ISSN 2224-087X. Електроніка та інформаційні технології. 2017. Випуск 8. С. 3–17
Electronics and information technologies. 2017. Issue 8. P. 3–17

ОГЛЯДОВІ СТАТТІ

УДК 004.056.53:004.056.55

СУЧАСНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Ю. Корчак[1], Ю. Фургала[1], Л. Корчак[2]

[1] Львівський національний університет імені Івана Франка,
вул. ген. Тарнавського, 107, 79017 Львів, Україна
yurakorchak@yahoo.co.uk

[2] Національна академія сухопутних військ імені гетьмана Петра Сагайдачного,
вул. Героїв Майдану, 32, 79012 Львів, Україна

Наведено огляд стеганографічних та біометричних методів і засобів захисту інформації, а також паролів, їхній сучасний стан, перспективи. Особливу увагу приділено методам створення паролів, вимогам до їхньої довжини та якості. Розглянуто етапи використання стеганографії для інформаційної безпеки й описано низку прикладних програмних інструментів для створення стеганографічного повідомлення та проведення стеганалізу. Сьогодні бурхливо розвиваються біометричні методи захисту інформації, які здатні з найбільшою імовірністю ідентифікувати особу. Описано сучасні технології та пристрої, які використовують для ідентифікації відбитків пальців особи, що дає змогу забезпечити надійний захист від несанкціонованого втручання.

Ключові слова: інформаційна безпека, пароль, стеганографія, стеганаліз, біометрика, дактилоскопія.

Широке застосування інформаційних технологій у практичній діяльності людини в поєднанні зі зростанням обсягу мережевих операцій зумовило необхідність посилення захисту інформації на комп'ютерах і в мережах.

Чому ж проблема захисту "комп'ютерної" інформації сьогодні вийшла на перше місце серед усіх завдань, пов'язаних із впровадженням інформаційних технологій? Сучасні комп'ютерні системи контролюють і керують роботою:

- понад 40 тис. ядерних боєголовок;
- десятками тисяч найскладніших хімічних виробництв і величезних заводів;
- тисячами літаків, які одночасно перебувають у повітрі;
- понад 670 промисловими ядерними реакторами;
- сотнями навігаційних, дослідницьких і військових супутників.

Збиток від "комп'ютерних" злочинів щорічно оцінюють десятками мільярдів у грошових одиницях країн, найбільш розвинених у застосуванні інформаційних технологій.

Сьогодні є достатньо методів і засобів захисту інформації від несанкціонованого втручання. Це і створення надійних та якісних паролів, і біометричні методи захисту інформації, і стеганографія, і криптографія. Однак вони потребують постійного вдосконалення та модернізації, оскільки зловмисники використовують щоразу новіші технологічні ідеї і досягнення для злочинних цілей. Криптографічні методи пов'язані з певним

шифруванням інформації, вони становлять левову частку кібербезпеки. Описові їхнього сучасного стану можна присвятити окрему статтю. Нижче розглянемо детальніше перші три групи методів захисту інформації.

Паролі, вимоги до їхнього створення. Паролі стоять на варті наших даних. Ступінь їхньої надійності відіграє надзвичайно важливу роль. Зрозуміло, що складний пароль і зламати непросто. Ось тільки особистих рахунків і систем, які потребують авторизації, дуже багато. І пам'ятати десятки, якщо не сотні різних комбінацій із символів практично неможливо.

Хороші паролі важко запам'ятати, а шаблон, який робить пароль легким для запам'ятовування, найшвидше, зробить його вразливим для атак. Якщо запам'ятати один безпечний пароль важко, то запам'ятовування декількох таких паролів повністю непрактично.

Отже, люди часто створюють один хороший пароль і використовують його для різних облікових записів. Згідно з дослідженнями RSA, саме так діють 69 % користувачів [1]. У цьому випадку порушення безпеки в будь-якому місці, де цей пароль використовують, означає, що стають вразливими всі системи, де цей пароль застосовано.

Значно безпечніше мати різні паролі для кожного облікового запису. Тоді, якщо пароль скомпрометований, втрата обмежується одним обліковим записом.

Неможливо придумати надійний пароль, не знаючи методи роботи зловмисників. Найпоширеніші способи підбирання і зламу паролів такі:

– найпопулярніший і водночас найменш ефективний спосіб зламу пароля – *ручне підбирання*. Найпростіше вручну підібрати комбінації, що складаються з цифр (1, 2, 3 і т.д.), слова "код", "пароль", а також імені, прізвища та дати народження. А ось пароль вигляду "5-ий пАрольЧик" буде нелегко зламати методом ручного підбирання, якщо й взагалі неможливо;

– *метод* "*грубої сили*" (англ. *Brute force*) – це вже підбирання комбінацій, яке виконує спеціально створена для цього програма в автоматичному режимі. У разі використання цього методу участь людини не потрібна. Неважко здогадатися, що чим менше символів у вашому паролі, тим швидше його розгадає штучний інтелект. Виділяють два види підбирання в автоматичному режимі: словниковий і символьний. Перший полягає в перебиранні значень зі словникового запасу програми, тому паролі, що складаються з елементарних слів типу "мама", "музика", дуже ненадійні. Символьний вид методу "грубої сили" є послідовним перебиранням значень (*а*, *б*, *в* ... *аа*, *AB*, *AC* і т. д.);

– ще один відомий спосіб крадіжки пароля – це інфікування комп'ютера вірусом. Тут уже зовсім неважливо, чи складається пароль з пари символів, чи з п'ятнадцяти, тому що вірус зможе викрасти будь-яку інформацію, що міститься на ПК або введена на сайтах інтернету. Запобігти цьому може тільки антивірус, який регулярно оновлюють.

Далі розглянемо декілька методів створення паролів, які, з одного боку, будуть надійними, а з іншого боку, їх легко запам'ятати [1].

