DOI: 10.18372/2410-7840.21.13547
УДК 004.021

ГЕНЕРУВАННЯ ПАРОЛЮ ДЛЯ БЕЗДРОТОВИХ МЕРЕЖ З ВИКОРИСТАННЯМ ЗМІННОГО ПРАВИЛА УСКЛАДНЕННЯ

Володимир Бурячок, Андрій Аносов, Артем Платоненко

Найбільшу небезпеку для інформації останнім часом несуть відкриті Wi-Fi мережі, адже кожен має змогу підключитись до них та виконувати певні зловмисні дії. Небезпечними можна вважати також і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись дізнавшись, наприклад, пароль у працівника. Однією з причин кібернетичних атак на ресурси таких мереж є нестійкі до підбору паролі. Їх застосування дозволяє зловмисникам підключатися до зазначених мереж та отримувати доступ до всіх підключених до мереж пристроїв. Крім того, якщо нестійкий або стандартний пароль використовується для панелі налаштувань, то всі пристрої піддаються ризику кібернетичної атаки, яка може здійснюватися віддалено. Використання зловмисниками комплексного підходу для спроб несанкціонованого доступу до систем бездротового зв'язку (шляхом об'єднання соціальної інженерії та перехоплення даних з використанням зловмисного програмного забезпечення), а також нових видів кібератак, що дозволяють приховано встановлювати шкідливе програмне забезпечення на мобільні пристрої може сприяти зниженню ефективності існуючих методів та засобів захисту бездротових мереж. З метою уникнення таких і подібних ним проблем у статті запропоновано спосіб підвищення захисту бездротових мереж від перехоплення інформації та впливу на неї, шляхом створення паролю, стійкого до підбору зі змінним правилом ускладнення. Даний спосіб може бути використано при створенні програмно-апаратних засобів захисту, а також для підвищення захисту облікових записів користувачів та інших систем захисту, де необхідне використання надійного паролю. Враховуючи статистику та проведені в роботі розрахунки, можна стверджувати, що впровадження способу генерування ускладнених паролів дозволить суттєво підвищити рівень захищеності бездротових мереж.

Ключові слова: *інформаційна безпека; загрози інформаційної безпеки; бездротові мережі; захист мереж від несанкціонованого доступу; захист мобільних пристроїв; стійкість паролів; зменшення ймовірності підбору пароля.*

1. ВСТУП

Паролі невідповідальних користувачів зазвичай стають причиною хакерських атак [1]. Після того як зловмисник підключиться до мережі, він отримує доступ до підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі підключені пристрої також піддаються ризику хакерської атаки, яка вже може здійснюватися віддалено [2].

Більшість атак направлена на підбір паролю, стійкість якого залежить від можливої швидкості підбору, саме тому постає необхідність в ускладненні паролю, для зменшення ймовірності його злому.

Вдосконалення способу генерування випадкових паролів, що дозволить завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів, а також можливості урахування співпадіння з паролями системи словників, підвищити рівень захищеності систем бездротового зв'язку від можливого злому.

Дослідженню проблеми захищеності бездротових мереж присвячені роботи: Л.А. Шувалової [3], О.К. Юдіна [4], А.В. Чунарьової [5], J. Doherty [6] та багатьох інших. За їх висновками встановлено, що основними проблемами захищеності бездротових мереж є: вразливість паролів до підбору, відсутність обізнаності користувачів в налаштуванні та неефективне використання технічних засобів, велика кількість зловмисного програмного забезпечення, що використовує збільшення технічних можливостей мобільного обладнання. Дані вразливості несуть небезпеку, як для користувачів особисто, так і для організацій де вони працюють, що показано в загальній моделі перехоплення та захисту інформації в бездротових мережах [7-9].

Метою статті є висвітлення вдосконаленого авторами способу генерування ускладнених паролів за показниками довжини та набору символів, з метою формування більш стійких паролів, у порівнянні з відомими способами-аналогами.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Процедура (послідовність) вдосконалення відомого способу генерування випадкових паролів полягає в такому порядку реалізації етапів.

2.1. Етап 1. Визначення швидкості підбору паролів та обґрунтування їх стійкості.

Для сучасного комп'ютера домашнього користувача при стандартних режимах його роботи з використанням центральних процесорів (CPU), швидкість підбору може становити 6000-7000 паролів за секунду. Залежно від моделі та режиму роботи, вона може відрізнятись.

