання стандартної облікового запису користувача може сприяти забезпеченню більш високого рівня безпеки комп'ютера. Таким чином, інші люди (або хакери), отримавши доступ до комп'ютера, на якому користувач увійшов в систему зі стандартним обліковим записом, не зможуть зіпсувати параметри безпеки комп'ютера або облікові записи інших користувачів. Увійшовши в систему, користувач може перевірити тип свого облікового запису, виконавши наступні дії.

1. ***Пуск, Панель управления, Учетные записи пользователей и семейная безопасность.***

Тип облікового запису відображається під іменем користувача. Якщо обліковий запис відноситься до типу Адміністратор, то поточний користувач увійшов як адміністратор.

2. Усі облікові записи на комп'ютері можна переглянути, клацнувши ***Управление другой учетной записью***. При появі запиту пароля адміністратора або підтвердження, введіть пароль або надайте підтвердження.

При цьому виводяться всі облікові записи користувачів і їх типи.

Зазвичай за домашніми комп’ютерами працюють кілька членів сім’ї. У тому випадку, якщо користувачем домашнього комп’ютера є тільки його власник, йому не варто хвилюватися про захист файлів і встановлених параметрів операційної системи. Буде достатньо лише встановити безпечний пароль і забути про багато проблем. Але якщо один комп’ютер використовують кілька людей, то варто подумати про прийняття додаткових заходів захисту персональної інформації кожного окремо взятого користувача. Ви можете створити для всіх користувачів окремі облікові записи з обмеженими правами, навіть якщо один або декілька користувачів буде дуже рідко використовувати свій обліковий запис. Також слід видаляти облікові записи тих користувачів, які вже не працюють на цьому комп’ютері. Але як же бути, якщо вашим комп’ютером користується ще й дитина? Для цього був створений компонент, який називається «Батьківський контроль».

За допомогою цього компонента ви можете використовувати рейтинг для того, щоб контролювати, в які ігри може грати ваша дитина, додати тимчасові обмеження, за допомогою яких діти зможуть користуватися комп’ютером тільки в певні години, а також блокувати доступ до деяких програм, які діти не повинні відкривати. Компонент «Батьківський контроль» з’явився ще в операційній

системі Windows Vista. У Windows 7 з функціоналу батьківського контролю були виключені компоненти веб-фільтрації та звіту про активність. Тепер їх можна завантажити з веб-сайту Windows Live, встановити і додати в ту службу батьківського контролю, яка вже використовується. Функціонал батьківського контролю доступний у всіх редакціях Windows 7. Далі в цьому керівництві будуть детально описані всі дії, які можна виконувати з «Батьківським контролем», крім функціоналу додаткових компонентів, який завантажується від інших постачальників послуг.

Використання батьківського контролю

Перед тим як встановити батьківський контроль, створіть обліковий запис для вашої дитини. Про способи створення облікових записів я детально розповідав в статті Робота з обліковими записами користувачів в Windows 7 – докладне керівництво (Частина 1). Після того як обліковий запис буде створена, можна приступати до установки обмежень використання комп'ютера для дитини.

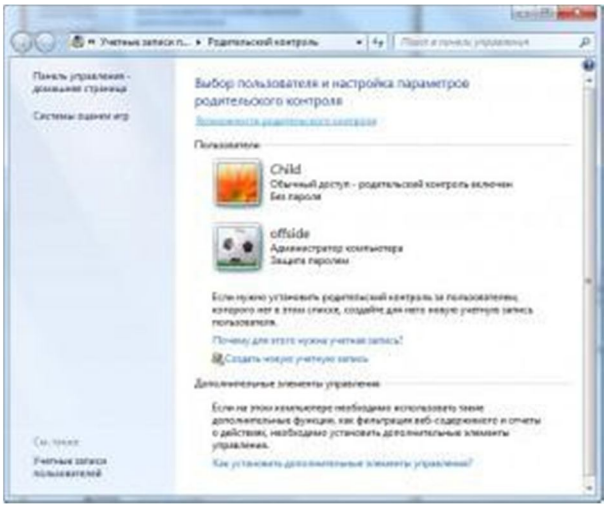
Відкриття компонента «Батьківський контроль»

