УДК 004.632

Хлистун В.В.
Кіровоградський національний технічний університет

Метод синтезу паролів підвищеної складності

На сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів. Разом з тим вже буденним і конче необхідним є використання інфокомунікаційних технологій, в тому числі електронної пошти, захист якої від несанкціонованого доступу є актуальною задачею не тільки для постачальника сервісу, але й для користувача.

Однією з причин кібератак на електронну пошту є отримання прибутку шляхом, наприклад, їх продажу зацікавленим особам. Найчастіше купівлею поштових скриньок у великих обсягах займаються спамери, адже "зламані" е–скриньки використовують для масових розсилок повідомлень. Іншою ціллю зловмисника є дані, які зберігаються у е–скриньці. Це можуть бути, наприклад, облікові записи соцмереж, хостингів, банків, електронних коштів, ігрових акаунтів тощо. Якщо в е–скриньці відсутні безпосередньо паролі, зловмисник має можливість запросити відновлення пароля на e–mail. Також шахрай обов'язково перевірить, чи не підходить поштовий пароль до облікових записів на інших Інтернет–ресурсах [1]. Отже, будь–яка поштова скринька має цінність для зловмисника, а найпопулярнішими серед українців є сервіс електронної пошти у домені ukr.net [2].

Мета роботи полягає у підвищенні складності пароля на прикладі електронної скриньки у домені ukr.net. Для її досягнення слід розробити метод ускладнення пароля задля збільшення складності його атаки повним перебором.

Під складністю пароля у роботі розуміється міра ефективності, з якою пароль здатний протистояти його вгадуванню або методу повного перебору.

Експеримент випробування поштового сервісу ukr.net показав, що він дозволяє встановити пароль довжиною від 8 до 16 символів, кожен шостий некоректний вхід контролюється капчею (captcha). При цьому, якщо неправильно вводити капчу 12 разів підряд, то на 13 раз вона зникає і ввід пароля здійснюється без капчі. Якщо потім п'ять разів неправильно ввести пароль, то на шостий раз знову з'являється капча і т.д. Отже, виявлено істотний недолік, оскільки блокування IP в разі n–кількості невдалих спроб ввести пароль відсутнє. Це дозволяє здійснити перебір паролів зловмисником, а капчі можливо уникнути за допомогою сервісів, що вводять її автоматично. Таким чином, випливає висновок про те, що для максимальної безпеки е–скриньки у домені ukr.net треба використовувати пароль, який складається з 16 символів і в свою чергу має мати цифри, символи, а також літери верхнього та нижнього регістрів.

Тож, для створення надійного пароля потрібно:

1) вибрати ідентифікаційну фразу, тобто основу майбутнього пароля (наприклад, це може бути улюблений вислів, крилата фраза);

2) синтезувати пароль;

3) скомпонувати пароль (видалити пропуски, замінити символи спеціальними знаками, використати верхній регістр тощо).

Дотримання означених рекомендацій значно підвищить рівень безпеки комп'ютерної мережі та її ресурсів, а також зведе до мінімуму несанкціонований доступ до неї зловмисників [3].

Для прикладу розглянемо пароль «lfdfq;bnblhe;yj!». З першого погляду його неможливо запам'ятати. Але якщо подивитись на українську розкладку клавіатури, то це – «давайжитидружно!». Для того, щоб допрацювати пароль і зробити його більш складним для

перебору можна замінити літеру «l» на «1» (один) та замінити «f» на «F». В результаті отримаємо «1FdFq;bnb1he;yj!», який буде значно складніше перебрати, ніж первісний. Отже, кількість варіантів перебору такого пароля становить 37,157,429,083,410,091,685,945,089,785,856 ітерацій. Для того, щоб підібрати його зі швидкістю 10 млн паролів за секунду, знадобиться приблизно 117825 тлрд років.

