**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії***

**ЛАБОРАТОРНА РОБОТА № 1**

з курсу

***«Безпека програм та даних»***

**ТЕМА: Засоби парольної ідентифікації та адміністрування.**

**Студент : Трембіцький Нікіта**

**Група : 31ІПЗ**

**Факультет : Інформатики**

**Викладач : Галицький О.В.**

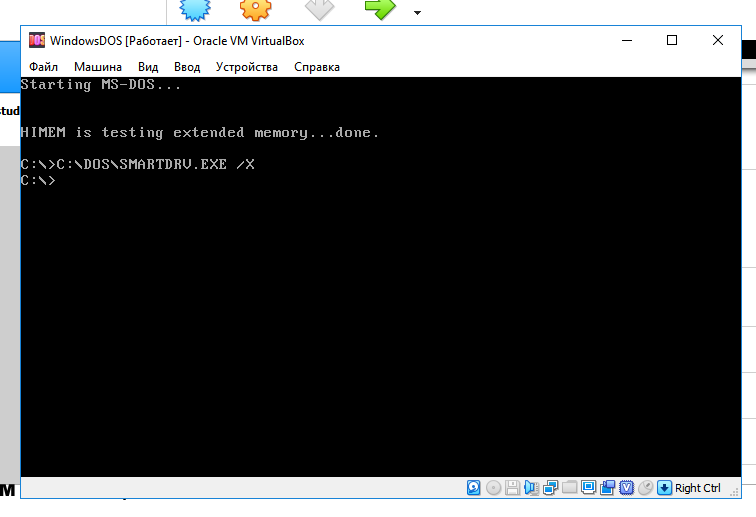
Київ 2019

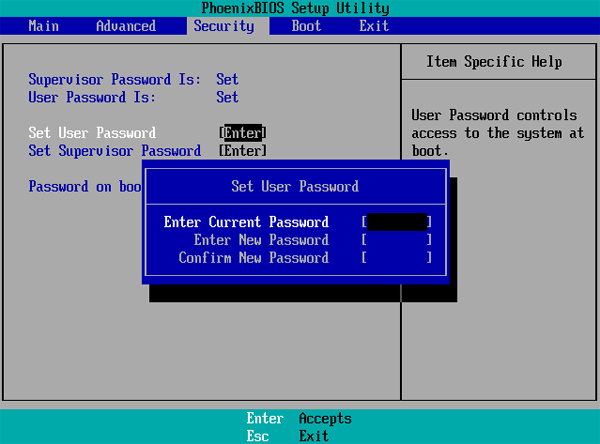
**1.** **Продемонструвати роботу парольного захисту в BIOS.**

**• Завантажити програмний засіб для роботи з віртуальними ПК (Windows Virtual PC).**

**• Ввімкнути віртуальний комп’ютер, який працює під управлінням ОС MS DOS .**

**• На віртуальному комп’ютері, який працює під управлінням ОС MS DOS встановити парольний захист на завантаження операційної системи. Продемонструвати роботу парольного захисту в BIOS.**





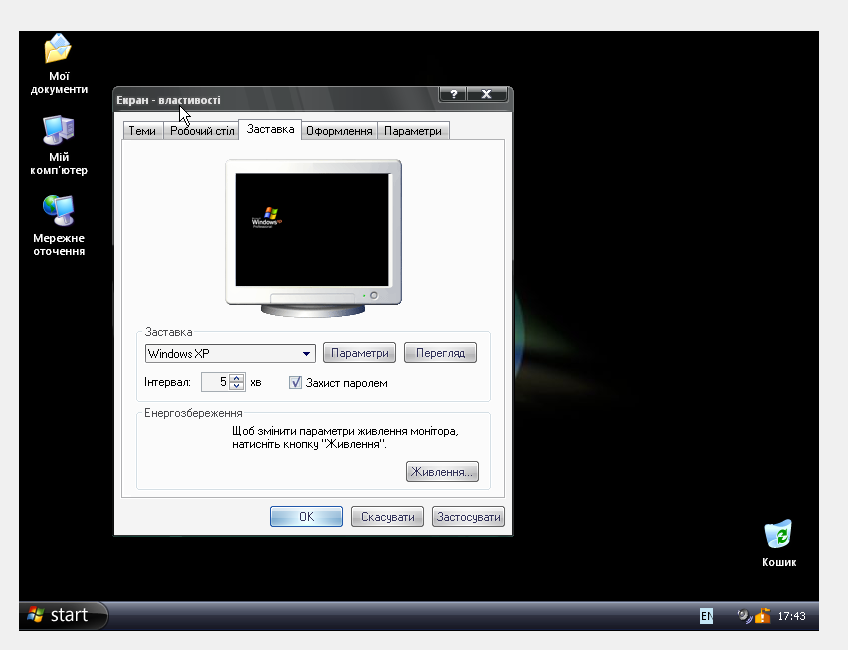
**2. Продемонструвати використання пароля та налагодження заставки в операційній системі.**

