Автори: Шпортько О. В., Сущук О. А., Красін М. А.

Лабораторна робота № 6.

Тема. Аналіз ефективності парольного захисту PDF-документів, архівів у різних форматах, текстових документів та електронних таблиць. Створення стійких паролів.

Мета. Формування вмінь і навиків створення стійких паролів. Отримання знань методів і способів подолання парольного захисту та навиків використання відповідного програмного забезпечення. Закріплення знань файлової структури, вмінь і навиків використання можливостей віртуальних принтерів, архіваторів, текстових і табличних редакторів для організації парольного захисту.

Теоретичні відомості

На сьогодні багато користувачів архівують свої файли за допомогою популярних архіваторів ARJ, ZIP, RAR, або створюють PDF чи офісні документи, вказуючи при цьому нескладні паролі, за допомогою яких вміст цих файлів шифрується. Але підбір паролів до таких файлів не складає особливих труднощів. Досить скористатися відповідними програмами Advanced Archive Password Recovery (ARCHPR), Advanced ARJ Password Recovery (AAPR), Advanced ZIP Password Recovery (AZPR), Advanced RAR Password Recovery (ARPR), Advanced PDF Password Recovery (APDFPR), Advanced Office Password Recovery (AOPR) чи подібними до них. Всі вони використовують наступні види зламу:

- послідовного перебору різних комбінацій символів (Brute-force чи „грубої сили”);
- послідовного перебору по масці, якщо відома хоча б частина паролю;
- атака по словнику, коли перебір виконується серед найуживаніших паролей;
- гібридний метод (атака по словнику + метод послідовного перебору).

Крім цього, для архівів можливий злам на основі частини "відомого тексту" (known-plaintext attacks).

На сьогодні програми зламу захисту архівів здатні:

- забезпечувати швидкість перебору паролів понад два мільйони в секунду;
- підтримувати всі методи стискування;
- опрацьовувати саморозпаковуючі архіви;
- встановлювати параметри перебору паролів: діапазон кодової довжини, кодову сторінку, набір символів та ін.;
- підтримувати не англійські літери при використанні методу "грубої сили";
- атакувати за допомогою словника" з можливістю його зміни.

Використовувати програмне забезпечення для підбору пароля доцільно, коли ви його забули. Але цими ж засобами можуть скористатися зловмисники для доступу до захищених даних. Тому для надійного шифрування необхідно встановлювати стійкі паролі з довжиною від 10 символів.

Жоден пароль не може бути на 100 відсотків безпечним. Його завжди можна відгадати або розшифрувати. Проте ви можете додати шанси на свою користь, застосувавши надійний пароль. Надійний пароль важко розкрити стороннім особам. Такі паролі слід використовувати у всіх випадках, коли потрібен пароль: наприклад, для входу на комп'ютер, в обліковому записі Інтернету або для захисту документів.

Надійні паролі:

- відрізняються для різних ідентифікаторів;
- складаються не менше, ніж з семи знаків;
- містять одночасно великі й малі літери, цифри та спеціальні символи на позиціях від другої;
- мають вигляд випадкової сукупності знаків;
- не містять повторюваних знаків;
- не містять послідовних знаків, наприклад, *1234*, *abed* або *qwerty*;
- не дають змоги розпізнати будь-яку закономірність, тематику або цілі слова будь-якою мовою;
- не використовують цифри або символи замість подібних до них знаків (наприклад, $ замість S або 1 замість l), оскільки це полегшує розкриття паролю;
- не містять частково або повністю вашого імені користувача для входу до комп’ютера, інтернету або до мережі;
- не вказують на ваші особисті дані, ключові дати чи дані близьких вам людей.

Часто змінюйте паролі – принаймні кожні три місяці. Стежте за тим, щоб новий пароль повністю відрізнявся від старого, і в ньому не було жодної частини старого паролю.

Будьте обережні, коли в діалоговому вікні операційна система пропонує запам'ятати пароль. Якщо ви дозволите це, то кожен, хто ввійшов на ваш комп'ютер (навіть через мережу), матиме доступ до цього захищеного паролем об'єкта.

Надійний пароль можна порівняти із замком. Він замикає ваш документ від сторонніх, але, як і замок, його можна зламати. Забути пароль – це все одно що загубити ключа. Проте ситуація може бути не дуже серйозною, залежно від того, який пароль ви забули. Якщо це мережний пароль, адміністратор може зняти його. Якщо це пароль для облікового запису Інтернету – постачальник послуг, як правило, надішле вам електронною поштою повідомлення з паролем або нагадуванням. Але якщо ви забули пароль документа, ви не зможете відкрити його, доки не пригадаєте чи не підберете пароль.

