

Практична робота №1

Захист інформації ПК, вінчестерів, локальних дисків, окремих каталогів та файлів

Мета: вивчити основи захисту інформації, яка знаходиться на ПК, основується на використанні захисту вінчестерів, локальних дисків та окремих каталогів.

Теоретичні відомості

Більшість комп'ютерів використовують файлові системи FAT, NTFS, HPFS. Перша використовується в операційних системах DOS та Windows 95, дві наступні використовуються в операційних системах Windows NT та OS/2.

Файлові системи NTFS, HPFS підтримують можливість розмежування користувачів на рівні файлів. Тобто кожний користувач має свої права доступу до кожного файлу, каталогу, диску, машини в цілому. Ці можливості підтримуються на рівні операційної системи, а права доступу встановлюються людиною, яка виконує функції системного адміністратора мережі.

Встановлення паролю на право включення комп'ютера. На кожному ПК є вбудована в нього система BIOS, що являє собою декілька низькорівневих процедур, що тестують комп'ютер після включення його живлення і запускають операційну систему. Більшість BIOS підтримують можливість завдання так званого пароля включення. Якщо пароль заданий, то комп'ютер виконає будь-яку операцію тільки після правильної вказівки пароля.

Для того, щоб задати пароль BIOS, необхідно при завантаженні комп'ютера, коли в правому нижньому кутку з'явиться напис Press DEL to enter Setup, натиснути клавішу DELETE (або іншу вказану), після чого слідувати підказкам, що з'являються при виділенні якого-небудь пункту меню. Розглянемо механізм завдання пароля BIOS для AWARD BIOS і AMI BIOS. При цьому необхідно мати на увазі, що при роботі з BIOS необхідно дотримуватися граничної обережності, оскільки неправильна настройка може негативно позначитися на функціонуванні комп'ютера або навіть привести до виходу з ладу деяких його вузлів.

Існує 2 типи паролів, які можна задавати в BIOS, - пароль на завантаження комп'ютера і на завантаження меню Setup BIOS.

Завдання пароля AWARD BIOS. Спершу розглянемо, як задається пароль в BIOS виробництва Award. При завантаженні комп'ютера необхідно натиснути клавішу Delete, після чого можна вибрати один з двох варіантів завдання пароля:

1. Set User Password (Встановити пароль користувача). Він може задаватися або на вхід в меню Setup BIOS, або на вхід в Setup і завантаження комп'ютера. Для того, щоб вибрати будь-який з вище перелічених методів блокування, необхідно в меню Advanced BIOS Features вибрати рядок Password Check. Потім після натиснення клавіші Enter у вікні, що з'явилося, слід виділити або Setup (тобто пароль тільки не Setup BIOS), або System (тобто пароль на завантаження системи і Setup BIOS);

2. Set Supervisor Password (Встановити пароль супервізора). Має пріоритет перед паролем користувача. Решта функцій і настройок такі ж, як у User Password.

Завдання пароля AMI BIOS. Виклик вікна настройок AMI BIOS здійснюється натисненням клавіші F2 в процесі тестування устаткування після включення комп'ютера. Тут для завдання пароля необхідно вибрати вкладку Security, в якій доступні Set Supervisor Password і Set User Password.

Характерною особливістю AMI BIOS є те, що користувач, знаючий Supervisor Password, може обмежувати можливості користувача, що знає тільки User Password. Для того, щоб задати пароль, необхідно підсвітити бажаний тип пароля. Після натиснення клавіші Enter відобразиться вікно з двома полями: у першому полі необхідно ввести пароль, а у другому – продублювати його.

Скидання налаштувань CMOS BIOS. Якщо ПК відмовляється завантажуватися після змін, внесених до BIOS, то повернути настройки назад ви не зможете. У таких випадках допомагає скидання настройок CMOS. Для цього потрібно слідувати інструкції по скиданню CMOS для вашої материнської плати. В деяких випадках для скидання CMOS слід замкнути (або розімкнути) перемичку, подавши сигнал «Clear CMOS», або використати DIP-перемикач. Обов'язково після скидання CMOS потрібно повернути перемичку в первинне положення. Як ще один варіант, - можна дістати батарею материнської плати і відключити комп'ютер від мережі. Але при цьому іноді потрібно почекати декілька годин.