Для початку відкрийте вікно «Батьківський контроль». Це можна зробити наступним чином:

Натисніть на кнопку «Пуск» для відкриття меню, в поле пошуку або введіть Родитель та відкрийте в знайдених результатах;

Скористайтеся комбінацією клавіш + R для відкриття діалогу "Виконати". У діалоговому вікні «Виконати», в полі «Відкрити» введіть %systemroot%\system32\control.exe /name Microsoft.ParentalControls і натисніть на кнопку «ОК»;

Натисніть на кнопку «Пуск» для відкриття меню, відкрийте «Панель управління», зі списку компонентів панелі управління оберіть "Батьківський контроль»;

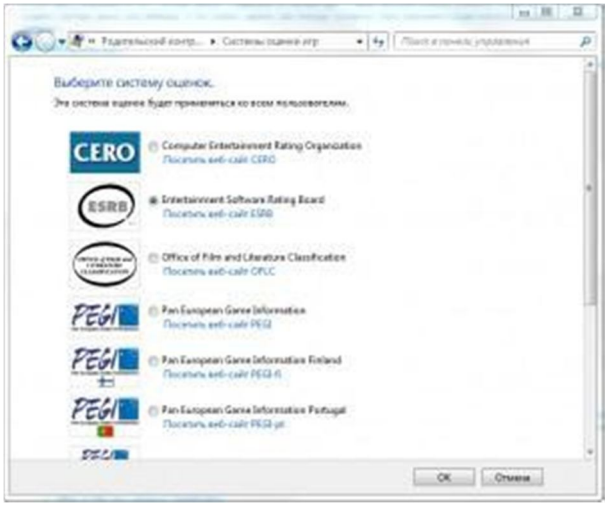


Вікно «Батьківський контроль» зображено на наступному скріншоті:

У цьому вікні відображаються всі облікові записи, зроблені на комп'ютері, а також додаткові елементи управління, якщо вони були встановлені. Якщо ви ще не встигли створити обліковий запис для дитини, то це можна зробити за допомогою основного вікна компонента батьківського контролю. Натисніть на посилання «Створити новий обліковий запис».

Система оцінки ігор

У лівій області вікна «Батьківського контролю» перейдіть за посиланням «Системи оцінки ігор» для того, щоб вибрати ту систему, яка буде застосовуватися до всіх користувачів. Діалог вибору системи оцінювання відображено на наступному скріншоті:



Системи оцінки і категорії для ігор визначаються спеціальними комісіями, які створюють рекомендації по вмісту ігор для різних країн. В основному, у всіх системах присутні вікові категорії для ігор. Перед тим як ігри надходять на прилавки магазинів, ці комісії уважно вивчають вміст ігор і дають свої рецензії.

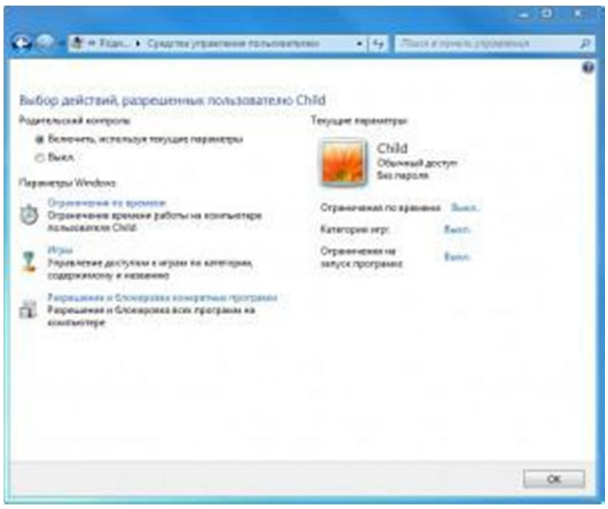
В операційній системі Windows 7 ви можете встановити одну з десяти можливих систем оцінок, а саме:

1. Computer Entertainment Rating Organization;
2. Entertainment Software Rating Organization;
3. Office of Film and Literature Classification;
4. Pan European Game Information;
5. Pan European Game Information Finland;
6. Pan European Game Information Portugal;
7. Pan European Game Information і British Board of Film Classification;
8. Unterhaltungssoftware Selbstkontrolle;
9. Комісія з класифікації програмного забезпечення для комп'ютерів;
10. Комісія з оцінки ігор.