**• Завантажити програмний засіб для роботи з віртуальними ПК (Oracle VM VirtualBox).**

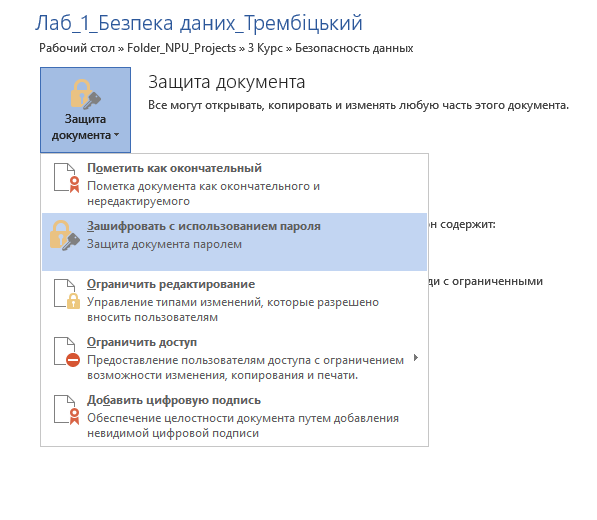
**• Ввімкнути віртуальний комп’ютер, який працює під управлінням ОС Windows XP.**

**• Встановити режим включення заставки через 5 хвилин після «простою» комп’ютера.**

**• Продемонструвати використання пароля та налагодження заставки.**

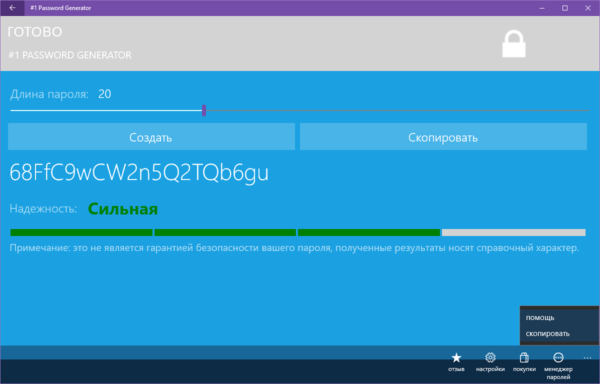


**3.** **Продемонструвати використання парольного захисту в програмному пакеті MS Office (Word, Excel, Access).**



**4.** **За допомогою пошукової системи глобальної мережі Інтернет знайти, встановити (встановлювати програмні засоби слід на віртуальну машину) та дослідити програмні засоби для генерування паролів.**

**1)Password Generator**

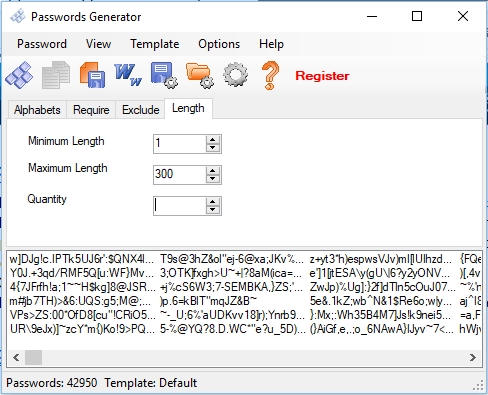


* Підтримувані платформи: Windows 10.
* Вартість: безкоштовно.

Програма генерує один пароль довжиною, налаштованої користувачем. У налаштуваннях програми можна включити використання цифр і спецсимволів в паролі, а також відмовитися від неоднозначних символів. У головному вікні програма показує результат перевірки складності пароля.

Додаткова функція програми - нагадування про термін закінчення дії пароля.

**2) Passwords Generator**



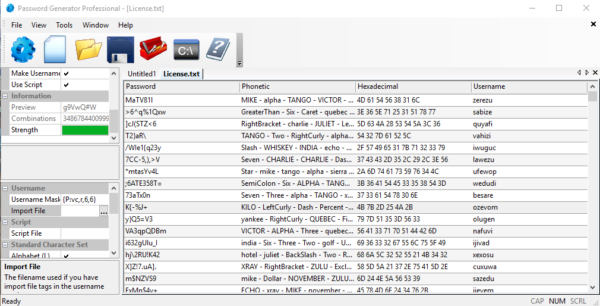
* Підтримувані платформи: Windows.
* Вартість: $14,99.

Додаток генерує будь-яку кількість паролів довжиною від одного до 300 символів. Користувач може налаштувати, які символи повинні входити в пароль - малі та великі літери латинського алфавіту, цифри, спецсимволи. Можна виключити використання схожих символів.

