УДК 35.078

В. О. Собина, *к.т.н., доцент, нач. каф. (ORCID 0000-0001-6908-8037)*
Д. В. Тарадуда, *к.т.н., заст. нач. каф. (ORCID 0000-0001-9167-0058)*
М. О. Демент, *к.пед.н., доц. каф. (ORCID 0000-0003-4975-384X)*
Національний університет цивільного захисту України, Харків, Україна

ЗАХИСТ ІНФОРМАЦІЇ ВІДОМЧОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ПАРОЛЬНОЇ СИСТЕМИ

Теоретично обґрунтовано підхід до кількісної оцінки стійкості парольних систем з урахування потужності простору паролів і довжини пароля. Формалізована ідея інформаційної ентропії як підхід до вимірювання кількості інформації, яка невідома через випадкові величини, визначається випадковість змінної на основі знань, що містяться в іншій частині повідомлення. Встановлено, що, чим більше ентропії в даному розподілі паролів, тим складніше вгадати пароль, який було обрано з цього розподілу; паролі з більшими значеннями ентропії вимагають більшої очікуваної кількості припущень, що робить ентропію корисною як міру стійкості пароля. Надано пропозиції щодо управління паролями відомчої інформаційно-телекомунікаційної мережі об'єкта критичної інформаційної інфраструктури. Дослідження показують, що велика частина ентропії, внесена великими та не буквеними символами, створюється користувачами, які перевищують мінімальні вимоги політики стійкості пароля. Безпечне створення паролів ускладнюється компромісом між розробкою паролів, які одночасно важко зламати і використовувати. Відповідно важливою є політика управління доступом. Дослідження показують, що велика частина ентропії, внесена великими та не буквеними символами, створюється користувачами, які перевищують мінімальні вимоги політики стійкості пароля: використання кількості цифр більше, ніж потрібно, різні позиції спеціальних символів. Зроблено висновок, що текстові паролі залишаються домінуючим методом автентифікації в комп'ютерних системах, незважаючи на значні вдосконалення, включаючи смарт-карти, картки RFID, USB-токени та графічні паролі, що мають свої переваги і є придатними для використання в певному середовищі або для певної програми. Зазначено, що опублікованих емпіричних досліджень, які б вивчали стратегії, що використовуються користувачами за різними політиками щодо паролів, мало. Подальші дослідження планується провести в цьому напрямку.

Ключові слова: аутентифікація, пароль, стійкість парольної системи, ентропія Шеннона, політика стійкості пароля

1. Вступ

Згідно із Законом України від 12.11.2003 № 1280 «Про телекомунікації» (ст.65) і Постановою КМУ від 29.06.2004 № 812 «Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» (редакція від 06.02.2019) ДСНС, як спеціальний споживач телекомунікаційних мереж, з метою впорядкування роботи відомчої інформаційно-телекомунікаційної мережі ДСНС здійснює загальний контроль за готовністю та функціонуванням телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Комунікаційні системи, що використовуються у ДСНС, відносяться до критичної інформаційної інфраструктури і є об'єктами кіберзахисту.

Для забезпечення інформаційної безпеки відповідно до стандарту ISO / IEC 27001-2013 [1] парольний захист повинен виконувати процедуру безпечного входу в операційну систему, система управління паролями має гарантувати якісні паролі, всі користувачі зобов'язані мати унікальний ідентифікатор для їх індивідуального розпізнання.

Адміністратори інформаційних систем часто використовуються паролі низької стійкості, які можуть міститися в словниках вільного доступу (15%), і повністю співпадати з логіном (10%) або зовсім відсутні (2%).

Тому актуальною проблемою є низька ефективність підсистеми управління доступом до інформації відомчої інформаційно-телекомунікаційної мережі об'єктів критичної інформаційної інфраструктури.

2. Аналіз літературних даних та постановка проблеми

У роботі [2] описані сучасні методи зламування паролів. Розглядаються проблеми, повзанні з людським фактором, пропонуються методи підвищення захищеності пароля, враховуючи довжину пароля, складність пароля і можливість його запам'ятовування, але не враховувалася стійкість парольної системи протистояти атаці зловмисника, який заволодів базою даних облікових записів для відновлення паролів.