Деякі люди рекомендують у жодному разі не записувати паролі, деякі радять тримати список паролів у надійному місці, відомому лише вам (наприклад, на аркуші паперу). Але ніде ви не почуєте поради написати пароль на стікері та прикріпити його до монітора.

Підготовчий етап заняття. Актуалізація знань

1. Віднайдіть ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту та скопіюйте його в буфер обміну.
2. Вставте скопійований файл та змініть його назву на *Proba.docx*. Відкрийте цей файл у текстовому процесорі MS Word 2010.
3. Створіть у редакторі електронних таблиць MS Excel 2010 наступну таблицю для фіксування часу зламу паролів різної довжини документів різних типів:

Тривалість зламу паролів різної довжини документів різних типів, с

Тип документа	Довжина паролю (символів)						
	1	2	3	4	5	6	N
PDF							
RAR							
ZIP							
DOCX							

Подолання парольного захисту PDF-документів

4. Збережіть файл *Proba.docx* у форматі PDF під назвою *Proba1.pdf*, заборонивши копіювання та друк його фрагментів. Для цього:
   4.1. Розпочніть друк завантаженого документа на віртуальному принтері **PDF Creator**;
   4.2. У вікні основних параметрів PDF-файла перейдіть у вікно додаткових параметрів створення;
   4.3. Оберіть параметри PDF-документа, віднайдіть і встановіть на його відповідній закладці прапорець **Использовать защиту**, прапорець задання паролю та редагування, та прапорці, які забороняють копіювання та друк PDF-документа;
   4.4. Закрийте вікно додаткових параметрів з збереженням внесених змін;
   4.5. Продовжте створення PDF-документа та введіть пароль з одного символа для його редагування.
5. Самостійно почергово збережіть файл *Proba.docx* у форматі PDF під назвами *Proba2.pdf*, *Proba3.pdf*, *Proba4.pdf*, *Proba5.pdf*, задаючи паролі відповідно з 2, 3, 4 та 5 символів чи знаків.
6. Збережіть файл *Proba.docx* у форматі PDF під назвою *Proba6.pdf* з шифруванням паролем його вмісту. Для цього:
   6.1. Відкрийте файл *Proba.docx* у текстовому процесорі MS Word 2010;
   6.2. Розпочніть створення PDF-файла, використовуючи пункт стрічки меню **Файл – Сохранить как**, після чого вкажіть у відповідному вікні назву нового файла та його тип;
   6.3. За допомогою кнопки **Параметры** у нижній частині цього вікна відкрийте вікно параметрів PDF-файла, встановіть у ньому прапорець **Зашифровать документ с помощью пароля** та збережіть внесені зміни;
   6.4. Продовжте створення PDF-документа та введіть пароль для його редагування.
7. Самостійно збережіть файл *Proba.docx* у форматі PDF під назвами *ProbaS.pdf*, зашифрувавши його послідовними знаками, наприклад, *1234*, *abcd* або *qwerty*.
8. Самостійно збережіть файл *Proba.docx* у форматі PDF під назвами *ProbaN.pdf*, зашифрувавши його надійним, на вашу думку, паролем.
9. Підберіть паролі до створених захищених PDF-документів за допомогою програми Advanced PDF Password Recovery (APDFPR). Для цього почергово:
   9.1. Самостійно завантажте програму APDFPR (рис. 1), врахувавши, що вона створена корпорацією Elcomsoft;
   9.2. За допомогою кнопки **Открыть** оберіть PDF-файл для зламу;
   9.3. У списку **Тип атаки** оберіть вид зламу **По словарю**;
   9.4. Для початку підбору натисніть кнопку **Старт**;
   9.5. Якщо підібрати пароль по словнику не вдалося, то самостійно відновіть його послідовним перебором, обираючи необхідний набір символів та максимальну довжину (на закладці **Длина**). Тривалість зламу в секундах, яку визначає сама програма, занесіть у перший рядок з даними порівняльної таблиці. Коли прогнозована тривалість зламу перевищує 10 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