Для зручності обчислення кількості можливих варіантів підбору паролю за певний проміжок часу в роботі було зроблено припущення, що за одну

секунду роботи CPU може перебрати біля 10 000 паролів із обраних сукупностей. Збільшити швидкість підбору паролів у сотні й тисячі разів можливо завдяки використанню графічних процесорів у відео-картах (GPU) та GPU-ферм (наприклад 12 відео-карт, об'єднаних для спільної роботи). За таких умов швидкість підбору паролів становитиме від 15 млрд. до 180 млрд. за секунду й більше.

Ймовірні значення кількості підбору паролів для випадків підбору з використанням CPU, GPU та GPU-ферми (з 12 GPU) в межах від одної секунди до одного року наведено в таблиці 1.

Якщо в якості певної сукупності паролів взяти множину можливих мобільних телефонів, у форматі + 380 YY XXX XX XX (YY код регіону або мобільного оператора, де є 16 кодів оператора, або 48 кодів регіонів та операторів України, XXX XX XX номер телефону), то для перебору з використанням CPU, наприклад, мобільних номерів потрібно 4 години 26 хвилин, а для перебору кодів регіонів та операторів України приблизно 13 годин 18 хвилин. З використанням для перебору паролів GPU-ферм тривалість відповідних операцій можна зменшити, як мінімум, у 18 млн. разів.

Таблиця 1

Кількість можливих варіантів підбору паролю за певний проміжок часу

Кількість паролів			
CPU	**GPU**	**GPU-ферма (з 12 GPU)**	**Час**
10^4	$1{,}5\cdot10^{10}$	$1{,}8\cdot10^{11}$	1 секунда
$6\cdot10^5$	$9\cdot10^{11}$	$1{,}08\cdot10^{13}$	1 хвилина
$3{,}6\cdot10^7$	$5{,}4\cdot10^{13}$	$6{,}48\cdot10^{14}$	1 година
$8{,}64\cdot10^8$	$1{,}3\cdot10^{15}$	$1{,}56\cdot10^{16}$	1 доба
$3{,}15\cdot10^{11}$	$4{,}73\cdot10^{17}$	$5{,}68\cdot10^{18}$	1 рік

Як результат, логічним є висновок: чим більша тривалість підбору – тим пароль буде більш стійким до підбору і навпаки. Оскільки множини паролів можуть здаватися стійкими до підбору на CPU, а швидкості GPU та GPU-ферм по підбору паролів є значно більшими, то постає необхідність у пошуку множин паролів для формування парольних політик.

Розраховані результати обрані, як приклад, оскільки можуть збільшуватись, завдяки розвитку сучасної техніки, але їх зміна суттєво не вплине на отримані дані.

2.2. Етап 2. Визначення множин паролів для парольних політик.

Математично парольні множини для парольних політик можна описати, як вибірку з певних символів:

– *сполучення з символів для паролів* (комбінація), коли з n елементів (кількості можливих символів) вибирають k (довжина обраного паролю), порядок не має значення;

– *розміщення з символів для паролів,* коли з n елементів вибирають k в певному порядку;

– *розміщення з повтореннями з символів для паролів*, коли число всіх розміщень з n елементів вибирають k, з повтореннями.

Залежно від обраного типу захисту мережі та варіанту обмеження у виборі з множин символів, можливі різні значення кількості паролів. В таблиці 2 розглянуто можливі множини паролів для парольних політик, залежно від варіанту захисту бездротових мереж Wi-Fi, з використанням WPA/WPA2.

Таблиця 2

Кількість паролів, що використовуються для захисту бездротових мереж Wi-Fi

Варіанти захисту	**Кількість символів в паролі**	**Кількість отриманих паролів для парольних політик**		
		Сполучення	Розміщення	Розміщення з повтореннями
WPA/WPA2	64 шістнадцяткових символи	0	$1.12\cdot10^{21}$	$8.22\cdot10^{85}$
WPA/WPA2 (TKIP 128 біт)	**63 символи ASCII**	**$6.03\cdot10^{21}$**	**$1.19\cdot10^{109}$**	**$3.18\cdot10^{122}$**
+WPS (QSS) Налаштування швидкого підключення, що несе уразливість	8 цифр, одна з яких відповідає за контрольну суму, тому підбирається 7, через помилку підбирається 4 перших, або 4 останніх з 7	$6.05\cdot10^5$	10^4+10^3	10^7

Примітка: *n=88* - ASCII: 26 прописних літер, 26 заголовних літер, 10 цифр, 26 спеціальних символів;
k=63 - кількість символів у паролі для WPA/WPA2.

Як видно з таблиці 2, знання зловмисником технологій формування парольних політик (наприклад, шляхом сполучення множини паролів або розміщення з повтореннями множини паролів) надасть йому перевагу в часі на підбір паролю без повторень приблизно у $5.27 \cdot 10^{100}$ разів.