Якщо ви не знаєте, яку систему вам потрібно вибрати, то можете перейти по посиланню, розташованої під назвою системи на веб-сайт цієї комісії, і докладно познайомитися з їх класифікацією та вимогами до ігор. Найбільш поширеними системами оцінки є ESRB і PEGI. Я рекомендую вибрати систему ESRB, тому що в цій системі ви можете вибрати безліч коротких описів, які використовуються для позначення вмісту, який може виявитися небажаним для дітей. На наступному скріншоті ви можете побачити приклади значків різних систем оцінок для однієї і тієї ж гри:

Але, незважаючи на описи до гри, які встановила комісія, найкраще подивіться самі, чи варто забороняти дитині грати в цю гру, оскільки думка фахівців може виявитися упередженим.

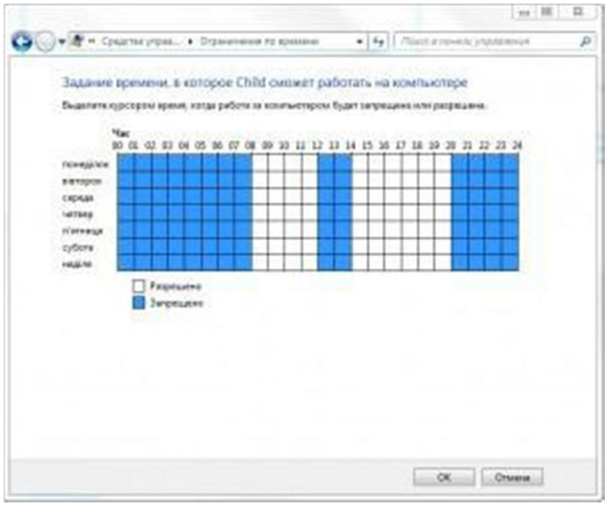
Вибравши систему оцінки ігор, натисніть на кнопку «ОК» для того щоб назад перейти в головне вікно «Батьківського контролю». У головному вікні натисніть на значку облікового запису дитини, для якого будуть застосовуватися обмеження використання комп'ютера. Після вибору облікового запису ви перейдете у вікно «Засоби керування користувачами». Це вікно допоможе вам визначити час роботи комп'ютера, обмежити запуск ігор, а також блокувати запуск програм для вибраного користувача. Вікно засобів управління користувачами відображено нижче:



Для включення батьківського контролю над обліковим записом дитини в області «Батьківський контроль» встановіть перемикач на опції «Включити, використовуючи поточні параметри». Після того як цей пункт буде активовано, ви зможете настроювати параметри батьківського контролю.