Шифри заміни – клас методів шифрування, який існує практично стільки ж, скільки й абетка. Його зміст полягає в заміні літер іншими літерами, цифрами чи символами. Не заглиблюючись в особливості й тонкощі шифру, можна вибрати найпростіший метод шифрування – той, де кожну літеру замінюють наступною за нею в абетці. Наприклад, зашифруємо слова *car* і *bus*: після *c* в абетці йде *d* ($c = d$), після *a* буде *b* ($a = b$), після *r* є *s* ($r = s$). Та ж формула і для іншого слова: $b = c$, $u = v$, $s = t$. Як наслідок, отримуємо два шифри – *dbs* і *cvt*. Цей метод не можна назвати достатньо надійним. Його все-таки не складно зламати, якщо порівняти декілька зашифрованих речень чи знати принципи

використання. Однак можна поекспериментувати й урізноманітнити метод. Наприклад, задати власний порядок заміни літер, додати цифри тощо.

Мнемонічний метод допомагає візуалізувати об'єкт за допомогою його повного опису, спрощуючи запам'ятовування чи ідентифікацію. У спрощеному вигляді отримуємо приблизно таке: "*а* – це ананас, *б* – це банан, *в* – це вишня". Наприклад, потрібно створити пароль для сайту *bank.com*. Візьмемо за основу код з перших двох літер від назви веб-ресурсу *b* і *a*. Згідно з конструкцією "*b is for banana, a is for apple*" отримаємо *bananaapple*. Якщо додати між ними дефіс, то пароль набуде ще й необхідного спеціального символу. А якщо об'єднати це все з шифром простої заміни, де наступними є літери і символи з клавіатури, то пароль для *bank.com* стане справді надійним *nsmsms=s[[;r*.

Технічний директор компанії з мережевої безпеки "Panda Security" Луїс Корронс пропонує такий варіант: щоб зробити пароль унікальним і зрозумілим для кожного сайту (без потреби його записувати), можна додати назву веб-ресурсу в його кінець. Розглянемо це на прикладі того ж сайту *bank.com*. До вибраного пароля в кінці додамо *-bank*. Отримаємо складнішу конструкцію, яка робить пароль і зрозумілим, і складним. Те ж саме можна реалізовувати з обліковими записами в соціальних мережах *-twitter*, *-facebook* і *-linkedin* чи скорочені варіанти типу *-twit*, *-face* і *-link*.

Мануель Блюм, професор обчислювальних наук з Університету Карнегі Меллона (США), лауреат премії Т'юрінга 1995 р., запропонував метод паролів, які "обчислює людина" [2]. Переваги методу в тому, що паролі отримують досить складними, та найголовніше – їх не потрібно запам'ятовувати. Якщо запам'ятати сам алгоритм обчислення паролів і наперед обраний єдиний ключ, то згодом за адресою сайту можна самостійно швидко генерувати і відтворювати паролі. Суть методу полягає в тому, що за допомогою алгоритму і ключа кожній літері адреси сайту ставлять у відповідність іншу літеру чи цифру. Їхня комбінація надалі і є паролем.

Наприклад, використаємо ключ у вигляді матриці 6×6, яка заповнена 26 літерами (англійська абетка) і 10 цифрами (табл. 1).

Таблиця 1

Зразок ключа для створення паролів за методом Блюма

E	T	A	O	I	N
S	H	R	D	L	U
C	M	F	W	Y	P
V	B	G	K	Q	J
X	Z	1	2	3	4
5	6	7	8	9	0

Далі потрібно вибрати алгоритм, відповідно до якого літери адреси замінюватимуться символами з матриці. Для розглядуваного прикладу використаємо запропонований Блюмом алгоритм, який ґрунтується на "чергуванні сторін світу".

Створимо пароль для сайту *Champion*. Для цього знаходимо літеру *C* в матриці і переходимо на одну клітинку на "північ". У цьому випадку літера *S* замінює літеру *C*. Далі знаходимо літеру *H* і замінюємо її на символ, який є на "сході", – *R*. Наступний символ беремо з "півдня", тобто літеру *A* замінюємо літерою *R*, літеру *M* замінюємо "західним" символом *C* і так далі; послідовно проходячи всі сторони світу за годинниковою стрілкою: північ, схід, південь, захід, отримуємо пароль SRRCUNDI (табл. 2). Якщо символ, для якого шукають заміну, розміщений на краю матриці і в нього немає потріб-

ної “сторони світу”, то беруть той символ, який міститься найближче за годинниковою стрілкою. Наприклад, якщо для *J* потрібно взяти символ зі “сходу”, то беруть *4*, оскільки “південь” є після “сходу” в цьому алгоритмі.

Таблиця 2

Приклад створення пароля для веб-сайту *Champion* за методом Блюма

C	H	A	M	P	I	O	N
S	R	R	C	U	N	D	I

Звичайно, можна модифікувати цей метод для ускладнення пароля, наприклад, додавши у ключ спеціальні символи або використавши нижні і верхні регістри. Можна застосовувати й інші алгоритми для підбирання замін.

Зрозуміло, що цей спосіб не надто зручний для випадків, коли потрібно часто вводити пароль на якомусь ресурсі. З іншого боку, досить швидко його можна запам’ятати, тримаючи алгоритм у голові і ключ під рукою. Зате можна забути про генератори паролів, запам’ятовування комбінацій, переживання, що хтось дізнається про часто використовуваний пароль.

Є компанії, які змушують своїх клієнтів змінювати паролі раз у півроку чи рік. Тут теж можна знайти вихід з ситуації. Просто додавати необхідний рік, квартал до початку чи у кінці пароля. Візьмемо за основу вже відомий пароль “*banana*”, додамо до нього 2018 рік і перший квартал. Отримаємо *banana-16-q1*. А якщо виконати зміщення всього по одному ключу на клавіатурі, то пароль значно ускладниться і набуде вигляду *nsmsms=27=w2*. Маємо унікальний код, досить складний, надійний, який можна запам’ятати і без особливих труднощів регулярно змінювати (за місяцями чи роками).