Разом з тим, слід зазначити, що кількість паролів для певної множини дозволяє оцінити лише саму множину паролів за її величиною, але не дає можливості оцінити власне стійкість паролю, оскільки вона залежить від способу, за яким створюється пароль та від можливої швидкості його підбору. Тому постає задача з вибору множин і підмножин паролів для ускладнення, а також формування відповідних змінних правил, які б дозволили зменшити ймовірність підбору ускладнених паролів.

2.3. Етап 3. Формування змінних правил ускладнення для сполучення множини паролів.

Із сполучення множини паролів U_p відбирається множина U_z (рис. 1), що складається з паролів, які мають в собі малі літери англійського алфавіту.

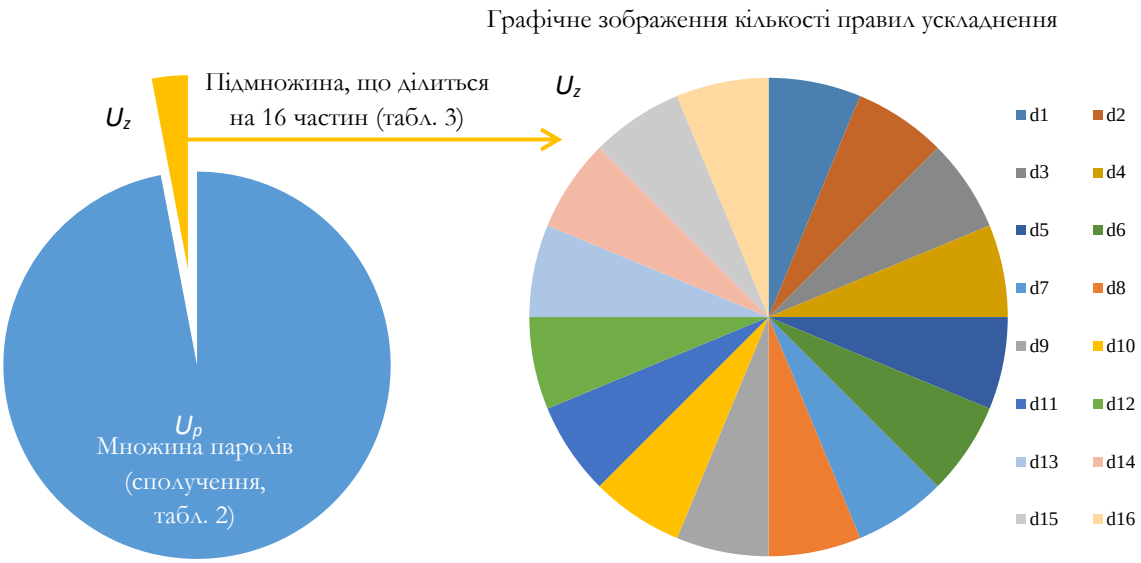

Рис. 1. Кількість слів, або набору символів, що може бути частиною паролю

До U_z потрапляють паролі, які містять 3 або більше простих слів англійською мовою (з 26 прописних літер ASCII, *l*=26) довжиною до 6 символів, або комбінацій набору символів, що можуть бути в словниках.

Із множини U_z за певним правилом *d (d1…d16)*, що визначається кількістю та довжиною слів (набору символів), виділяються 16 підмножин $U_{l(d)}$, (від 3 до 6 літер), що прописуються в кожному рядку таблиці 3.

З підмножини $U_{l(d)}$ відповідно до обраного номеру правила *d* обираються паролі, які додаються до множини (U_p - U_z). Це, в свою чергу, створює множину U_k. Графічно умовні множини символів для паролів можна зобразити так, як показано на рис. 1.

Даний підхід забезпечує трирівневе ускладнення паролю, оскільки:

– *по-перше*, при додаванні паролів обираються лише ті, що складаються з певної кількості літер (відповідно до певного правила *d*);

– *по-друге*, при виборі правила *d* для множини ускладнених паролів воно може бути як змінним (тобто не мати залежності/порядку), так і сталим (наприклад: всі паролі за одним правилом);

– *по-третє*, при використанні змінного порядку правил ускладнення *d* під час генерування паролів (наприклад, кожен пароль по черзі за певним правилом, або будь-яка кількість паролів за кожним із правил у хаотичному порядку і т.д.), унеможливлюється створення такого ж алгоритму генерування паролів зловмисником.