У описаного вище методах є два недоліки. Перший і найзначніший недолік полягає в тому, що скидаючи BIOS, окрім пароля скидаються ще і всі старі настройки, які потім знову доведеться відновлювати. Другий недолік полягає в тому, що на багатьох сучасних материнських платах використовується інший тип пам'яті і є можливість спалити материнську плату при замиканні (розмиканні) перемички.

Існує метод встановлення паролів на жорсткий диск комп'ютера. В цьому випадку за допомогою спеціальної програми можливо закодувати 0-ву доріжку вінчестера. При вмиканні комп'ютера при звертанні до вінчестера встановлена програма запитує пароль, використовуючи який програма розкодує 0-ву доріжку. При відсутності паролю вінчестер стає недоступним для користувача. Крім того, якщо пароль буде втрачено (забуто) вся інформація на вінчестері в більшості випадків буде втрачена (відкриття системи можуть зробити висококваліфіковані спеціалісти при наявності необхідної інформації про вінчестер (копія FAT, Partition Table, Boot Record та ін.).

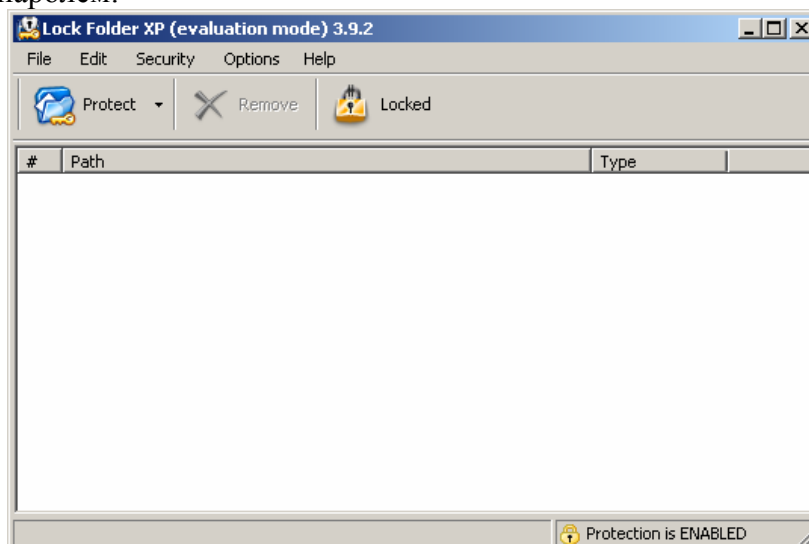
Програми захисту інформації, що знаходиться на вінчестері.

Існує широкий спектр програмного забезпечення, яке дає можливість встановлювати паролі на окремі драйвери, каталоги та файли. Ці програми основані на різних алгоритмах. Найбільш поширеними є: кодування інформації, яка знаходиться в вибраних файлах; дописування інформаційної частини в кінець файлу, яка надає право на копіювання, перенос, запис та зчитування файлу і дописується в кінець файлу; системи перехвату звертань до FAT і по праву доступу програма вирішує який сервіс надати користувачу при роботі з файлом, директорією чи каталогом.

Програма CD-DVD Lock призначена для задання заборони доступу на зчитування та запис інформації з медіа-пристроїв, таких як компакт-диск, DVD, флеш-накопичувачі тощо. Також є можливість захисту окремих розділів вінчестера.

Розглянемо ще один, більш потужний програмний продукт для захисту даних.