Важливою метою систем аутентифікації є допомога користувачам у виборі кращих паролів. У [3] вивчається складність використання пароля, статистичні проблеми оцінки цього показника за допомогою наборів емісійних даних, які можна змоделювати як випадкову вибірку з основного розподілу ймовірностей. Емпіричні оцінки, представлені дисертаційному дослідженні, показують, що рівень безпеки, що забезпечується сучасними системами, низький. Погоджуємося із висновками, що варто повернутися до вибору машиною паролів для програм, що мають найважливіше значення для безпеки. Тому вдосконалення стійкості парольного захисту є оптимальним для забезпечення автентифікації. Як правило, користувачі схильні віддавати перевагу паролям, що запам'ятовуються, але при цьому легко вгадуються зловмисниками, водночас надійні паролі, призначені системою, важко запам'ятати користувачам.

У [4] увага приділяється комплексній оцінці системи графічних паролів Persuasive Cued Click Points, яка включає оцінку зручності використання і безпеки на трьох різних рівнях, що забезпечується за рахунок посилення ролі ефективного простору паролів, тобто в створенні переконливої графічної системи паролів на основі кліків мишкою. Схема точок кліків мишкою з підказками ефективна для зменшення кількості гарячих точок на області зображення, де користувачі з більшою ймовірністю вибирають правильні точки кліків. Однак, як недолік можна відмітити те, що у графічних паролях, заснованих на кліках, погано обрані паролі призводять до появи гарячих точок (ділянки зображення, на яких користувачі з більшою ймовірністю вибирають точки кліку, що дозволяє зловмисникам проводити більш успішні словникові атаки).

У [5] представлена інтегрована оцінка графічної схеми паролів Persuasive Cued Click-Points, ключова особливість яких полягає в тому, що створення важчого для вгадування пароля забезпечується зведенням до мінімуму формування гарячих точок у користувачів, збільшуючи ефективний простір паролів, використовуючи пам'ять людини для візуалізації. Однак, аналіз досліджень, попри сподівання на людську пам'ять для візуалізації, показує, що дизайн користувальницького інтерфейсу впливає на користувачів і може сприяти як безпечному, так і небезпечному вибору пароля, тому проблема забезпечення стійкості парольного захисту не є вирішеною.

У дослідженні [6] запропоновано декілька можливих показників для вимірювання стійкості індивідуального пароля. На відміну від спеціальних підходів, які спирались на текстові властивості паролів, розглядається проблема без будь-яких знань про структуру паролів, що дає змогу оцінювати стійкість щодо семантики паролів. Порівняно результати загальних показників із результатами метрик NIST та інших метрик «на основі ентропії» для великого набору даних паролів. Проте недоліком даних досліджень є висока ефективність вгадування зловмисниками паролів на основі мови словника паролів і паролів користувачів, які вибирали їх в наборі даних.

У [7] на основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів інформаційно-телекомунікаційних систем

показано, що парольний захист на сьогодні є одним із найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах розподілених систем. Проте без використовування інших механізмів захисту парольний захист не є надійним, оскільки не може забезпечити потрібного захисту, тому вважаємо за необхідне розраховувати стійкість парольної системи за формулою оцінки ентропії, що не висвітлено в даній роботі.

У [8] розглянуті особливості алгоритмів оцінки стійкості паролів до зламів на основі аналізу сучасних методів хакерських атак на системи авторизації, запропоновано алгоритм стійкості паролів для його перевірки на етапі створення, але не проаналізовані статистичні показники для надійності індивідуального пароля.

Таким чином, не вирішеною частиною проблеми захисту інформації відомчої інформаційно-телекомунікаційної мережі є кількісна оцінка стійкості парольних систем.

3. Мета та завдання дослідження

Метою роботи є аналіз і пропозиції щодо посилення системи аутентифікації до інформаційно-телекомунікаційної мережі об'єкта критичної інформаційної інфраструктури, де обробляються державні інформаційні ресурси або інформація з обмеженим доступом.

Досягнення поставленої мети потребує вирішення наступних завдань:

1. Теоретично обґрунтувати підхід до кількісної оцінки стійкості парольних систем з урахування потужності простору паролів і довжини пароля.

2. Надати пропозиції щодо управління паролями відомчої інформаційно-телекомунікаційної мережі об'єкта критичної інформаційної інфраструктури.