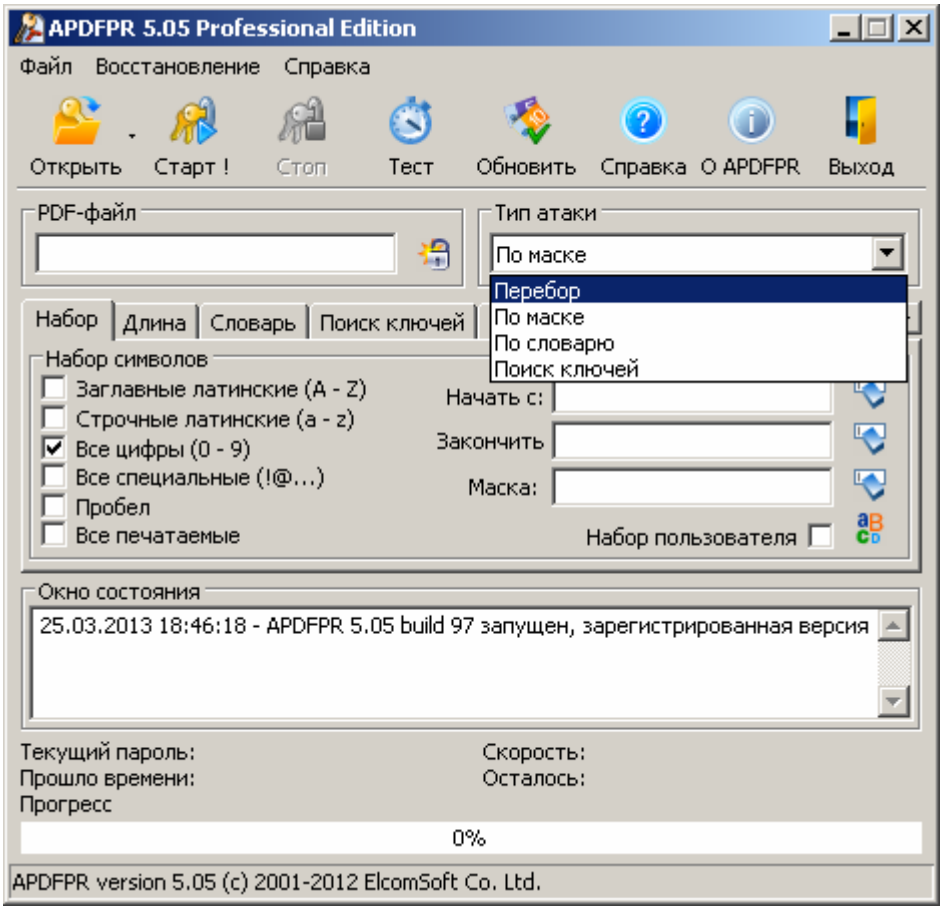

Рис. 1. Вибір виду зламу у програмі APDFPR

Подолання парольного захисту Zip та RAR-архівів

10. Заархівуйте вміст файла *Proba.docx* у ZIP та RAR-архівах під назвами *Proba1.zip*, *Proba2.zip*, *Proba3.zip*, *Proba4.zip*, *Proba5.zip*, *Proba6.zip*, *ProbaS.zip*, *ProbaN.zip*, *Proba1.rar*, *Proba2.rar*, *Proba3.rar*, *Proba4.rar*, *Proba5.rar*, *Proba6.rar*, *ProbaS.rar*, *ProbaN.rar*, де остання цифра назви вказує на довжину пароля чи його надійність. Для цього:
    10.1. В контекстному меню файла *Proba.docx* оберіть пункт **Упаковать в архив**;
    10.2. У вікні архіватора, яке з'явиться на екрані, на закладці **Общие** вкажіть назву файла архіву та його формат, а на закладці **Дополнительно** натисніть кнопку **Установить пароль** для його задання;
    10.3. Самостійно завершіть створення архіву.
11. Самостійно підберіть паролі до створених захищених архівів за допомогою програми Advanced Archive Password Recovery (ARCHPR), використовуючи способи словника та послідовного перебору (рис. 2). Тривалість зламу в секундах, яку визначає сама програма, занесіть у відповідно у другий та третій рядки з даними порівняльної таблиці. Якщо прогнозована тривалість зламу перевищує 10 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