Lock Folder XP - новий інструмент безпеки, який дозволяє замикати файли, папки і диски особистим паролем:

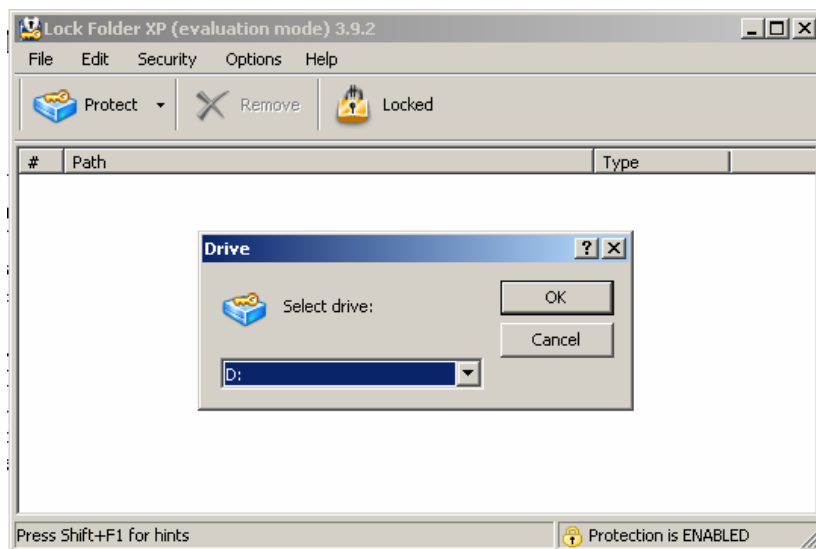


Інтерфейс програми

Програма, забороняючи доступ до інформації, також ефективно захищає від зловмисних програм типу вірусів, черв'яків і троянських коней.

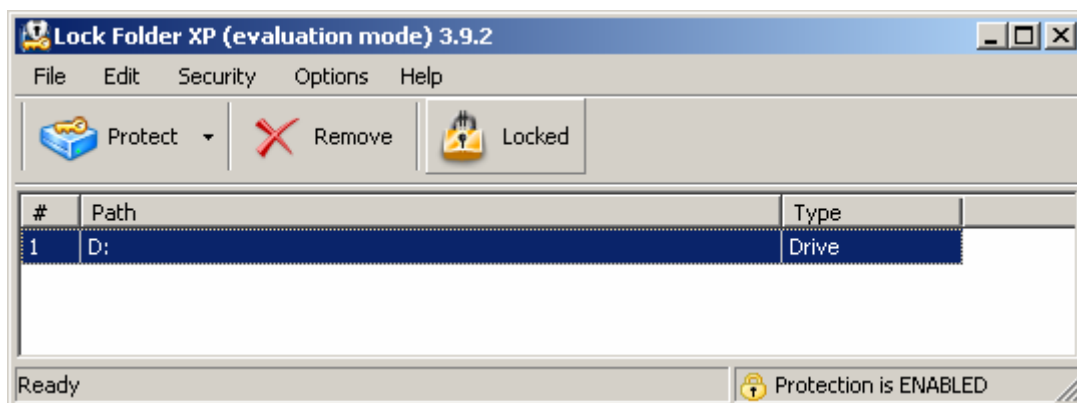
При встановленні програмного продукту буде запропоновано вказати пароль, який і буде застосовуватись для відкриття налаштувань програми. При цьому дуже важливо, щоб Ви його запам'ятали, оскільки для встановлення і зняття заборон на файли, папки чи диски необхідно буде вказати цей пароль. При деінсталяції програми також необхідно буде ввести особистий пароль, інакше Ви просто не зможете цього зробити.

Для того, щоб заборонити доступ до локального диска, необхідно в вікні Lock Folder XP вибрати: File\Protect...\Drive... У вікні, що відкрилось, з запропонованого списку вибрати потрібний диск, який Ви хочете захистити особистим паролем (заборонити доступ) і натиснути клавішу ОК.



Вікно вибору диску

Після здійснення такої послідовності дій даний диск з'явиться в робочій області програми. При цьому доступ до нього ще не буде заблокований («замок» відкритий і захист відсутній). Для здійснення заборони необхідно виділити диск та натиснути на піктограму Unlocked, після чого вона змінить своє значення на Locked, дозволивши заборону доступу (Protection is ENABLED). Для збереження налаштувань просто здійснюємо вихід з програмного продукту натиснувши комбінацію клавіш Alt+X чи вибравши File\Exit.