4. Теоретичне обґрунтування підходу до кількісної оцінки стійкості парольних систем

Аудит інформаційної безпеки починається з аналізу ризиків і загроз з точки зору системи захисту. Елементи тестування на проникнення при цьому можуть (у відповідності з [1], а саме 11.2.3 – управління паролями користувача, 11.3.1 – використання пароля, 11.5.3 – система управлення паролями) використовуватися для оцінки ефективності реалізації таких захисних механізмів, як «захист від зловмисного коду», «забезпечення мережевої безпеки» та ін.

Загроза неавторизованого проникнення до системи охоплює всі типи несанкціонованого доступу, у тому числі такі: фальсифікація санкції на доступ, неправомірне використання паролів; спроби працювати від імені іншої особи; несанкціоноване використання носіїв даних; перехоплення повідомлень у каналах зв'язку; вірусні атаки тощо.

Парольна система є невід'ємною складовою підсистеми управління доступом системи захисту інформації (СЗІ) і стає одним із перших об'єктів атаки при вторгненні в захищену систему. Підсистема управління доступом СЗІ включає пароль – ідентифікатор об'єкта доступу. Ідентифікатор також називають ім'ям користувача або іменем облікового запису користувача. Обліковий запис – це сукупність ідентифікатора і пароля.

При створенні пароля використовують загальновідому інформацію (адресу, номер телефону, дату дня народження); мнемонічну інформацію, коли пароль будується з перших літер фрази; на основі іноземного слова; цифр або символів, доданих до початку чи кінця, цифр або символів, що замінюють букви, та відсутніх букв. Часто користувачі поєднують кілька стратегій при створенні пароля.

Дозволенними є наступні варіанти зберігання паролів в системі: у відкритому вигляді; як хеш-значення; зашифрованим деяким ключем. Найбільш надійними є другий і третій спосіб, які мають певні особливості.

Можливість добору пароля залежить в основному від двох параметрів: довжини пароля і обсягу алфавіту, і якщо пароль вибирається випадково і рівноймовірно, то для її оцінки використовуються формули:

– ймовірність підібрати пароль з першої спроби:

$$P_{П1} = \frac{1}{A^s}, \tag{1}$$

де – A обсяг – алфавіту, S– довжина пароля;

– ймовірність підібрати пароль з і-спроби:

$$P_{П1} = \frac{1}{A^s + 1 - i}, \tag{2}$$

– ймовірність підібрати пароль з ak-спроб:

$$P_{П1} = \frac{k}{A^s}, \tag{3}$$

– ймовірність підібрати пароль в період його безпечного часу дії:

$$P_{Тв} = \frac{3600 \cdot T_в}{A^s \cdot t_П}, \tag{4}$$

де $T_в$ безпечний час дії, $t_П$ – час набору пароля.

Сьогоднішні соціальні мережі об’єднують велику кількість користувачів, і тому оцінка стійкості парольних систем аутентифікації до атак підбору пароля, компрометації пароля і крадіжки файлу паролів є необхідною.

Існують різні показники стійкості парольних систем – парольні метрики:

– чисельні метрики;
– імовірнісні метрики;
– інформаційна ентропія по Шеннону;
– евристичні модифікації ентропії;
– імовірнісні модифікації ентропії.

Чисельні метрики – це значення часу повного перебору пароля.

Імовірнісні метрики отримують з наявної парольної статистики для конкретних систем.

Виходячи із формули імовірності підбору пароля:

$$P = \frac{V \cdot T}{|A|^n}, \tag{5}$$

де V – швидкість підбору пароля, T – термін дії пароля, $|A|^n$ потужність простору паролів, n– довжина пароля. Можна дійти висновку, що на стійкість пароля впливають частота зміни пароля, потужність простору паролів, котра характеризується довжиною і алфавітом, що застосовується при складанні пароля.

Ентропію можна описати як міру того, наскільки важко передбачити значення змінної. Більш конкретно, ентропію можна вважати мірою складності відгадування пароля. Загалом, чим більше ентропії в даному розподілі паролів, тим складніше вгадати пароль, який було обрано з цього розподілу. Паролі з більшими значеннями ентропії вимагають більшої очікуваної кількості припущень, що робить ентропію корисною як міру стійкості пароля.

4. Розробка пропозицій щодо управління паролями відомчої інформаційно-телекомунікаційної мережі

У теорії інформації ентропія – це середня швидкість генерування значень деяким випадковим джерелом даних.