Окрім шифрування, важливе значення має якість самого пароля, тобто його довжина, а також те, які символи використовують для створення. Повний набір символів може містити 26 літер (верхній і нижній регістри) у випадку англійської абетки, 10 цифр і приблизно 30 спеціальних символів. З застосуванням сервісу перевірки складності паролів GRC password crack checker [3] оцінено час зламу пароля “Великим масивом для зламу” залежно від його довжини і використаних символів. Результати аналізу наведені в табл. 3. І хоча “Великий масив для зламу” складається з 24 звичайних GPU, оптимізованих для швидкого підбору хешів, сьогодні він доступний для будь-якого агентства і середнього бізнесу. Їх також не обов’язково купувати, а можна орендувати – наприклад, у хмарі.

Таблиця 3

Залежність часу зламу паролів від їхньої довжини і використовуваних символів

Довжина пароля	Час зламу			
	літери + цифри		літери + цифри + спецсимволи	
	літери одного регістру	літери обох регістрів	літери одного регістру	літери обох регістрів
8 символів	0,03 с	2,22 с	5,21 с	1,12 хв
9 символів	1,04 с	2,29 хв	6,00 хв	1,77 год
10 символів	37,61 с	2,37 год	6,89 год	1 тиждень
11 символів	22,56 хв	6,12 дня	2,83 тижня	1,83 року
12 символів	13,54 год	1,04 року	3,74 року	1,74 століття

За словами генерального директора фірми мережевої безпеки “FlowTraq” Вінсента Берка [1], більшість веб-сайтів і компаній потребують паролі, які налічують комбінацію мінімум з десяти символів нижнього і верхнього регістру, у цьому разі використовують цифри і спеціальні символи. Останнім часом спеціалісти з безпеки все ж рекомендують збільшувати довжину пароля до дванадцяти знаків. Ці рекомендації яскраво підтверджують дані табл. 3.

Зрозуміло, що не лише довжина робить пароль надійним. Він не повинен бути легким для вгадування чи передбачуваним. Наприклад, пароль *LadyGaga* – хороший лише для відданого прихильника чи самої співачки. Набір цифр *1234567890* теж не підходить – надто очевидно, що навіть дитина може його зламати, набираючи підряд усі десять цифр на клавіатурі. Ненадійним буде і комбінація з серії *password1234*, нехай навіть вона складається з дванадцяти символів.

Доцільно придумувати складні й не поширені паролі. Найліпше уникати слів, які можна знайти в словниках будь-якої мови. Популярні заміни літер числами (0 замість “*o*”, 4 замість “*ч*”) не відіграють особливої ролі. Більшість експертів з безпеки вважають, що паролі повинні бути легкими для запам’ятовування, але важко вгадуваними. Надто складні й незрозумілі комбінації з символів просто забудуть. А записувати паролі на стікерах, папірцях, у блокнотах чи ще десь – не найліпша ідея. У цьому випадку ліпше обмежитися підказкою, зрозумілою тільки господарю і нікому іншому.

Як пароль можна використовувати фразу, попередньо закодувавши її. Наприклад, англійською “*I want to be at the beach*” у кодуванні матиме вигляд *iw2b@theBeach*. Отримаємо пароль, який легко запам’ятати, але важко зламати. Під кожну систему можна підібрати різне закінчення. Деякі люди використовують повні речення як паролі. Такі паролі легко запам’ятати, а з додаванням спеціальних символів і цифр вони стають дуже надійними.

У 2016 р. відбулося багато різних витоків даних. Компанія “Keeper”, яка займається питаннями кібербезпеки, на початку 2017 р. опублікувала нове дослідження, присвячене найпопулярнішим паролям 2016 р. [4]. Команда дослідників опрацювала 10 мільйонів паролів, які стали доступними після витоків. Вона з’ясувала, що найпопулярнішим паролем і надалі є *123456* – таких паролів було майже 17 % від загальної кількості. Те ж саме було і в попередні роки, проте багато хто і далі не вчиться на чужих помилках. Далі йшли *123456789* і *qwerty*. Загалом усі найпопулярніші паролі були створені за банальними шаблонами, хоча є декілька винятків. Зокрема, у статистику потрапили два незвичайні паролі *3rjs1la7qe* і *18atcskd2w*. На думку дослідника Грема Клюлі, вони, найшвидше, були створені спам-ботом. Виділимо також пароль *mynoob*, який, мабуть, придуманий людьми. Компанія “Keeper” завершила доповідь, заявивши, що основна відповідальність повинна лежати на власниках сайтів, які мають впроваджувати жорстку політику використання складних паролів.

Отже, ось топ-25 паролів 2016 р.: *123456*, *123456789*, *qwerty*, *12345678*, *111111*, *1234567890*, *1234567*, *password*, *123123*, *987654321*, *qwertyuiop*, *mynoob*, *123321*, 666666, *18atcskd2w*, *7777777*, *1q2w3e4r*, *654321*, *555555*, *3rjs1la7qe*, *google*, *1q2w3e4r5t*, *123qwe*, *zxcvbnm*, *1q2w3e*.

Для підвищення безпеки даних відомим хмарним сервісом *Dropbox* створено перелік паролів, які заборонені для використання. У переліку є 85 100 паролів [5].

Біометричні методи захисту інформації. Сьогодні щораз більшої популярності набувають *біометричні методи захисту інформації* – методи, у яких ідентифікація користувача відбувається за допомогою технічних пристроїв біологічних характеристик

особи та перевірки їхньої відповідності заздалегідь сформованим особистим шаблонам. У цьому випадку використовують такі фізіологічні параметри людини, як відбитки пальців або долоні, зображення обличчя, райдужна оболонка або сітківка ока, голос, ДНК тощо.

Застосування цих технологій має певну історію, а їхнє "друге народження" почалось після відомих терористичних атак 11 вересня 2001 р. Наслідками стали бурхливий розвиток біометричних технологій та їхнє широке впровадження у системи безпеки різноманітного призначення. Відбулося значне здешевлення такої апаратури за підвищення безпомилковості її роботи. Звичайно біометричні методи поділяють на статичні, коли відповідні ознаки особи практично не змінюються в часі, та динамічні, які використовують дані про особливості поведінки людини.