Вікно зміни параметрів блокування

Якщо потрібно знову відкрити доступ до заблокованого нами диска – заходимо в Lock Folder XP, виділяємо потрібний диск та натискаємо на «замок» (Locked) після чого

він «відкриється», набувши значення Unlocked. Далі закриваємо програму, зберігши налаштування.

У випадку, коли надалі нам не потрібна буде заборона до диску, то можна видалити його з робочої області програми, виділивши та натиснувши на піктограмі Remove.

При здійсненні заборони доступу до певних папок (файлів) необхідно зайти в програму Lock Folder XP та вибрати File\Protect...\Folder...(File\Protect...\File...). У вікні Обзор папок чи Select file вибираємо потрібну для захисту папку (файл), після чого вона автоматично перенесеться в робочу область програми. Далі натискаємо піктограму Unlocked і закриваємо програму, зберігши зміни. Після здійснених дій дана папка чи файл зникнуть з того місця, де вони безпосередньо були присутні (тобто стануть невидимими іншим користувачам). Розблокування даних здійснюється аналогічно процедурі відкриття доступу до дисків.

Замикання файлів, папок і дисків – краща гарантія того, що ніхто випадково або навмисно не дістане доступ до Ваших фінансів, приватної чи конфіденційної інформації. Оскільки файли, папки чи диски робляться невидимими, вони не можуть бути видалені, пошкоджені або заражені будь-яким іншим способом.

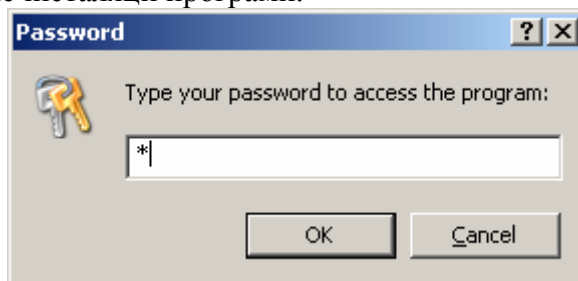
Інноваційні і надійні технології забезпечують найбезпечніший спосіб зберігати інформацію і захищати проти нападів хакера, зловмисного програмного забезпечення, і нечесних службовців.

Хід роботи

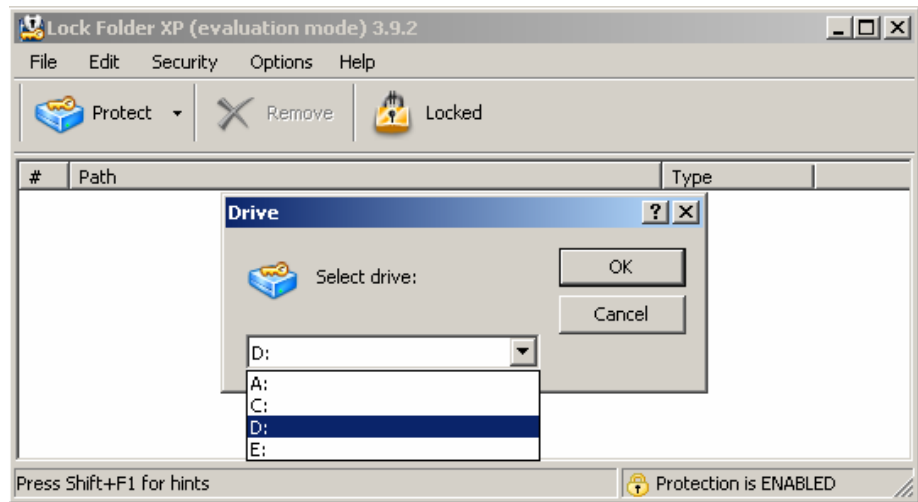
1. На диску C: в папці Мои документи створіть папку зі своїм прізвищем, а в ній два файли (текстовий документ з інформацією про себе та малюнок в форматі .jpg).
2. Запустіть програму Lock Folder XP та розгляньте її функціональні можливості, спочатку здійснивши заборону доступу до диска D:\, а потім послідовно до створених раніше папки та файлів. Результат роботи оформіть у звіті про виконання практичної роботи
3. Відмініть здійснені заборони, видаливши з робочої області Lock Folder XP усі заблоковані файли.
4. Видаліть створені Вами файли та папки.
5. Зробіть звіт по роботі та представте викладачу для захисту.