Для оцінки ентропії застосовується формула Клода Шеннона [9].

Оскільки формула Шеннона для ентропії є адитивною, можна розрахувати ентропію для розподілу паролів у цілому, підсумовуючи ентропію, отриману з окремих аспектів цих паролів; оцінити ентропію, отриману з довжини пароля, розміщення символів, кількості кожного типу символів у паролі та вмісту кожного символу; а потім об'єднати їх, щоб сформувати оцінку загальної ентропії пароля.

Величина інформаційної ентропії, що пов'язана з певним значенням даних, обчислюється за формулою:

$$H = -\sum_{i=1}^{n} P_i \mathrm{Log} P_i, \tag{6}$$

де P_i – імовірність і-го значення системи значення прийнятої змінної n-станів системи (значень прийнятих системою).

Коли джерело даних генерує значення, яке має низьку імовірність (тобто коли відбувається малоймовірна, несподівана подія), з ним пов'язана більша інформація, ніж з більш імовірною подією.

Кількість інформації, що виражається подією, пов'язаною з появою певного значення даних, розглядають як випадкову змінну, математичне очікування якої дорівнює інформаційній ентропії.

Таким чином, інформаційну ентропію можна розглядати як міру невпорядкованості або невизначеності стану деякої системи, що описує дані.

Ентропія по Шеннону обчислюється наступним чином:

$$H = \mathrm{Log}_2 |A|^n = n \cdot \mathrm{Log}_2 |A| = n \frac{\mathrm{Ln}|A|}{\mathrm{Ln}2}, \tag{7}$$

де $|A|$ – потужність алфавіту; n – довжина пароля.

Розрахунок ентропії за формулою Шеннона проводився на базі AMD Athlon(tm) 64 X2 Dual Core Processor 4000+ з використанням математичного апарату системи прикладного математичного моделювання «MathCad» 14-ї версії.

Табл. 1. Результати визначення інформаційної ентропії за формулою Шеннона

Алфавіт/довжина, знаків	5	6	7	8
Латиниця	23,5	28,2	32,9	37,6
Цифри	16,6	19,9	23,2	26,5
Латиниця + верхній регістр + цифри	29,7	35,7	41,6	47,6
Латиниця + кирилиця + верхній регістр + цифри	35	41,9	48,9	55.9

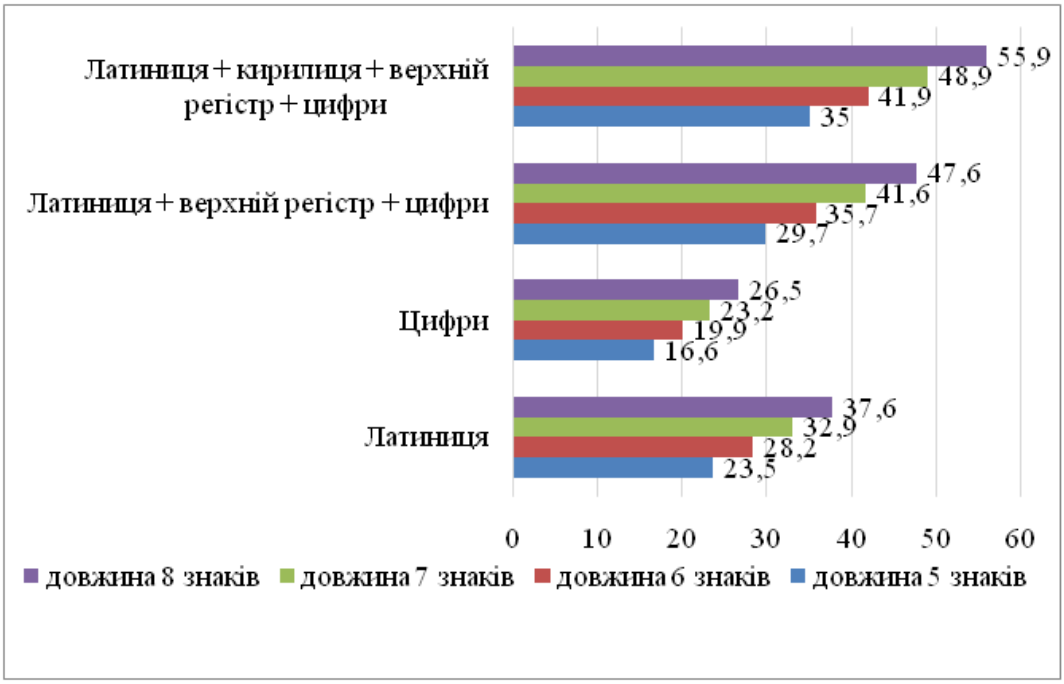

Рис. 1. Візуалізація результатів визначення інформаційної ентропії за формулою Шеннона