Оскільки дактилоскопічні біометричні системи сьогодні найпоширеніші (становлять 58 % від загальної кількості біометричних систем захисту інформації [6]), то розглянемо саме їх детальніше.

Відомо, що пальці людини мають унікальний папілярний візерунок, незмінний протягом усього життя. Імовірність його повторення в іншої людини – менше 10^{-9}. Він є різним навіть в однояйцевих близнюків з однаковим набором хромосом, тому давно став своєрідним "посвідченням" для ідентифікації особи. Вірогідність повторення в іншої людини папілярних візерунків одночасно двох сусідніх пальців – уже менше 10^{-18} [7].

У розкопках дохристиянських часів у Китаї, Вавилоні, Ассирії знайдено глиняні печатки владик і членів уряду, на яких зафіксовано відбитки пальців. У старовинних рукописах написано про те, що такі відбитки сприймали як посвідчення особи чи як власноручний підпис людини, а також про те, що китайські матері вивчали, прекрасно знали і могли впевнено розпізнати відбитки пальців своїх дітей.

Папілярний візерунок формується з невеликих (висотою 0,1–0,4 мм, шириною 0,2–0,7 мм) виступів шкіри і міні-канавок між ними (шириною 0,1–0,3 мм). На рис. 1 показано три основні типи папілярних візерунків – дугові, петльові, завиткові. За сотні років розвитку дактилоскопії вони добре деталізовані, класифіковані; розроблено методи їхньої індивідуалізації та ідентифікації. Типи папілярного візерунка – це "деталі першого рівня" (див. рис.1).

а *б* *в*

Рис. 1. Типи папілярних візерунків:
дуговий (*а*), завитковий (*б*), петльовий (*в*) [8].

Для точнішої ідентифікації розглядають і перевіряють мінімум ще деталі другого і третього рівнів. Деталі другого рівня – це види закінчень папілярних ліній, їхніх розгалужень, з'єднань, перетинів, зарубцювань тощо (рис. 2). На одному пальці налічується близько 100 таких деталей. Деталі третього рівня – це деталі кожної окремої папілярної лінії: її згини, звуження і розширення, відхилення від періодичності, відмінності між

виступами та ін. Виявляють і фіксують ще багато дрібніших деталей: виходи потових залоз, мікроскопічні дихальні пори у шкірі тощо.

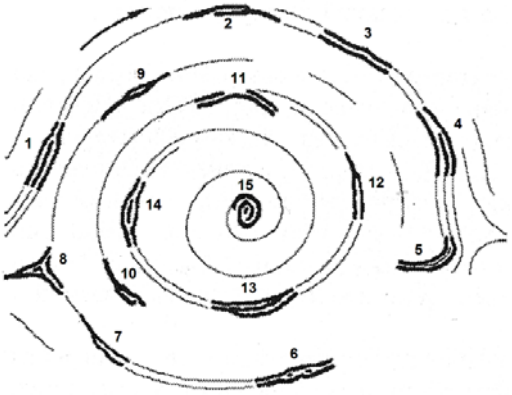

Рис. 2. Схематичне зображення особистих ознак:
1 – закінчення; 2 – зустрічне розташування; 3 – згин; 4 – початок; 5 – міжкапілярна лінія; 6 – точки; 7 – злиття; 8 – дельта; 9 – око; 10 – гачок; 11 – розрив; 12 – розгалуження; 13 – місток; 14 – фрагмент; 15 – центр узору [8].

З розвитком обчислювальної техніки розроблено детальні алгоритми і комп'ютерні програми ідентифікації відбитків пальців. Створено спеціалізовані комп'ютерні сканери відбитків пальців і методи відображення їх у цифровому вигляді. Однак тривалий час для оброблення отриманої інформації потрібні були надто великі обчислювальні ресурси і застосування дорогих надшвидкісних комп'ютерів. Проте бурхливий розвиток технології, математики й інформатики привів до того, що стало можливим створення компактних інтелектуальних дактилоскопічних сенсорів [7]. Іноді їх називають також *біометричними*. Чутливим вузлом таких сенсорів є вузол сканування, у якому папілярному візерунку одного, двох чи декількох пальців ставлять у відповідність послідовність електричних сигналів. Найбільш поширені нині ємнісні, потенціальні, теплові і фоточутливі сканери.

У фоточутливих сканерах збільшене зображення папілярного візерунка оптично проектується зі збільшенням на лінійку чи матрицю фотоприймачів, які перетворюють його у послідовність електричних сигналів.

Мікропроцесор, який входить до складу дактилоскопічного сенсора, не тільки організовує зчитування і фільтрування інформації про папілярний візерунок пальців, а й обробляє її, приводить до стандартної форми. Він же виконує порівняння зі зразками типових візерунків, які зберігаються в його довготривалій пам'яті, і за заданими критеріями вирішує, яким зразкам відповідають досліджувані пальці. Тобто він автоматично виконує ту складну роботу, яку протягом попередніх століть могли виконати лише висококваліфіковані експерти.

Дактилоскопічні сенсори мають низку застосувань. Компанія "Sharp", наприклад, використала біометричний сенсор AT77C101B FingerChip™ [9] у мобільному планшетному персональному комп'ютері Sharp Mebius Muramasa PC-TN1-H1W для контролю доступу. Контроль цей ґрунтується на оперативній перевірці відбитків пальців користувача. Компанія вважає, що біометричний сенсор "забезпечує користувачеві високий

рівень захисту приватної, бізнесової та іншої закритої інформації, неможливість несанкціонованого використання комп'ютера при збереженні зручності" [8]. Для доступу до операційної системи і бази даних зареєстрованому користувачеві достатньо провести пальцем по сенсору AT77C101B FingerChip™. У цьому сенсорі застосовують тепловий сканер розміром 26,6×9,8×1,5 мм, виготовлений з використанням КМОН-технології з роздільною здатністю 20 точок/мм. Стверджують, що "теплова технологія" добре працює навіть за таких несприятливих умов, як підвищена вологість, забрудненість, жир на пальцях, спека чи мороз.