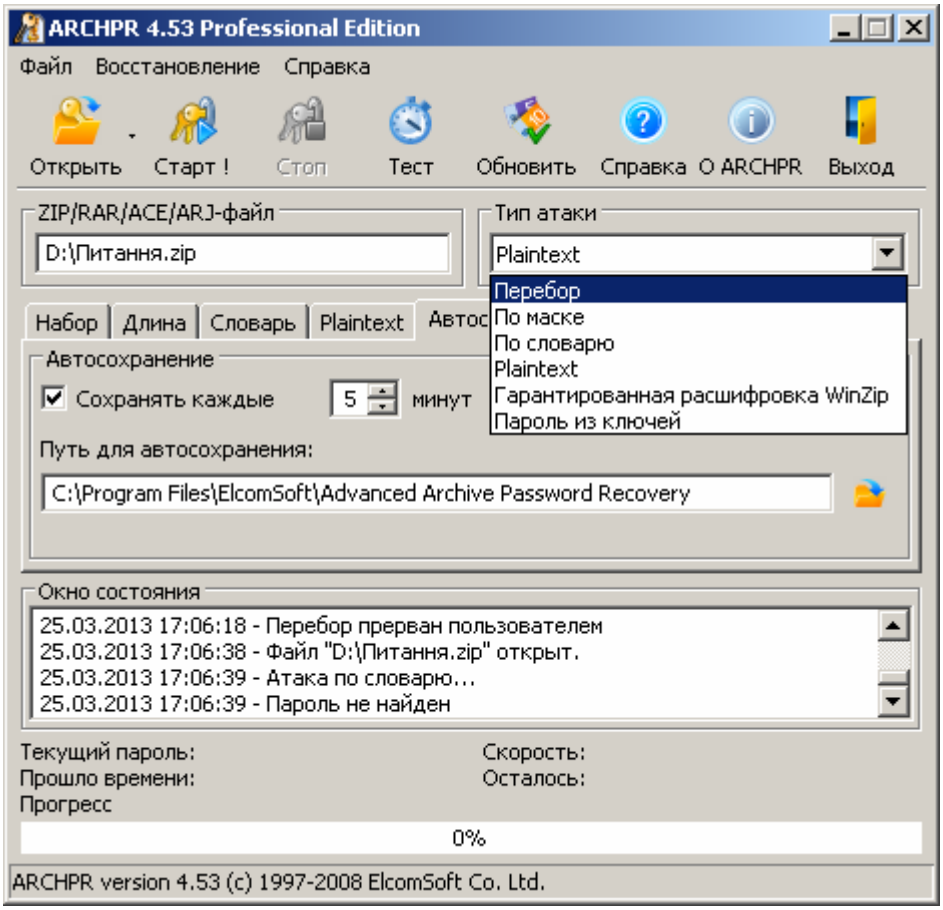

Рис. 2. Вибір виду зламу у програмі ARCHPR

12. Самостійно заархівуйте надійним паролем файли *Proba.docx* та *ZaxLR6.doc* у спільний ZIP-архів під назвою *ProbaSumisn.zip*, попередньо виділивши ці файли у вікні провідника. Заархівуйте без пароля файл *ZaxLR6.doc* у ZIP-архів *ZaxLR6.zip*.
13. Зламайте пароль архіву *ProbaSumisn.zip* способом підбору на основі частини "відомого тексту". Для цього:
    13.1. Завантажте програму ARCHPR;
    13.2. За допомогою кнопки **Открыть** оберіть файл *ProbaSumisn.zip* для зламу;
    13.3. У списку **Тип атаки** оберіть вид зламу **Plaintext** (рис. 2);
    13.4. Перейдіть на закладку **Plaintext** та оберіть на ній файл *ZaxLR6.zip*, як такий, що містить частину "відомого тексту";
    13.5. Для початку підбору натисніть кнопку **Старт**.
14. Зробіть висновки про можливість зламу надійних паролей архівів декількох файлів, якщо вони містять доступні файли.

Завершальний етап заняття

15. Самостійно збережіть файл *Proba.docx* під назвами *Proba1.docx*, *Proba2.docx*, *Proba3.docx*, *Proba4.docx*, *Proba5.docx*, вказуючи **паролі для їх відкриття** відповідної довжини.
16. Самостійно збережіть файл *Proba.docx* під назвами *Proba6.docx*, *ProbaS.docx*, *ProbaN.docx*, задаючи відповідно **паролі для шифрування** довжиною 6 символів, послідовності символів та надійний пароль.
17. Самостійно підберіть паролі до створених захищених архівів за допомогою програми Advanced Office Password Recovery (AOPR), використовуючи способи словника та послідовного перебору (рис. 3). Тривалість зламу в секундах, яку визначає сама програма, занесіть у четвертий рядки з даними порівняльної таблиці. Якщо прогнозована тривалість зламу перевищує 10 хвилин, то зупиніть процес підбору та внесіть у таблицю прогнозований час перебору.