Методичні рекомендації

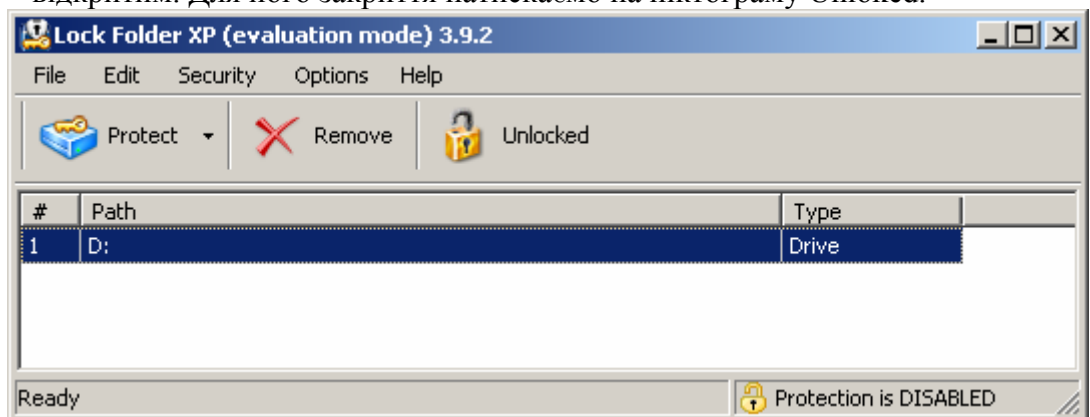
1. Для здійснення заборони доступу до диску D:\ необхідно відкрити програму Lock Folder XP. У поле вводу пароля внести 1, або ж той пароль, який задавався під час інсталяції програми.



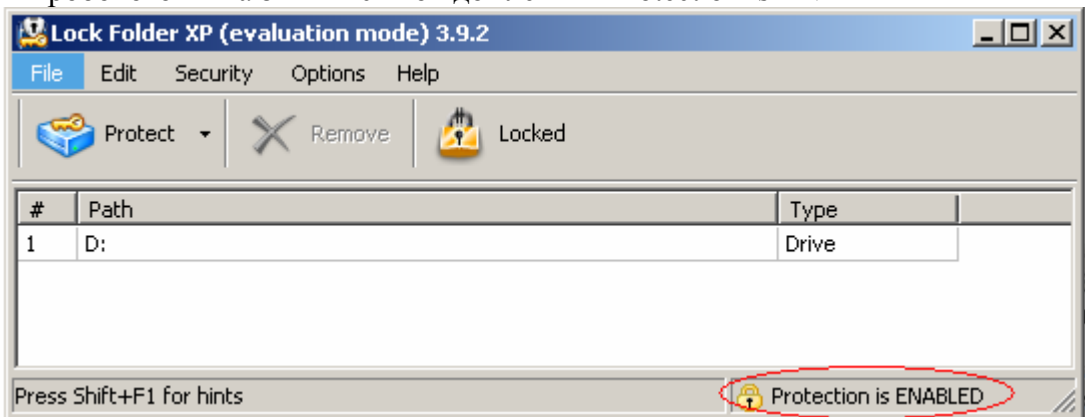
2. У відкритому робочому вікні програми виконати послідовність дій File\Protect Object...\Drive. З запропонованого списку обрати диск для якого потрібно заблокувати доступ.