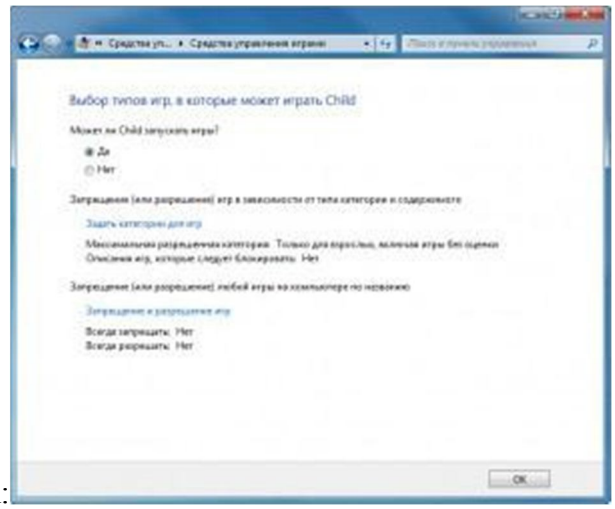
Обмеження за часом

Вікно «Обмеження по часу» призначено для визначення часу, який дозволяється дітям для використання комп'ютера. Тут кожен рядок відповідає за день тижня, а кожен стовпець за годину. Ви можете встановити годинник, які дозволяються для доступу на кожен день тижня, у зв'язку з чим, дитина не зможе ввійти в систему протягом певного періоду часу. Натиснувши лівою кнопкою миші на будь-який з осередків, цю годину буде заблокований. Знизу відображена легенда, де ви можете дізнатися, що означають ті позначки, які ви встановлюєте. Вікно обмеження за часом ви можете побачити нижче:



Обмеження на ігри

За допомогою вікна «Засоби керування іграми» ви можете дозволити або заборонити доступ відразу до всіх ігор, встановленим на комп'ютері, обмежити доступ до ігор на основі вікової оцінки або категорії ігор, а також заблокувати або дозволити доступ до певних ігор. Вікно «Засоби керування

іграми» відображує на наступному скріншоті: 

Блокування доступу до всіх ігор

Ви можете повністю відключити для користувача можливість доступу до ігор. Для цього в розділі «Чи може% USERNAME% запускати ігри» встановіть перемикач на опції «Ні». У тому випадку, якщо перемикач встановлений на опцію «Так», користувач зможе запускати ігри, а вам для установки обмежень, потрібно буде налаштувати наступні два розділи, щоб визначити в які саме ігри зможе грати ваша дитина.

Блокування доступу до ігор на підставі категорії та вмісту ігор

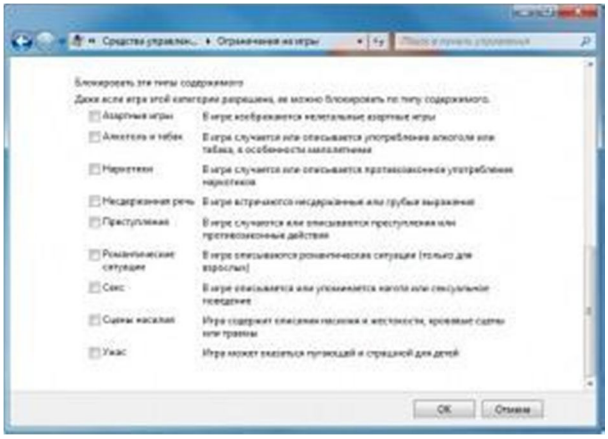
Замість того щоб повністю заблокувати доступ до встановлених на комп'ютер ігор, ви можете дозволити або заборонити дитині відкривати ігри певного типу. Для цього у вікні «Засоби керування іграми» перейдіть по посиланню «Поставити категорії ігор».

У вікні «Обмеження на ігри» ви можете встановити перемикач на опцію «Блокувати ігри, категорія яких не зазначена» для того, щоб дитина не змогла запускати ті ігри, для яких комісія з оцінки ігор категорію не вказала. Трохи нижче, в розділі «В ігри з якою оцінкою може грати% USERNAME%?» Встановіть перемикач напроти тієї категорії, яку хочете зробити максимально допустимої для користувача, якому ви обмежуєте доступ. Наприклад, як показано на наступному скріншоті, якщо встановити перемикач біля категорії «Старше 10 років», даний користувач зможе грати в ігри, тільки з категоріями «Для дітей», «Для всіх», а також «Старше 10 років». У свою чергу, ігри, для яких встановлена категорія «Для підлітків», «Для старшого віку» і «Тільки для дорослих» дитина грати не зможе.

