ВИБІР НАДІЙНОГО ПАРОЛЮ

бакалавр Г.В. Гряник, бакалавр Є.К .Бондаренко, Національний технічний університет "Харківський політехнічний інститут", м. Харків

За довгі роки життя люди придумали безліч хитрих способів захисту – від паролів до криптографічних ключів. Однак, сам принцип залишається таким же, якщо є замок, отже він може бути зламаний. У сучасному житті користувачі захищають акаунти паролями, пін-кодами та графічними ключами.

Паролі не завжди є надійними. На жаль, найпопулярнішими паролями залишаються "123456", "qwerty", "password", "Picture1", "iloveyou", а також імена, дні народження, номера телефонів і т. д. Топ серед пін-кодів: 1234, 0000,1212, 7777 [1].

Графічні ключи теж мають схожу проблему. Майже половина ключів починається з верхнього лівого кута, та йде зліва направо і зверху вниз. Багато, хто використовує красиві ключі замість безпечних. Таким чином, кожний десятий аккаунт можна зламати простим перебором паролів, а кожний п'ятий користувач використовує один і той же пароль до всіх ресурсів. Якщо хакер дізнається пароль, то він матиме доступ до всіх акаунтів користувача.

Для захисту та ідентифікації використовують біометричні дані. Але навіть така система є вразливою. Зловмисник лише по одному фото палиця може скопіювати біометричні дані. На протидію Touch ID можна використати Face ID. Однак, зламати цю систему допоможе маска-копія обличчя на 3D принтері. При цьому необов'язково відтворювати повністю обличчя, досить тільки надрукувати форму та зліпити ніс, а на місце губ і очей наклеїти детальні двовимірні зображення.

Таким чиним, за результатами проведеного дослідження, для надійності та зручності можна створювати пароль, в якому було б не менше 16 символів – рядок з улюбленого вірша, чи прізвище та ім’я улюбленого актора. Також на сьогодні практичним є шифрування з відкритим ключем. При створенні цього класу шифрів є генерація двох ключів. Один відкритий ключ поширюється по відкритих каналах зв’язку й використовується при шифруванні повідомлень, на прийомній стороні за допомогою секретного ключа проводиться розшифрування повідомлення.

Список літератури: 1. Безпека комп'ютера. Як придумати надійний пароль? [Електронний ресурс]. – Режим доступу до ресурсу: https://winpcguide.ru/the-security-of-your-computer/