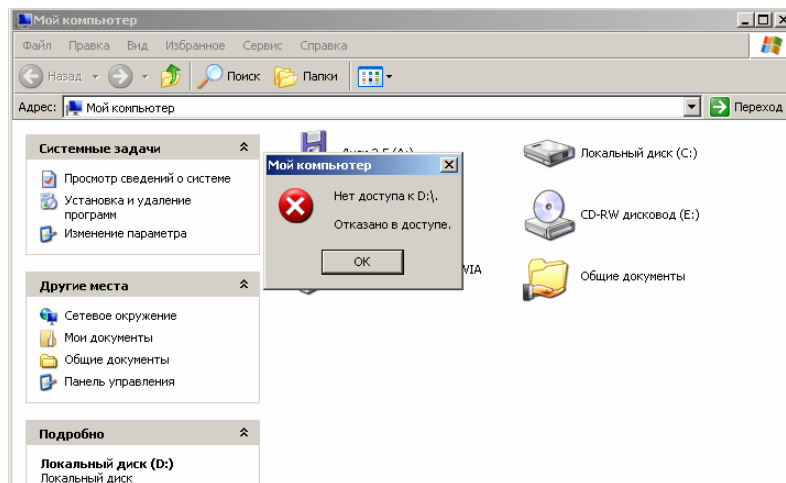
3. У робочій області з'явиться обраний диск, але доступ до нього залишається відкритим. Для його закриття натискаємо на піктограму Unlocked.



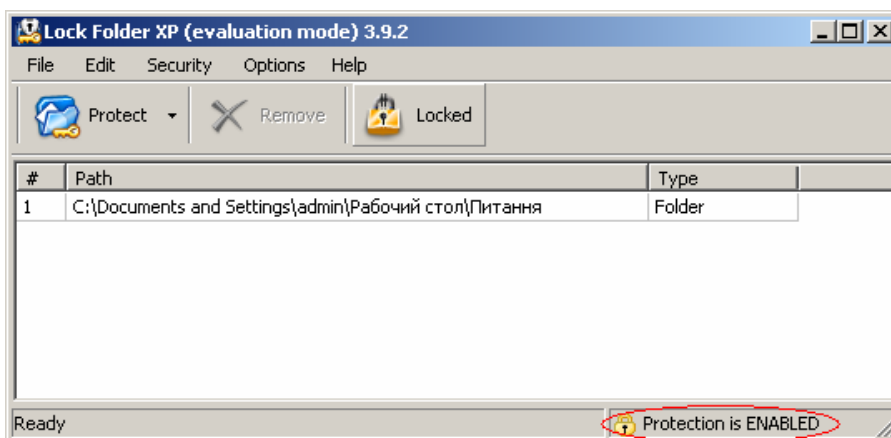
4. Піктограма змінить своє значення на Locked, а в правому нижньому кутку робочого вікна з'явиться повідомлення «Protection is ENABLED»



5. Закриємо програму одним із способів, котрі зазначалися в теоретичному матеріалі, та перевіримо результат:



6. Для встановлення заборони доступу до папки у робочому вікні програми Lock Folder XP виконується послідовність дій: File\Protect Object...\Folder. Із запропонованого списку обираємо необхідну папку. Після того, коли вона потрапляє до списку у робочій області програми проводимо ідентичні дії, як при забороні доступу до локального диску.



7. При виконанні послідовності дій File\Protect Object...\File, аналогічно виконується заборона доступу до файлів.

Зміст звіту

Звіт повинен містити в собі короткі теоретичні відомості, які необхідні для виконання практичного заняття та відповіді на контрольні питання; результати виконання дій при роботі з запропонованими програмами, а також використовувані налаштування. До звіту додати скріншоти виконання завдання та скріншоти отриманих результатів (заблокованого диска, папки, файла).

Контрольні запитання:

1. Що таке FAT, NTFS, HPFS?
2. Що таке BIOS і яке його основне призначення?
3. Які існують два типи паролів BIOS?
4. Яким чином здійснюється завдання пароля в AWARD BIOS?
5. Яким чином здійснюється завдання пароля в Amі BIOS?
6. Які Ви знаєте способи скидання паролю BIOS?
7. Що собою являє програма CD-DVD Lock та які її функціональні можливості?

8. Які існують способи захисту даних в програмному продукті CD-DVD Lock та яким чином вони реалізуються?
9. Що собою являє програма Lock Folder XP?
10. Яким чином здійснюється заборона до локальних дисків в Lock FolderXP?
11. Яким чином здійснюється заборона до файлів та папок в Lock Folder XP?
12. Як відкрити доступ до заблокованої в програмі Lock Folder XP інформації?