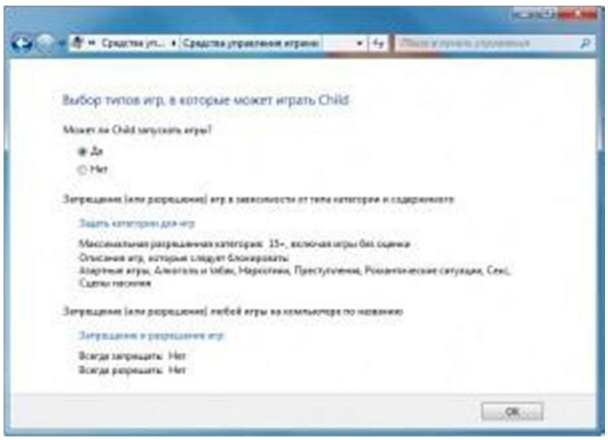
На першому прикладі можна побачити обмеження на ігри для системи оцінки ESRB:

Якщо у вікні «Системи оцінки ігор» ви оберете систему CERO, то в діалозі «Обмеження на ігри» оцінки будуть виглядати наступним чином:

Крім блокування системи ігор, ви також можете заборонити дитині грати в ті ігри, вміст яких не повинно потрапляти йому на очі. Для цього у вікні «Обмеження на ігри» знайдіть розділ «Блокувати ці типи вмісту» і в докладному переліку типів вмісту встановіть прапорці навпроти того типу, який потрібно виключити. Якщо ви не хочете, щоб ваша дитина грав в ігри, в яких присутня будь-якого виду насильства, азартні ігри та нецензурна лексика, установіть відповідні прапорці. У цьому випадку, дитина не зможе запустити гру навіть в тому випадку, якщо вона входить в той склад вікової категорії, яка доступна.



Після натискання на кнопку «ОК», ви повернетеся до вікна «Коштів управління іграми», де ви можете побачити ті настройки, які були вказані у вікні «Обмеження на ігри». У деяких випадках для ігор не вказується вікова категорія і вміст. У такому випадку, ви можете самостійно додати категорію і перелік типів вмісту, про що буде розказано в одній з наступних статей.

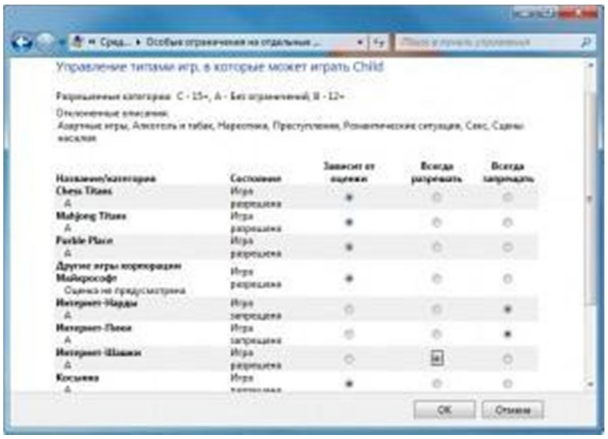


Блокування доступу до певних ігор

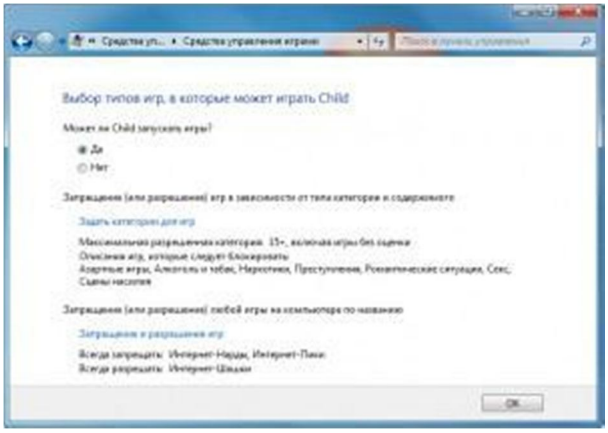
Крім способів блокування доступу до ігор зазначених вище, ви можете точно налаштувати управління іграми засобами визначення обмежень для тих ігор, які вже встановлені на вашому комп'ютері. Для цього у вікні «Засоби керування іграми» перейдіть по посиланню «Заборона і дозвіл ігор». У вікні «Особливі обмеження на окремі ігри» відобразиться таблиця, в якій міститься така інформація:

- Найменування всіх ігор, встановлених на вашому комп’ютері, а також їх категорії;
- Стан гри, де можна побачити дозволена або заборонена дана гра;
- Три стовпця з перемикачами для вибору дозволів.