По парольним базам, викладених хакерами у відкритий доступ у мережі Інтернет, отримана статистика скомпрометованої бази паролів Google та ін., що показані у табл. 2, 3.

На початку 2021 року, проаналізувавши майже 275,7 мільйона паролів, NordPass опублікував список найбільш часто використовуваних паролів для онлайн-акаунтів [10]. Результати наведені в табл. 4.

Табл. 2. Довжина паролів

Довжина пароля	Кількість паролів Яндекс	Кількість паролів Mail.ru	Кількість паролів Google
6	380732	17484	924154
7	174782	4155	663510
8	282641	12562	1422999
9	130676	3212	683315
10	103926	2421	682811
11	71948	1399	152256
12	45387	1106	93202
13	20127	627	42387
14	14950	438	24853
15	9895	293	14851
16	7646	205	7291
17	3487	12	2549
18	3104	20	1781
19	1747	2	1082
20	2660	15	1166

Табл. 3. Алфавіт паролів

Алфавіт, що використовується	Кількість паролів Яндекс	Кількість паролів Mail.ru	Кількість паролів Google
Паролі, що складаються лише з цифр	608125	18806	774669
Паролі, що складаються із символів	233561	14650	1968873
Паролі, що складаються із нижнього регістра	218319	13835	1968873

Продовження табл. 3

Паролі, що складаються із верхнього регістра	3136	53	-
Сході на номер мобільного телефона	40980	138	22751
Паролі, що співпадають із логіном	1489	3619	45010
Паролі, що співпадають із датами	171906	9287	156142
Паролі, що підходять під змістовний опис стійкого пароля	345	5	-
Підходять за стійкістю по Шеннону	143802	3916	290530

Табл. 4. Розподіл випадкових витоків по каналах передачі інформації

Витоки по каналах передачі інформації (%)	2015	2016	2017	2018	2019	2020
крадіжка / втрата обладнання	13,4	26,1	14,8	5,3	6,9	7,2
мобільні пристрої	-	-	0,3	0,4	0,8	1,4
знімні носії	12	5,9	6,9	6,7	3,1	5,3
мережа (браузер, Cloud)	20,2	22,3	34,7	46,9	45,3	54,6
електронна пошта	23,3	14,8	15,4	23,9	28,3	32,8
паперові документи	30,8	30,8	27,4	23,9	28,3	27,1
ІМ (текст, голос, відео)	0,3	0,5	0,3	0,8	2,1	3,8

Порівняльний аналіз статистики за два попередні роки, що наведені в літературі, показав тенденцію підсилення стійкості паролів за рахунок довжини і застосуванню складнішого алфавіту.

Виходячи з підходів до проведення атаки можна сформулювати критерії стійкості пароля до неї та надати пропозиції щодо управління паролями відомчої інформаційно-телекомунікаційної мережі об’єкта критичної інформаційної інфраструктури:

– найбільш поширена мінімальна довжина – вісім символів. З тієї ж причини він не повинен складатися з одних цифр;

– пароль не повинен бути словниковим словом або простим їх поєднанням, це спрощує його підбір за словником;

– пароль не повинен складатися з загальнодоступної інформації про користувача;

– для складання пароля необхідне використання поєднання слів з цифрами і спеціальними символами (#, $, * і т.д.), використання малопоширених або неіснуючих слів;

– установлення максимального терміна дії пароля;

– установлення вимоги неповторності паролів;

– обмеження числа спроб введення пароля (блокує користувача після перевищення певного числа спроб введення, що здійсненні поспіль).

В останні роки запропоновано ряд пристроїв та методів, включаючи смарт-карти, картки RFID, USB-токени та графічні паролі, щоб зробити аутентифікацію більш зручною та безпечною. Хоча кожна з цих технологій має свої переваги і є придатною для використання в певному середовищі або для певної програми, текстові паролі залишаються найбільш часто використовуваним механізмом автентифікації.