Компанія "CardMedia" випустила на ринок флеш-брелоки *StoreGuard* ємністю 128, 256, 512 Мб і 1 Гб із вбудованим дактилоскопічним сенсором, який відкриває доступ до записаної інформації лише господарю після аналізу папілярного візерунка його пальців. Час перевірки становить близько 0,25 с. Дактилоскопічно захищені флеш-пристрої пам'яті продукують і пропонують також інші виробники [10].

Компанія "Microsoft", щоб звільнити користувача від потреби запам'ятовувати багато логінів і паролів для доступу до різних комп'ютерних та інтернет-ресурсів, застосувала "пристрій біометричної ідентифікації" MS Fingerprint Reader [11]. Це також спеціалізований інтелектуальний дактилоскопічний сенсор, який після аналізу папілярного візерунка пальців автоматично вводить необхідні в конкретній ситуації логін і пароль. Чутливий сканер сенсора вбудовують у клавіатуру комп'ютера чи в маніпулятор мишу (рис. 3). Конструкція MS Fingerprint Reader має змогу реєструвати й обслуговувати не одного, а декількох користувачів офісного комп'ютера.

Рис. 3. Маніпулятори комп'ютерні миші з вбудованим чутливим сканером дактилоскопічного сенсора [11].

Компактні сканери для дактилоскопічних сенсорів виробляють японська компанія "Fujitsu" (ємнісний сенсор MBF300, 20 точок/мм), американська компанія "AuthenTec" (світлочутливий сенсор EntrePad площею лише 6,5 мм^2), компанії "Precise Biometrics", "Applied Biometrics Products", "Mytec" та ін. Ці сканери призначені для застосувань з метою ідентифікації господаря у фірмових мобільних телефонах, органайзерах, ноутбуках та інших важливих мобільних пристроях.

У 2013 р. компанія "Apple" уперше використала в iPhone 5s біометричний сенсор Touch ID [12]. КМОН-сенсор Touch ID є набором мікроконденсаторів, що створюють образ з рельєфом пальця, який прикладають, тобто його відбиток. Технологія розроблена компанією "AuthenTec". Дактилоскопічний сенсор iPhone 5s, вбудований у кнопку Home, за товщини 170 мікронів (приблизно вдвічі товстіший, ніж людська волосина) аналізує субепідерміальні шари шкіри і дає змогу отримати зображення з розділенням 500 ppi. Це забезпечує надзвичайно високу точність розпізнавання (рис. 4).

Рис. 4. Використання дактилоскопічного сенсора Touch ID у iPhone 5s [12].

Користувач може навчити Touch ID розпізнавати декілька пальців, причому торкатися сенсора можна як завгодно – орієнтація пальця значення не має. До речі, кнопка Home, починаючи з цієї моделі, втратила фірмовий квадрат із закругленими кутами, ззовні вона покрита сапфіровим склом для захисту від подряпин, які могли б погіршити ефективність роботи дактилоскопічного сенсора. У всіх наступних моделях смартфона iPhone компанія "Apple" продовжила вбудовувати Touch ID, який використовують для розблокування смартфона й авторизації покупок у App Store.

Компанія "BioLink Technologies" розробила і пропонує інтелектуальний сенсор контролю доступу BioLink OBE Module DDK (On-Board Extraction Module Design Development Kit) [13]. У ньому використовують оптичний пристрій з площею сканування 24×16 мм і ПЗЗ-матрицю. У пам'яті сенсора можуть зберігатися зразки відбитків пальців до 150 різних осіб. Такі сенсори можуть встановлювати на вході у приміщення чи на територію, куди дозволений доступ лише наперед визначеним особам, і виконувати функції непідкупного електронного охоронця чи контролера-лічильника робочого часу. Їх уже встановлюють як основний засіб захисту від несанкціонованого доступу на деякі моделі сейфів, банківські депозитарні комірки, банкомати і касові термінали, дверцята енергетичних щитів, вузлів інформаційних з'єднань, автомобілів тощо.

Стеганографія. *Стеганографія* (від грец. *steganos* – секрет, таємниця, і *graphy* – запис) дослівно означає тайнопис, хоча методи стеганографії з'явились, імовірно, раніше, ніж сама писемність (спочатку використовували умовні знаки і позначення).

Стеганографія відома ще з часів Геродота. У Давній Греції послання писали гострими паличками на дощечках, покритих воском. В одній з історій Демерат хотів надіслати в Спарту повідомлення про загрозу нападу Ксеркса. Тоді він зняв віск з дощечки, написав послання безпосередньо на дереві, далі знову покрив її воском. Дощечка виглядала як невикористана і її без проблем пропустили центуріони. Ще один досить несподіваний спосіб приховування інформації чи умовних знаків – татуювання на голові побритого посланця. Коли в V ст. до н.е. тиран Гістій, перебуваючи під наглядом царя Дарія в Сузах, мав надіслати таємне повідомлення своєму родичеві в анатолійське місто Мілет, він побрив наголо свого раба і витатуював повідомлення на його голові. Коли волосся знову відросло, раба відправили в дорогу. Так Геродот описав один з перших випадків застосування у давньому світі стеганографії – мистецтва прихованого письма [14].

Надалі для захисту інформації стали використовувати ефективніші методи кодування і криптографії. Від криптографії стеганографія відрізняється тим, що за допомо-

гою криптографії можна приховати зміст повідомлення, а користуючись стеганографією, – власне існування повідомлення. Комп'ютерні технології надали нового імпульсу розвиткові й удосконаленню стеганографії, з'явився новий напрям у галузі захисту інформації – комп'ютерна стеганографія.

Комп'ютерна стеганографія – це приховування повідомлення чи файлу в іншому повідомленні чи файлі. Наприклад, стеганографи можуть сховати аудіо- чи відеофайл в іншому інформаційному чи навіть у великому графічному файлі.

Боротьба з тероризмом і переслідування винних у вчиненні терористичного акту 11 вересня 2001 року привернули особливу увагу до стеганографії. Деякі фахівці вважають, що терористична організація Аль-Каїда використовувала інтернет для розробки плану нападу, а стеганографія допомогла зберегти в таємниці їхні злочинні наміри.