Для збільшення кількості переборів пароля і ускладнення його повного перебору пропонується метод, сутність якого полягає у використанні у паролях символів, що відсутні на клавіатурі, але які можна додати за допомогою клавіші Alt та відповідного коду символа (Alt-код). Це дозволяє збільшити кількість символів пароля з 94 до 255. Таким чином, пароль «1FdFq;bnb1he;yj!» можливо істотно ускладнити шляхом заміни символу «b» на «☺»: «1FdFq; ☺n☺1he;yj!». Кількість варіантів перебору такого пароля складає 319,626,579,315,078,487,616,775,634,918,212,890,625. Тобто, у порівнянні з попереднім варіантом кількість переборів зросла у 8601956 разів, а для того, щоб підібрати його зі швидкістю 10,000,000 паролів у секунду знадобиться приблизно 1013529234256337162661008 років.

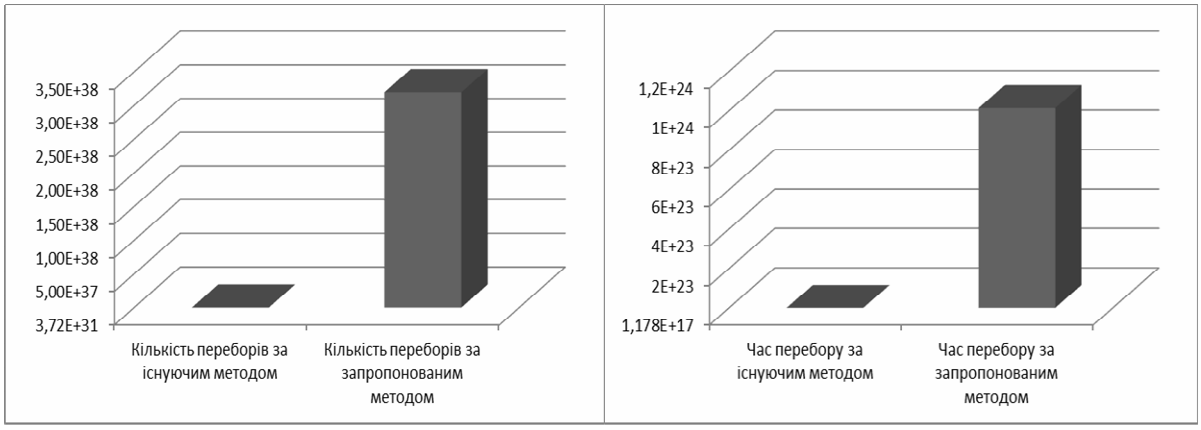

Рисунок 1 – Порівняння ефективності існуючого та запропонованого методів синтезу паролів

Недоліком запропонованого методу є збільшення складності запам’ятовування такого пароля. Але означене легко усунути шляхом визначення ключових чисел та трансформування їх у коди (дата народження, вага, зріст тощо).

В роботі запропоновано ефективний метод синтезу пароля, який забезпечує збільшення складності його атаки повним перебором у 8601956 разів. Завдяки застосуванню запропонованого метода можна бути впевненим у тому, що пароль не зможуть вгадати або атакувати методом повного перебору.

Практична цінність результатів роботи полягає у доцільності використання метода під час створення надійного пароля як для електронної скриньки, так і для інших сервісів в Інтернет: аккаунтів на форумах, соціальних мереж тощо.

Список використаних джерел

1. *Про безпеку пошти [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://habrahabr.ru/company/mailru/blog/169801/ (дата звернення 02.11.2016). – Назва з екрана.*
2. *Статистика популярності поштових сервісів [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: http://www.ar25.org/article/statystyka-populyarnosti-poshtovyh-servisiv.html (дата звернення 02.11.2016). – Назва з екрана.*
3. *Доренський О.П. Мережні інформаційні технології : Навч. посіб. / О.П. Доренський. – Кіровоград: Вид-во “КОД”, 2010. – 234 с.*