Для того щоб дозволити користувачеві запускати певну гру, яка вже встановлена на вашому комп’ютері, установіть перемикач на опції «Завжди дозволяти», а для того щоб заборонити – на опції «Завжди забороняти». Вікно особливих обмежень на окремі ігри відображує на наступному скріншоті:

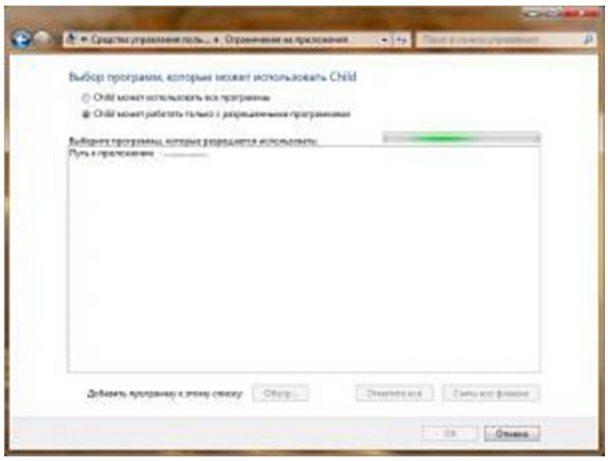


Після того як ви натиснете на кнопку «ОК», у вікні «Засоби керування іграми» ви зможете побачити зведену інформацію про всі обмеження, які були встановлені для даної користувача облікового запису.

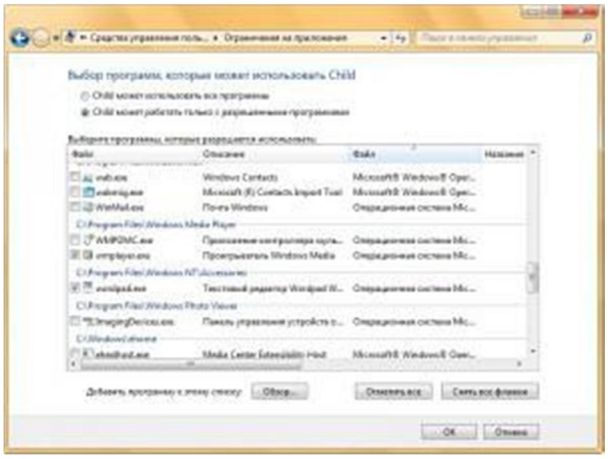


Обмеження на додатки

Крім блокування доступу до ігор та Обмеження користувача за часом, функціонал батьківського контролю операційної системи Windows 7 дозволяє навіть обмежувати доступ користувача до конкретних програм. Тобто ви можете заборонити дитині звертатися до програм, які не повинні його торкатися і бути впевненим в тому, що вам дитина буде відкривати тільки ті програми, які дозволені в списку. Для того щоб обмежити дитині доступ до програм у вікні «Засоби керування користувачем» перейдіть за посиланням «Дозвіл і блокування конкретних програм». Встановивши перемикач на опцію «% USERNAME% може працювати тільки з дозволеними програмами», операційна система сканує комп’ютер на наявність встановлених програм, як показано на наступному скріншоті:

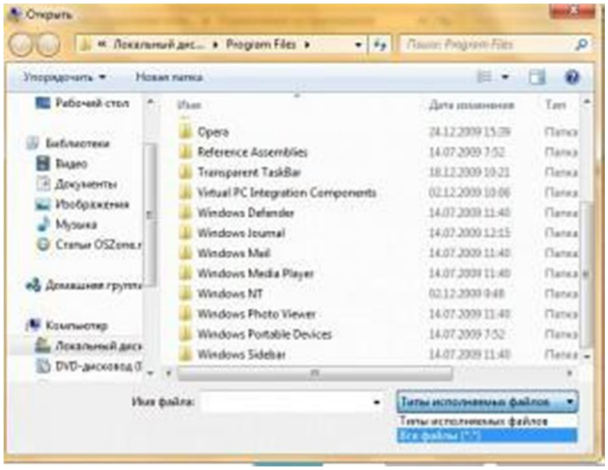


Після того як сканування буде закінчено, у вікні «Обмеження на додатки» ви побачите всі програми, які встановлені на вашому комп'ютері. Для того щоб користувачеві дозволити працювати з певною програмою, встановіть прапорець біля її найменування. Вікно «Обмеження на додатки» можна побачити на наступному скріншоті:

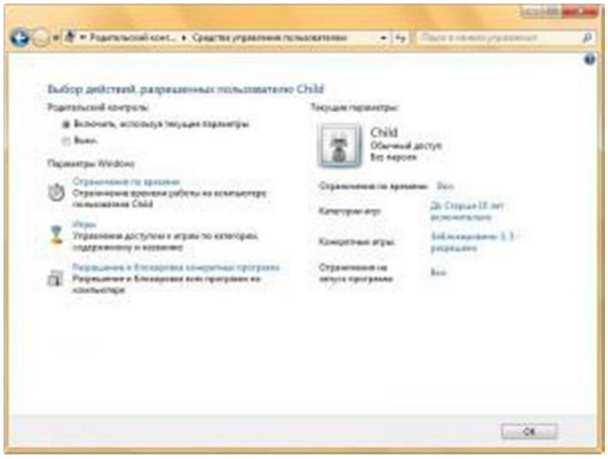


Після того як ви встановите прапорці біля всіх програм, якими може користуватися ваша дитина, до всіх інших програм доступ автоматично буде заблокований. Якщо ви не знайшли в списку якусь програму, то її можна додати до списку за допомогою кнопки «Обзор».

У діалоговому вікні «Відкрити», пересуваючись по дереву каталогів, відкрийте папку, яка містить потрібний файл. У діалоговому вікні будуть виведені всі типи виконуваних файлів. Після того, як потрібний файл буде знайдений, виділіть його, клацнувши на ньому лівою кнопкою миші, що помістить його ім'я в рядок для введення імені файлу і натисніть на кнопку «Відкрити».



Після того як ви визначите дозволу для всіх програм, встановлених на вашому комп'ютері, натисніть на кнопку «ОК». Батьківський контроль перемістить вас у вікно «Засоби керування користувачем», де ви зможете побачити коротку інформацію про ті обмеження, які були встановлені.



На цьому установка батьківського контролю, використовуючи штатні засоби, закінчується. У наступному розділі ви побачите роботу користувача, для якого були застосовані обмеження, використовуючи батьківський контроль Windows 7.

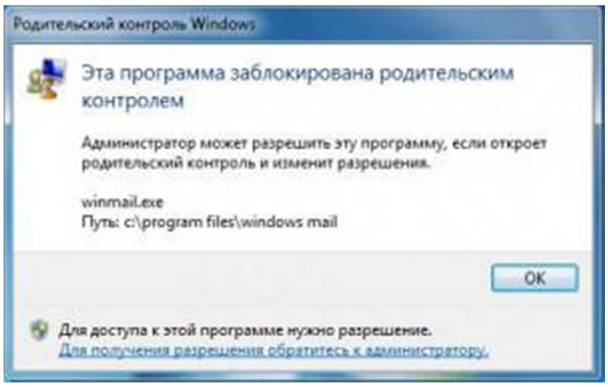
Робота користувача, на якого застосовується батьківський контроль

У цьому розділі ви можете побачити приклади всіх обмежень батьківського контролю «в дії», які можна застосувати для облікового запису вашої дитини.