Процес стеганографії можна розділити на декілька етапів:

– *вибір інформаційного файлу*. Першим етапом у процесі стеганографії є вибір файлу, який потрібно сховати. Його ще називають *інформаційним файлом*;

– *вибір файлу-контейнера*. Другим етапом у процесі стеганографії є вибір файлу, який використовують для приховування інформації. Його ще називають *файлом-контейнером*. У більшості відомих програм зі стеганографії зазначають, що для приховування інформації ємність пам'яті файлу-контейнера повинна приблизно у вісім разів перевищувати ємність пам'яті інформаційного файлу. Звідси, щоби приховати файл розміром 710 кБ, знадобиться графіка об'ємом 5 600 кБ;

– *вибір стеганографічної програми*. Третім етапом у процесі стеганографії є вибір стеганографічної програми.

Одним з найліпших і найпоширеніших продуктів у цій галузі для платформ Windows є S-Tools (Steganography Tools, має статус freeware). Програма дає змогу ховати будь-які файли як у зображеннях растрових форматів GIF і BMP, так і в аудіофайлах формату WAV. Тобто S-Tools – це стеганографія і криптографія в одному, тому що файл, який потрібно приховати, ще й шифрують за допомогою одного з криптографічних алгоритмів з симетричним ключем: DES (уже не використовують), потрійний DES чи IDEA (сьогодні цілком заслуговують на довіру) [15]. Приклад використання цієї програми показано на рис.5.

а *б*

Рис. 5. Приклад використання програми S-Tools для приховування інформаційного файлу:
початкове зображення (*а*); приховане зображення (*б*) [16].

Інша поширена стеганографічна програма – Steganos for Windows, яка є легкою у користуванні, та все ж потужною програмою для шифрування файлів і приховування їх усередині BMP-, DIB-, VOC-, WAV-, ASCII- та HTML-файлів. Вона надає практично ті ж можливості, що й S-Tools, проте використовує інший криптографічний алгоритм

(HWY1), і здатна приховати дані не тільки у файлах форматів BMP і WAV, а й у звичайних текстових та HTML-файлах, причому досить оригінальним способом – у кінці кожного рядка додається певна кількість пробілів. З новими властивостями і додатковими можливостями Steganos for Windows є серйозним конкурентом на ринку інформаційної безпеки для приховування файлів Contraband – програмне забезпечення, яке дає змогу сховати будь-які файли в 24-бітових графічних файлах формату BMP [17].

Ще одна програма – JSteg – призначена для приховування інформації у файлах формату JPEG. Ця програма використовує для приховування інформації спектральні коефіцієнти дискретного косинусного перетворення. Коефіцієнти, які дорівнюють нулю або одиниці, не змінюються, а інші можуть бути використані для вбудовування в них одного біта прихованої інформації з використанням алгоритму заміни найменшого значущого біта.

Однією з найпростіших програм є Hide-in-Picture, яка дає змогу закодувати та приховати будь-які файли у зображеннях. Ця програма створює додаткові записи колірної палітри, тому вихідне зображення на початку має 32 кольори, а згенероване зображення з прихованою інформацією доповнює це число до 256 завдяки створенню нових кольорів [16];

– *кодування файлу*. Після того, як обрано інформаційний файл, файл-контейнер і програмне забезпечення зі стеганографії, необхідно встановити захист нового файлу за паролем;

– *відсилання прихованого повідомлення електронною поштою та його декодування*. П'ятим, і останнім, етапом у процесі стеганографії є відсилання прихованого файлу електронною поштою та його подальше розшифровування, яке пов'язане зі *стеганалізом* (методом виявлення стеганографії і знищення початкового повідомлення). Сьогодні існує достатня кількість програмних інструментів, які виконують стеганаліз. Серед них можна виділити StegDetect, FTK Imager, Stegosuite, File Signature Header, Maresware Forensic Suite. Розглянемо коротко кожен із них:

StegDetect – перевіряє найдоступніші сховища: поля-коментарі і поля розширення різних форматів файлів, наявність штучно створених зображень, а також зображень з великою кількістю ділянок однотипного заливання. Програма порівнює частоту розподілу кольорів для можливого носія прихованої інформації. Вона дає достатньо об'єктивні результати у тому випадку, коли вміст інформаційного файлу перевищує 10 % об'єму файлу-контейнера [18];

FTK Imager – дає змогу швидко створити образ жорсткого диска для подальшого вивчення, а також паралельно переглянути файли MS Office, архівів чи зображень. Аналіз даних виконується завдяки вбудованій у програму базі контрольних сум – усі файли, які містять інформаційні файли чи додаткові зміни, відразу відображаються [19];

Stegosuite – автоматичний програмний сканер, який містить дев'ять стеганографічних алгоритмів детектування, розрахованих на всі типи файлів цифрового зображення й аудіофайлів. Містить два модулі: Stego Analyst – візуальний аналітичний пакет для всебічного аналізу цифрових зображень і аудіофайлів; Stego Break – інструмент зламу стеганографічного захисту. Stego Suite змінює молодші розряди кожного байта мультимедіафайлу на нульовий біт, знищуючи несанкціоноване передавання даних [20];

File Signature Header – визначає можливість приховування інформації у файлах зі зміненим розширенням. Наприклад, якщо файл зображення test.jpg перейменувати на test.txt, то ОС Windows відкриє його в блокноті – замість зображення отримаємо беззмістовний текст. Ця програма дає змогу не тільки визначити належність якого-небудь фай-

лу, а й, частково, ідентифікувати програму, яка його створила, чи звернути увагу на якінебудь файли, а далі вже використати програму Stegdetect [21];

Maresware Forensic Suite – містить усі можливі стандарти – створення і відтворення образу, підрахунок і порівняння контрольних сум, перевірка на hash sets, file signature header, пошук за багатьма параметрами, включаючи ADS для NTFS, визначення файлів PGP тощо. Кожна з утиліт, яка входить до Maresware Forensic Suite, може працювати як окремий продукт. Ця програма створена для роботи в середовищі Linux&Unix [22].