Згенеровані паролі можна скопіювати або зберегти в файл.

Безкоштовний період - десять днів. Російська мова не підтримується.

**3) Password Generator Professional**



* Підтримувані платформи: Windows 10.
* Вартість: безкоштовно.

За допомогою цього генератора паролів можна отримати до одного мільярда паролів довжиною від одного до 999 символів. Користувач може вибрати типи символів, що входять в пароль.

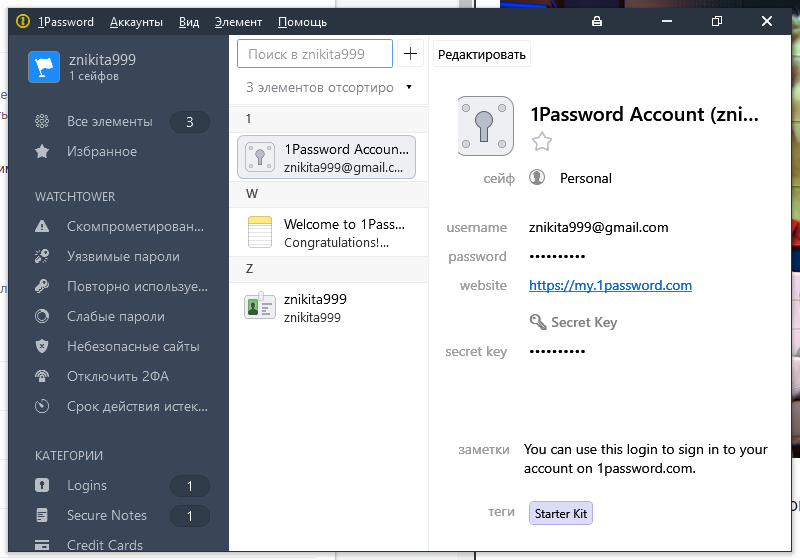
Програма здатна генерувати не тільки паролі, але і логіни (можна налаштувати маску логіна), показувати паролі в шістнадцятковій системі числення, а також допомагати запам'ятовувати згенерований пароль, пропонуючи слово на кожен символ.

Сформовані паролі можна скопіювати в буфер обміну і зберегти в текстовий файл, XML, HTML, CSV і Microsoft Excel. Програма дозволяє використовувати скрипти VBScript для зміни згенерованих паролів на свій розсуд.

Російська мова не підтримується.

**5.** **За допомогою пошукової системи глобальної мережі Інтернет знайти, встановити (встановлювати програмні засоби слід на віртуальну машину) та дослідити програмні засоби для збереження паролів.**

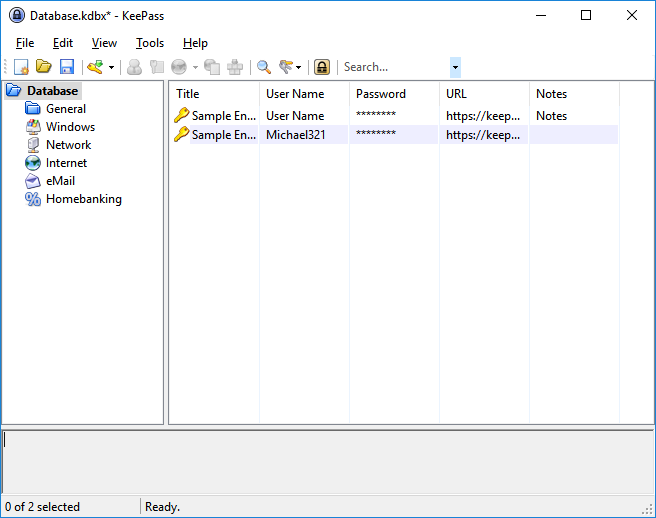
**1)** **1Password**



[1Password](https://root-nation.com/goto/https:/1password.com/) - популярний менеджер паролів. Сервіс працює без Інтернету, а також вміє синхронізувати дані через iCloud і Dropbox, Wi-Fi або мережеві папки на комп'ютері. 1Password дозволяє ділиться доступом або паролями з друзями або близькими через додавання останніх в довірені контакти.

В наявності розширення для браузерів Safari, Firefox, Opera і Google Chrome. Програма доступна на Android, iOS, mac і Windows. За мобільні додатки доведеться заплатити, але є тріал на 30 днів.