Для впорядкування роботи відомчої інформаційно-телекомунікаційної мережі ДСНС дотримуватися організації заходів протидії кіберзагрозами у відповідності до рекомендацій Національного стандарту України ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки».

5. Обговорення результатів кількісної оцінки стійкості парольних систем

Оцінка стійкості пароля може використовуватися для активної перевірки паролів, що вказує користувачеві на надійність певного пароля під час реєстрації.

Статистичні дані, зібрані з пошукових систем Google та ін. (табл. 2, 3), показують що: середня довжина пароля становить 10,5 символів, а режим – 8. Із 32 символів, найпопулярнішими варіантами є символи, що відповідають натисканням клавіші Shift та цифрам 1, 2 або 3 на стандартній клавіатурі; користувачі обиратимуть паролі, які повністю складаються з малих літер, якщо не змушені робити інакше; виконуючи правила політик паролів, які зобов'язують включати великі літери і не алфавітні символи, користувачі задовольняються найпростішими та найбільш передбачуваними, ставлячи велику літеру на початку та пунктуацію або спеціальні символи в кінці пароля. Результати аналізу статистики зламів зловмисниками паролів показує, що перші п'ять рядків зайняли такі поєднання, як «123456789», «picture1», «password» і «12345678». Найпоширенішим паролем виявився «1234562», який тільки за 2020 рік було зламано більше 23 мільйонів разів. Більш короткий пароль «12345» посідав перше місце в 2019 році. Але більш 188000 користувачів вибрали його в 2020 році, що дозволило зайняти йому восьме місце. Такі паролі можна зламати менш ніж за секунду, виняток становить «picture1» – три години.

Настройка пароля визначається довжиною паролю та режиму символів.

Існує консенсус щодо того, що правильно написана політика щодо стійкості паролів може забезпечити підвищений рівень безпеки. Аналіз обговорень стійкості паролів (таблиця 4) показує, майже 45% користувачів створюють свій пароль одним словом, незважаючи на те, що політика щодо паролів включає перевірку словників. Значною мірою слабкість текстових паролів пояснюється їх стислістю. Питання текстових паролів, що витягуються з відносно невеликого простору, ускладнюється схильністю користувачів вибирати особливо слабкі паролі, що містять або базуються на словникових словах. Це означає, що простір паролів, що фактично використовується, набагато менший, ніж простір теоретично доступних паролів, що суттєво збільшує ймовірність того, що зловмисник зможе виявити даний пароль за допомогою атаки грубої сили або навіть здогадок. Питання текстових паролів, що витягуються з відносно невеликого простору, ускладнюється схильністю користувачів вибирати особливо слабкі паролі, такі як ті, що містять або базуються на словникових словах. Це означає, що простір фактично використовуваних паролів набагато менший, ніж простір теоретично доступних паролів, що суттєво збільшує ймовірність того, що зловмисник зможе виявити даний пароль за допомогою атаки грубої сили або навіть здогадок.

Для убезпечення властивих і спричинених користувачем слабкостями текстових паролів, адміністратори зазвичай встановлюють ряд правил – політику щодо паролів – яких користувачі повинні дотримуватися при виборі пароля. Політика щодо паролів може вказувати, наприклад, що пароль повинен мати мінімальну кількість символів, що він повинен містити великі літери або цифри і що він не може містити слів словника. Призначення такої політики щодо паролів полягає в тому, щоб забезпечити великий простір можливих паролів і не дати користувачам вибрати паролі, які зловмиснику може бути легко виявити, відгадуючи чи через атака грубої сили.

Поточна практика покладається на основні правила, засновані на оцінках ентропії англійської мови. Визначення ефективності використання ентропії, як вимірювання безпеки, забезпечується різними політиками створення паролів. Результати

означають, що для стандартного пароля політикою створення є мінімальна довжина та вимоги до набору символів. Безпечне створення паролів ускладнюється компромісом між розробкою паролів, які одночасно важко зламати і використовувати.

Сьогодні мало опублікованих емпіричних досліджень які б вивчали стратегії, що використовуються користувачами за різними політиками щодо стійкості паролів.