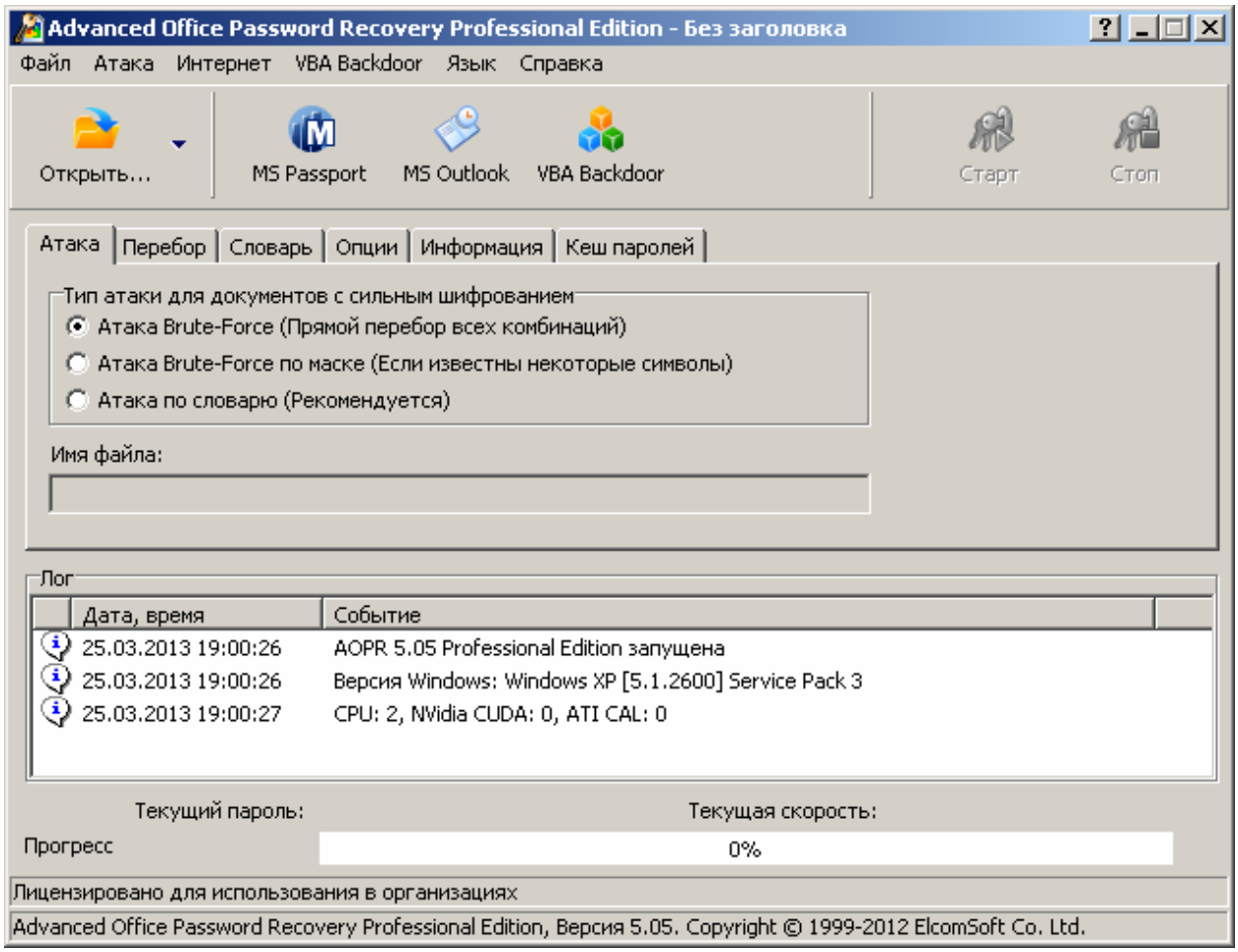

Рис. 3. Вибір виду зламу у програмі AOPR

18. На основі даних порівняльної таблиці побудуйте графіки залежності тривалості зламу від довжини паролю для різних форматів файлів. Який характер залежності при цьому спостерігається? Чому графіки відрізняються між собою та від графіків одногрупників? Спрогнозуйте тривалість зламу паролів довжиною 10 символів.
19. Створіть електронний лист з формулюваннями та відповідями на контрольні запитання у своїй поштовій скриньці на сайті gmail.com. Приєднайте до цього листа файл з даними порівняльної таблиці і відповідними графіками та файли *ProbaSumisn.zip*, *ZaxLR6.zip*, *Proba5.rar*, *Proba6.pdf*. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР6_Величко Володимир*. Надішліть створений лист на адресу LRZaxInf@gmail.com.

Контрольні запитання.

1. Які види зламу використовуються для документів і архівів, зашифрованих паролем?
2. Який додатковий вид зламу застосовується до архівів? Як такий злам реалізувати?
3. Які вимоги висуваються до надійних паролів?
4. Чому не доцільно дозволяти програмам запам'ятовувати паролі?
5. Чому не варто встановлювати один пароль для різних ресурсів?
6. Які файли не доцільно включити у спільні архіви при шифруванні паролем? Чому?