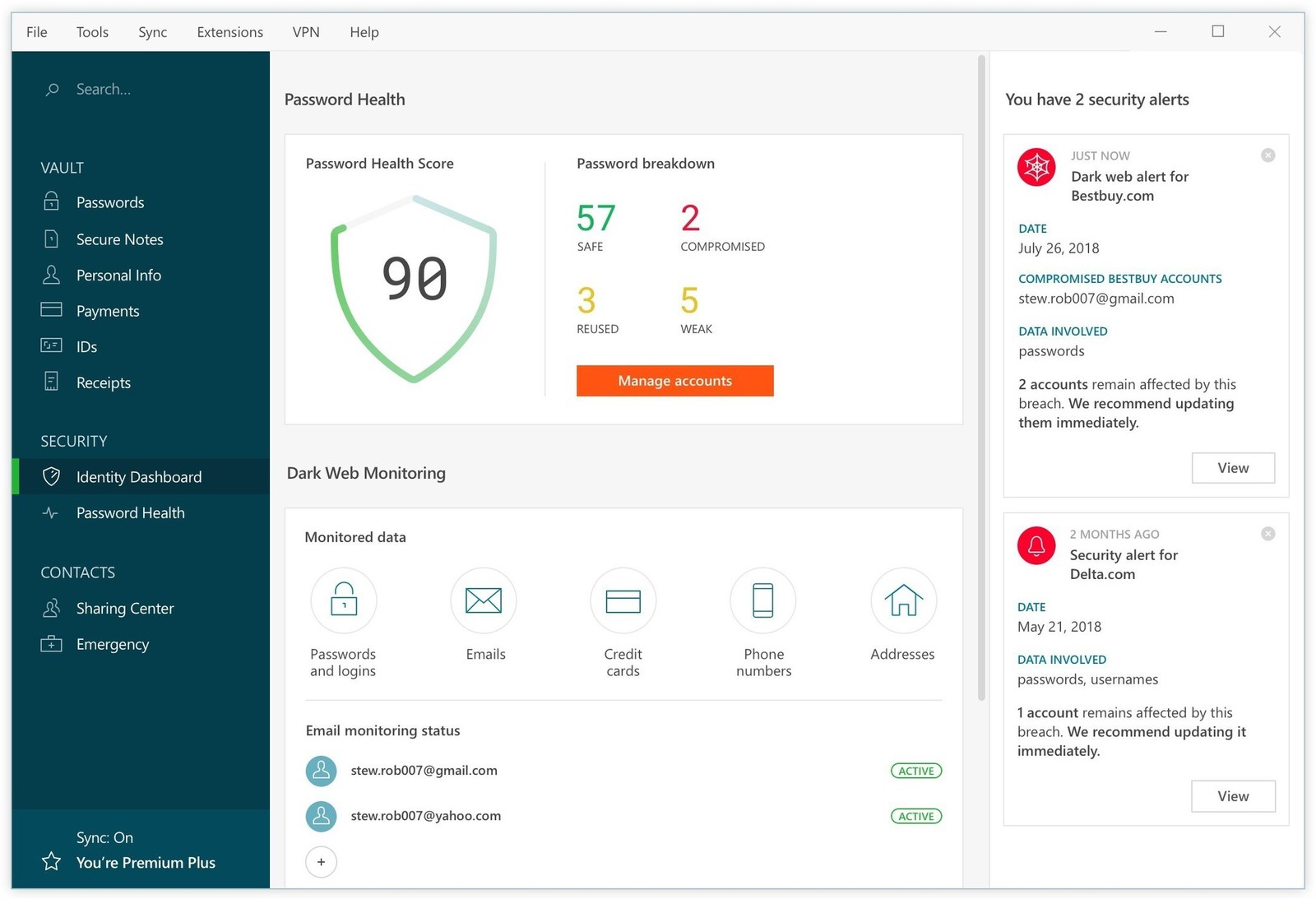
**2) KeePass**



Додаток [KeePass](https://root-nation.com/goto/https:/keepass.info/) має застарілий зовнішній вигляд, відкритий вихідний код і портативну версію, яка легко завантажується з флешки на будь-який комп'ютер. Оскільки у KeePass немає вбудованої синхронізації, там же, на особистії хмарі або іншому носії зберігається база даних паролів.

Для максимального захисту, рекомендується зберігати на особистії хмарі портативну версію KeePass і його базу даних. В цьому випадку скористатися можливостями програми вийде без проблем на будь-якому комп'ютері. KeePass доступна безкоштовно на Android, iOS, mac, Windows і Linux.

**3) Dashlane**



При першому запуску [Dashlane](https://root-nation.com/goto/https:/www.dashlane.com/) програма перевіряє вже створені паролі і якщо знаходить слабкі комбінації пропонує змінити, згенерувати і зберегти новий і надійний пароль. Dashlane оповіщає власника, якщо зловмисники зламають один з акаунтів користувача і відразу ж запропонують заблокувати його і змінити дані.

Крім шифрування, Dashlane здатна зберігати чеки і платіжки з покупок в інтернеті, банківські дані, номери карт, рахунки та іншу особисту інформацію. Програма доступна безкоштовно на Android, iOS, mac і Windows.