6. Висновки

1. Теоретично обґрунтовано підхід до кількісної оцінки стійкості парольних систем з урахування потужності простору паролів і довжини пароля. Ідея інформаційної ентропії формалізована як підхід до вимірювання кількості інформації, яка невідома через випадкові величини, певним чином визначається випадковість змінної на основі знань, що містяться в іншій частині повідомлення. Значення ентропії Шеннона є корисним для визначення середнього мінімального обсягу місця, необхідного для зберігання або передачі генерованого користувачем пароля. Таким чином, чим більше ентропії в даному розподілі паролів, тим складніше вгадати пароль, який було обрано з цього розподілу. Ентропія розподілу паролів важлива, оскільки вона нижча за межі очікуваної кількості припущень, необхідних зловмиснику. Паролі з більшими значеннями ентропії вимагають більшої очікуваної кількості припущень, що робить ентропію корисною як міру стійкості пароля. Ентропія, отримана з довжини пароля показує ймовірність того, що пароль має певну довжину, визначається діленням кількості паролів, які мають цю довжину, на загальну кількість паролів у розподілі. Формула Шеннона застосовується до ймовірностей для всіх довжин, які обчислюються. Цей розрахунок дає ентропію 2,68 біта довжини пароля, вказуючи, що довжина пароля вносить цю суму в загальну ентропію паролів відповідно до політики щодо паролів. Ентропію, в яку вносять багато аспектів паролів, таких як розміщення символів та номер кожного символу, можна обчислити аналогічно, використовуючи статистичні дані, зібрані з пошукових систем Google та ін. Одним із них є «які цифри», які, за оцінками досліджень, дорівнюють ентропії однієї випадкової цифри, використовуючи середнє значення з 2,45 цифр на пароль.

2. Ентропія пароля, що визначається як випадковість у наборі символів та послідовності символів, є показником надійності пароля. Допустиме значення ймовірності P підбору пароля протягом його терміну дії визначає необхідну потужність простору паролів S. Збільшення потужності алфавіту пароля зменшує його довжину. Очевидно, що зі збільшенням довжини пароля ймовірність його підбору зменшується; зменшення швидкості підбору паролів V зменшує можливість підбору пароля; при подовженні терміну життя пароля і швидкості перебору пароля, можливість його підбору збільшується. Відповідно, для політики щодо паролів, обов’язковим має бути: пароль не повинен містити комбінації із сусідніх символів і символів одного регістру; перевірка словника, видаленням всіх не алфавітних символів з пароля та перевіркою залишку рядка за словником; вимога задовольняється, якщо пароль містить слово-словник з наявними додатковими літерами до, після або в межах слова.

Література

1. International standard ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. 2013. 34 p. URL: https://www.iso.org/ru/standard/54534.html (дата звернення: 12.09.2021).

2. Weir M., Aggarwal S., Collins M., Stern H. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords // CCS '10:

Proceedings of the 17th ACM conference on Computer and communications security. United States 4–8 October 2010. P. 162–175. doi: 10.1145/1866307.1866327

3. Bonneau J. Guessing human-chosen secrets // University of Cambridge, Computer Laboratory. 2012. № 819. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-819.pdf (дата звернення: 02.10.2021).

4. Nayak A., Bansode R. Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points // 7th International Conference on Communication, Computing and Virtualization (ICCCV). 2016. V. 79. P. 553–560. doi: 10.1016/j.procs.2016.03.070

5. Chiasson S., Stobert E., Forget A., Biddle R., Van Oorschot P. C. Persuasive Cued Click-Points Design, implementation, and evaluation of a knowledge-based authentication mechanism // IEEE Transactions on Dependable and Secure Computing. 2012. V. 9. I. 2. P. 222–235. doi: 0.1109/TDSC.2011.55

6. Bonneau J. Statistical metrics for individual password strength // 20th international conference on Security Protocols. Berlin April 2012. doi: 10.1007/978-3-642-35694-0_10

7. Khorev P. B. User Authentication Based on Knowledge of Their Work on the Internet // Wireless Mesh Networks – Security, Architectures and Protocols. 2019. doi: 10.5772/intechopen.88620

8. Kelley P. G., Komanduri S., Mazurek M. L., Shay R., Bauer T. V. L., Christin N., Cranor L. F., Lopez J. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms // IEEE Symposium on Security and Privacy. Pittsburgh, USA 20–23 May 2012. P. 523–537. doi: 10.1109/SP.2012.38

9. Rioul O. Shannon's formula and Hartley's rule: A mathematical coincidence? // AIP Conference Proceedings. V. 1641. I. 1. Paris, France 17 February 2015. doi: 10.1063/1.4905969

10. Богуславская К. Nord Pass назвал 200 самых популярних паролей 2020 года // Электронное издание «Vector». 2020. URL: https://vctr.media/samyye-rasprostranennyye-paroli-2020-goda-52027 (дата звернення: 12.09.2021).