Розглянемо детальніше декілька основних механізмів, які використовують у стеганографії для приховування інформаційного файлу. Сьогодні будь-яка форма даних, така як текст, зображення, аудіо- чи відеоінформація, може бути переведена в цифрову форму, і під час перетворення в цифрову форму чи обробки можна в загальні дані вставити таємну двійкову інформацію. Таку приховану інформацію не обов'язково використовують для збереження таємниці. Її можуть також застосовувати як відмітку, щоб захистити авторське право, запобігти втручанню чи внести додаткову інформацію, яка коментує текст для деякого отримувача [23].

Тексти, які приховують. Для непомітного передавання таємних даних можна використати звичайний текст. Є декілька способів. Один з них – вставлення двійкових символів. Наприклад, можна використовувати пробіл між словами. Щоб зобразити двійкову цифру 0, використовують одинарний пробіл, а для відображення двійкової цифри 1 – два пробіли. Наведене нижче коротке повідомлення приховує двійкове 8-бітове відображення літери A (01000001) у коді ASCII.

Інформаційна безпека є однією із найважливіших пріоритетів будь-якої держави.
0 1 0 0 0 0 0 1

У наведеному вище повідомленні два пробіли стоять між словами "безпека" і "є" та між "будь-якої" і "держави". Звичайно, ускладнене програмне забезпечення може вставити пробіли, які розрізняються мінімально, щоби приховати код від безпосереднього візуального розпізнавання.

Інший, ефективніший метод використовує словник слів, які організовані згідно з їхніми граматичними значеннями (частинами мови). Нехай, наприклад, є словник, який містить 2 займенники, 16 дієслів, 32 іменники (підмети), 64 іменники (додатки). За кожним представником цього словника закріплено код. Нехай перший біт двійкових даних може бути представлений займенником, кожний з яких має код (наприклад, "я" – це 0, а "ми" – це 1). Наступні п'ять бітів можуть бути представлені іменником (наступним словом у реченні). У нашому прикладі можна позначити код 10010 словом "водій". Подальші чотири біти можуть позначати дієслово (у прикладі – словом "керую", яке представляє код 0001), і останні шість бітів – іншим іменником. У нашому прикладі "машиною" означає код 001001. Тоді можна домовитися застосовувати приховувальний текст, який завжди використовує речення типу *займенник – іменник – дієслово – іменник*. Таємні двійкові дані можуть бути розділені на проміжки по 16 бітів. Наприклад, таємне повідомлення "Ні", яке в ASCII відображене 0 10010 0001 001001, може бути приховане таким реченням:

Я водій керую машиною.
0 10010 0001 001001

Це – дуже тривіальний приклад. Реально застосовують складніший алгоритм і велике різноманіття використовуваних слів для одного й того ж коду.

Методи приховування, які використовують зображення. Дані можуть бути приховані іншим кольоровим зображенням. Переведені у цифрову форму зображення складаються з пікселів (елемент картинки), зазвичай, кожний піксель використовує 24 біти (три байти). Кожний байт відображає один з первинних кольорів (червоний, зелений чи синій). У підсумку отримують 2^8 різних відтінків кожного кольору. У методі, який називають LSB (Last Significant Bit), наймолодший біт кожного байта встановлений на нуль. Від цього зображення стає дещо світлішим у деяких ділянках, однак це, зазвичай, не помітно. Тепер можна приховати двійкові дані в зображенні, зберігаючи чи змінюючи наймолодший біт. Якщо наша двійкова цифра – 0, то зберігається біт; якщо це – 1, то змінюється біт на 1. Цим способом можна приховати символ (вісім бітів ASCII) у трьох пікселях. Останній біт останнього пікселя не враховують. Наприклад, наступні три пікселі можуть відобразити латинську літеру *M* (4D16 чи, у двійковій системі, 0100 1101):

01010010 10111100 01010100
01011111 10111101 01100101
01111110 01001011 00010100

Інші методи приховування. Можливі також інші методи приховування. Таємне повідомлення, наприклад, може бути приховане аудіо- (звук і музика) та відеоінформацією. І аудіо, і відео сьогодні можна стиснути. Таємні дані можна внести в інформацію у процесі чи перед стисненням.

Отже, аналіз засобів захисту інформації дає змогу зробити такі узагальнення та висновки. Якщо дозвіл на певні дії в системі відбувається введенням пароля, що складається з набору символів, то на етапі створення системи логування розробникам треба уважно вибирати алгоритми хешування; під час експлуатації – своєчасно її оновлювати, використовувати хеші, які важко підбирати на GPU, наприклад, scrypt, а вибравши правильний хеш, обирати й правильні налаштування для його роботи. Користувачам бажано створювати випадкові паролі, не коротші за 12 символів.

Набагато вищий ступінь захисту від несанкціонованого доступу забезпечують системи на основі біометричної ідентифікації особи. Цей підхід має величезні переваги за швидкодією і надійністю. Саме цей метод інформаційної безпеки є одним з найперспективніших, його вже сьогодні досить широко використовують виробники електронної та комп'ютерної техніки.