Перш за все, якщо ви обмежили доступ до комп'ютера для дитини, то при спробі входу в свій обліковий запис у заборонений час, дитина побачить наступне попередження:

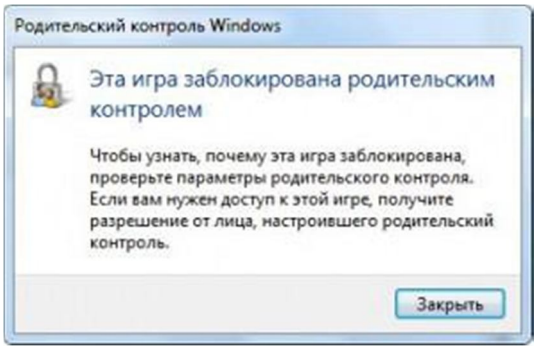
Тепер, як видно на попередньому скріншоті, ви можете бути впевнені, що ваша дитина зможе зайти у свій обліковий запис тільки у вказаний для нього час.

Після того як дитина зможе зайти у свій обліковий запис і спробує відкрити програму, для якого був заблокований доступ, він побачить таке повідомлення:

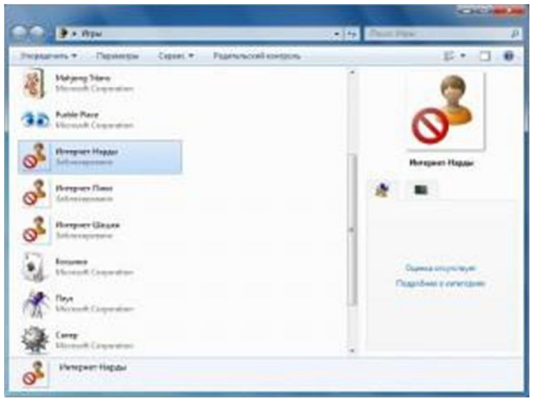


Побачивши це повідомлення, дитина не зможе запустити цю програму до тих пір, поки ви йому не дасте на це свою згоду.

При спробі відкрити гру, вікова категорія якої не входить в список дозволених, якщо вона заблокована по вмісту або якщо ви вручну її заблокували, при запуску з'явиться повідомлення батьківського контролю Windows:



Також, відкривши папку «Ігри», у того облікового запису, для якого застосовується батьківський контроль, на заборонених адміністратором іграх, дитина побачить значок, що свідчить про те, що доступ до цієї гри заблокований.



У цьому керівництві докладно описані всі штатні дії, які можна виконувати компонентом операційної системи Windows 7 – «Батьківським контролем». Існують також і інші програми Батьківського контролю, які можливо встановити на ОС.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

Користуючись інструкціями створити новий обліковий запис та налаштувати для нього батьківський контроль. Хід виконання описати у звіті, ілюструючи скріншотами.

1. З дозволу викладача ввійдіть в систему під обліковим записом «***Адміністратор***».
2. Створіть новий обліковий запис під іменем «***Дитина***».
3. Внесіть до нього зміни, обравши пункт «Установить родительський контроль».
4. Встановіть обмеження для часу роботи: дозвольте працювати на вихідні від 13.00 до 15.00, а в решту днів з 17.00 до 18.30.
5. Задайте категорію ігор «***Для детей***».
6. В пункті «***Запрещение и розрешение игр***» оберіть лише три гри, які дозволяються, до решти доступ закрийте.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Як встановити пароль для облікового захисту?
2. Як здійснюється захист файлів за допомогою шифрування дисків BitLocker?
3. Як здійснюється включення, призупинення роботи та відключення шифрування дисків BitLocker?
4. Що являє собою захист системи?
5. Що ви знаєте про захист доступу до мережі (NAP)?
6. Як реалізується в операційній системі запобігання виконання даних?
7. Опишіть захист, що забезпечується Захисником Windows, в реальному часі.
8. Що являє собою шифрована файлова система (EFS)?
9. Опишіть призначення, можливості, особливості налаштування та використання батьківського контролю, що забезпечується засобами операційної системи.
10. Назвіть та опишіть основні можливості захисту інформації засобами операційної системи.