V. Sobyna, *PhD, Associate Professor, Head of Department*
D. Taraduda, *PhD, Deputy Head of Department*
M. Dement, *PhD, Associate Professor of the Department*
National University of Civil Defence of Ukraine, Kharkiv, Ukraine

PROTECTION OF INFORMATION OF DEPARTMENTARY INFORMATION AND TELECOMMUNICATIONS NETWORK USING THE PASSWORD SYSTEM

The approach to quantitative estimation of stability of password systems taking into account power of space of passwords and length of the password is theoretically substantiated. The formalized idea of information entropy as an approach to measuring the amount of information that is unknown through random variables is determined by the randomness of a variable based on the knowledge contained in another part of the message. It is established that the greater the entropy in a given distribution of passwords, the more difficult it is to guess the password that was chosen from this distribution; passwords with higher entropy values require more expected assumptions, which makes entropy useful as a measure of password strength. Proposals for password management of the departmental information and telecommunication network of the object of critical information infrastructure are given. Studies show that much of the entropy introduced by uppercase and lowercase characters is created by users who exceed the minimum requirements of the password strength policy. Secure password creation is complicated by the trade-off between developing passwords that are both difficult to crack and use. Accordingly, the access control policy is important. Studies show that much of the entropy introduced by large and non-alphanumeric characters is created by users who exceed the minimum requirements of the password strength policy: the use of more digits than necessary, different positions of special characters. It is concluded that text passwords remain the dominant method of authentication in computer systems, despite

significant improvements, including smart cards, RFID cards, USB tokens and graphic passwords, which have their advantages and are suitable for use in a particular environment or for a specific program. It is noted that there are few published empirical studies that would examine the strategies used by users under different password policies. Further research is planned in this direction.

Keywords: authentication, password, password strength, Shannon entropy, password strength policy

References

1. International Organization for Standardization. (2013). International standard ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Retrieved from https://www.iso.org/ru/standard/54534.html

2. Weir, M., Aggarwal, S., Collins, M., Stern, H. (2010). Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. CCS '10: Proceedings of the 17th ACM conference on Computer and communications security, 62–175. doi: 10.1145/1866307.1866327

3. Bonneau, J. (2012). Guessing human-chosen secrets (Report No. 819). University of Cambridge, Computer Laboratory. Retrieved from https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-819.pdf

4. Nayak, A., Bansode, R. (2016). Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points. 7th International Conference on Communication, Computing and Virtualization 2016, 553–560. doi: 10.1016/j.procs.2016.03.070

5. Chiasson, S., Stobert, E., Forget, A., Biddle, R., Van Oorschot P. C. (2012). Persuasive Cued Click-Points Design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Transactions on Dependable and Secure Computing, 9, 2, 222–235. doi: 10.1109/TDSC.2011.55

6. Bonneau, J. (2012). Statistical metrics for individual password strength. The 20th international conference on Security Protocols. https://doi.org/10.1007/978-3-642-35694-0_10

7. Khorev, P. B. (2019). User Authentication Based on Knowledge of Their Work on the Internet. Security, Architectures and Protocols. doi: 10.5772/intechopen.88620

8. Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Bauer, T. V. L., Christin, N., … Lopez, J. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. IEEE Symposium on Security and Privacy, 523–537. doi: 10.1109/SP.2012.38

9. Rioul, O. (2015). Shannon's formula and Hartley's rule: A mathematical coincidence? AIP Conference Proceedings. V. 1641. I. 1. doi: 10.1063/1.4905969

10. Boguslavskaya, K. (2021). Nord Pass nazval 200 samykh populyarnikh paroley 2020 goda. Retrieved from https://vctr.media/samyye-rasprostranennyye-paroli-2020-goda-52027

Надійшла до редколегії: 13.10.2021
Прийнята до друку: 23.11.2021