Аналіз тенденцій розвитку комп'ютерної стеганографії засвідчує, що найближчим часом інтерес до розвитку її методів лише посилюватиметься. Передумови до цього вже сформувались. Зокрема, загальновідомо, що актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, бурхливий розвиток інформаційних технологій забезпечує можливість реалізації цих нових методів захисту. І зрозуміло, сильним каталізатором цього процесу є лавиноподібний розвиток інтернету, зокрема, такі невирішені проблеми, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, комп'ютерна злочинність і кібертероризм. Ще однією причиною підвищення інтересу до стеганографії є те, що низка країн прийняла обмеження на використання сильної криптографії і застосування стеганографії у цьому випадку є виходом із ситуації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Психическое криптография и хорошие пароли // Компьютеры, сети, программирование. – 2016. – № 7. – С. 10–12.
2. Метод Блюма // Компьютеры, сети, программирование. – 2016. – № 2. – С. 2–3.
3. GRC's Interactive Brute Force Password "Search Space" Calculator [Electronic resource]. – Mode of access : http://www.grc.com/haystack.htm
4. Найпопулярніші паролі 2016 року: 123456 та qwerty залишаються у топі [Електронний ресурс]. – Режим доступу : на http://osvita.mediasapiens.ua/web/cybersecurity
5. 85 тыс. паролей, которые запрещено использовать в Dropbox [Электронный ресурс]. – Режим доступа : https://tokar.ua/read/8193
6. *Чередниченко В. Б.* Біометричні методи у системах захисту інформації / В. Б. Чередниченко, К. Е. Чередниченко // Захист інформації в інформаційно-телекомунікаційних системах. – 2012. – Вип. 4 (102), т. 1. – С. 145–148.
7. *Войтович І. Д.* Інтелектуальні сенсори / І. Д. Войтович, В. М. Корсунський. – К. : Ін-т кібернетики ім. В. М. Глушкова, 2007. – 513 с.
8. *Русин Б. П.* Біометрична аутентифікація та криптографічний захист / Б. П. Русин, Я. Ю. Варецький. – Львів : Коло, 2007. – 287 с.
9. Thermal Fingerprint Sensor with 0.4 mm x 14 mm (0.02" x 0.55") Sensing Area and Digital Output (On-chip ADC) AT77C101B FingerChip™ [Electronic resource]. – Mode of access: http://web.sensor-ic.com:8000/JCCGQCX/sensor/AT77C101B.pdf
10. StoreGuard: USB-накопитель CardMedia на флэш-памяти с биометрическим сенсором [Электронный ресурс]. – Режим доступа : http://www.ixbt.com/news
11. Microsoft Fingerprint Reader [Electronic resource]. – Mode of access : http://en.wikipedia.org/wiki/Microsoft_Fingerprint_Reader
12. Як покращити точність роботи сканера відбитків пальців у iPhone 5S [Електронний ресурс]. – Режим доступу : http://svit-gadgetiv.blogspot.com/2013/12/yak-pokrashchyty-yakist-roboty-skanera-vidbytkiv-paltsiv-u-iphone-5s.html
13. *Лохтин А. А.* Анализ биометрических сканеров BioLink и их программного обеспечения / А. А. Лохтин // Захист інформації з обмеженим доступом та автоматизація її обробки : збірник ТЕЗ IV наук.-техн. конф. студентів та аспірантів, 9–10 лютого 2012 р. – Київ, 2012. – С. 56.
14. Стеганография // Компьютеры, сети, программирование. – 2015. – № 9. – С. 2–6.
15. *Карасев А.* Компьютерная тайнопись – графика и звук приобретают подтекст / А. Карасев // Мир ПК. – 1997. – № 1. – С. 132–134
16. *Лагун А.* Дослідження програмного забезпечення, яке використовує стеганографічні методи для приховування інформації в нерухомих зображеннях / А. Лагун, В. Пилипенко [Електронний ресурс]. – Режим доступу : ubgd.lviv.ua
17. Privacy Guide: Steganography [Electronic resource]. – Mode of access : http://www.all-nettools.com/privacy/stegano.htm
18. StegDetect [Electronic resource]. – Mode of access : https://app.assembla.com/wiki/show/Steganography/StegDetect
19. Forensic Toolkit (FTK). Digital Investigations [Electronic resource]. – Mode of access : http://www.accessdata.com/products-services/forensic-toolkit-ftk
20. Stegosuite [Electronic resource]. – Mode of access : https://stegosuite.org/
21. What is a File Signature? [Electronic resource]. – Mode of access : http://www.computer-forensics.net/what-is-a-file-signature.html

22. *Bidgoli H.* Handbook of Information Security. Vol. 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations / H. Bidgoli. – New Jersey : John Wiley & Sons, Inc., 2003. – 977 p.
23. Основні положення стеганографії [Електронний ресурс]. – Режим доступу : http://easy-code.com.ua/2010/11/osnovni-polozhennya-stenografiї/

Стаття: надійшла до редакції 18.09.2017,
доопрацьована 21.09.2017,
прийнята до друку 22.09.2017.

MODERN METHODS AND MEANS OF INFORMATION PROTECTION

Yu. Korchak[1], Yu. Furgala[1], L. Korchak[2]

[1]Ivan Franko National University of Lviv
107 Tarnavsky St., UA–79017 Lviv, Ukraine
yurakorchak@yahoo.co.uk

[2]Hetman Petro Sahaidachny National Army Academy
32 Heroes of Maidan St.,UA-79012 Lviv, Ukraine

The paper gives an overview of steganographic and biometric methods and means of information protection, as well as passwords, their current state and perspectives.

Particular attention is devoted to methods of creating passwords, requirements to their length and quality. Using the *GRC password crack checker* service, the analysis of the dependence of the password break time on its quality (length, type of characters used) is analyzed. It has been shown that for safe protection against unauthorized interference, the length of the password must be at least 12 characters, using upper and lower case letters, numbers and special characters. Several approaches to creating passwords are considered, including *replacement codes*, *mnemonic method*, *Blum's method*. An analysis of trends in the development of computer steganography shows that in the near future interest in the development of its methods will only increase. One of the reasons for increasing interest in steganography is that a few of countries have adopted restrictions on the use of strong cryptography and the use of steganography solves this problem.The stages of use of steganography for information security are considered and a series of applied software tools for creating a steganographic message (*S-Tools*, *Steganos*, *JSteg*, *Hide-in-Picture*), and conducting steganalization (*StegDetect*, *FTK Imager*, *Stegosuite*, *File Signature Header*, *Maresware Forensic Suite*) are described.

Today, the biometric methods of protecting information that are most likely to identify a person are rapidly developing. These information security methods are among the most promising and are already widely used today by such famous manufacturers of electronic and computer equipment as *Sharp*, *CardMedia*, *Fujitsu*, *Apple*, *Biolink Technologies*. The article describes modern technologies and devices that are already used to identify fingerprints of a person, which ensures reliable protection against unauthorized interference.

Key words: information security, password, steganography, steganalization, biometrics, fingerprinting.