Таблиця 3

Кількість слів, або набору символів, що може бути частиною паролю

$U_{l(d)}$	Кількість слів у паролі	Кількість літер у слові									Кількість комбінацій
d1	4	**6**	**6**	**6**	**6**	**2**					$U_{l\,(d1)}$
d2	5	**6**	**6**	**6**	**5**	**3**					$U_{l\,(d2)}$
d3	5	**6**	**6**	**5**	**5**	**4**					$U_{l\,(d3)}$
d4	5	**6**	**5**	**5**	**5**	**5**					$U_{l\,(d4)}$
d5	5	**5**	**5**	**5**	**5**	**5**	**1**				$U_{l\,(d5)}$
d6	5	**5**	**5**	**5**	**5**	**4**	**2**				$U_{l\,(d6)}$
d7	6	**5**	**5**	**5**	**4**	**4**	**3**				$U_{l\,(d7)}$
d8	6	**5**	**5**	**4**	**4**	**4**	**4**				$U_{l\,(d8)}$
d9	6	**5**	**4**	**4**	**4**	**4**	**4**	**1**			$U_{l\,(d9)}$
d10	6	**4**	**4**	**4**	**4**	**4**	**4**	**2**			$U_{l\,(d10)}$
d11	7	**4**	**4**	**4**	**4**	**4**	**3**	**3**			$U_{l\,(d11)}$
d12	7	**4**	**4**	**4**	**4**	**3**	**3**	**3**	**1**		$U_{l\,(d12)}$
d13	7	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**2**		$U_{l\,(d13)}$
d14	7	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**		$U_{l\,(d14)}$
d15	8	**4**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**1**	$U_{l\,(d15)}$
d16	8	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**2**	$U_{l\,(d16)}$

2.4. Етап 4. Розрахунок кількості паролів для можливих парольних множин.

Формула розрахунку кількості можливих комбінацій паролів матиме вигляд:

$$U_{l(d)} = C_l^m \cdot C_{l-m}^m \cdot C_{l-2m}^m \cdot \ldots \cdot C_{l-(r-1)m}^m \cdot C_{l-rm}^m, \quad (1)$$

де l – кількість літер алфавіту; m – кількість літер в слові (3…6); $r = 1\ldots m$, при умові: $m<rm<l$.

В даному випадку добуток комбінацій означає поєднання значень паролів, кількість літер у яких, сумарно складають довжину алфавіту. Для кожної довжини слова та поєднання слів різної довжини отримаємо певне значення комбінацій, що може бути використане для розрахунку.

Отже, для кожного $U_{l(d)}$ в таблиці 3 буде обчислене певне значення за формулою (1). Загальна кількість паролів для парольної множини U_z буде сумою значень підмножин $U_{l(d)}$, розрахованих за формулою (2):

$$U_z = U_{l(d1)} + \ldots + U_{l(d16)}. \quad (2)$$

Враховуючи, що при формуванні ускладненої парольної множини можливе використання (U_p - U_z) та *d1* або (U_p - U_z) та *d2* або (U_p - U_z) та *d3* і т.д., - кінцеве значення ускладненої множини буде розраховуватись за формулою (3):

$$U_k = (U_p - U_z) \cdot U_z, \quad (3)$$

де U_k – кінцева ускладнена множина; U_p – початкове значення (сполучення множини паролів з таблиці 2); U_z – значення комбінацій слів, з різної кількості літер, з формули (2).

Формула (3) отримана з суми добутків початкової комбінації U_p без множини U_z та значень d, що в результаті дає кінцеве, ускладнене значення.

Для окремого розрахунку ускладненої множини паролів, за одним із можливих правил d, використовується формула (4):

$$U_{k(d)} = (U_p - U_z) \cdot U_{l(d)}, \quad (4)$$

де $U_{k(d)}$ – ускладнена комбінація за обраним правилом d, U_p – початкове значення (сполучення множини паролів з таблиці 2), U_z – значення комбінацій слів, з різної кількості літер з формули (2), $U_{l(d)}$ – значення ком-бінацій слів, з кількості літер за правилом, формула (1).

Для впровадження розробленого способу сформовано алгоритм, який описує всі його етапи та дає змогу створити необхідне програмне забезпечення для автоматизованого генерування стійкого паролю в залежності від вимог системи, для якої буде використовуватись розглянутий спосіб. На рис. 2 приведено блок-схему алгоритму, що відображає процес генерування паролів для ускладненого паролю.

На початку обирається множина паролів U_p за правилом комбінації, з використанням символів без повторень, в якій кількість можливих паролів становить $6{,}03 \cdot 10^{21}$. Відпо-відно до таблиці 3, залежно від значення d, кожне значення $U_{l(d)}$ розраховується окремо, оскільки кількість можливих слів, або комбінацій символів може бути різної довжини. Розраховані значення кількості слів, що можуть бути частиною паролю, для кожного U_l наведено в таблиці 4.

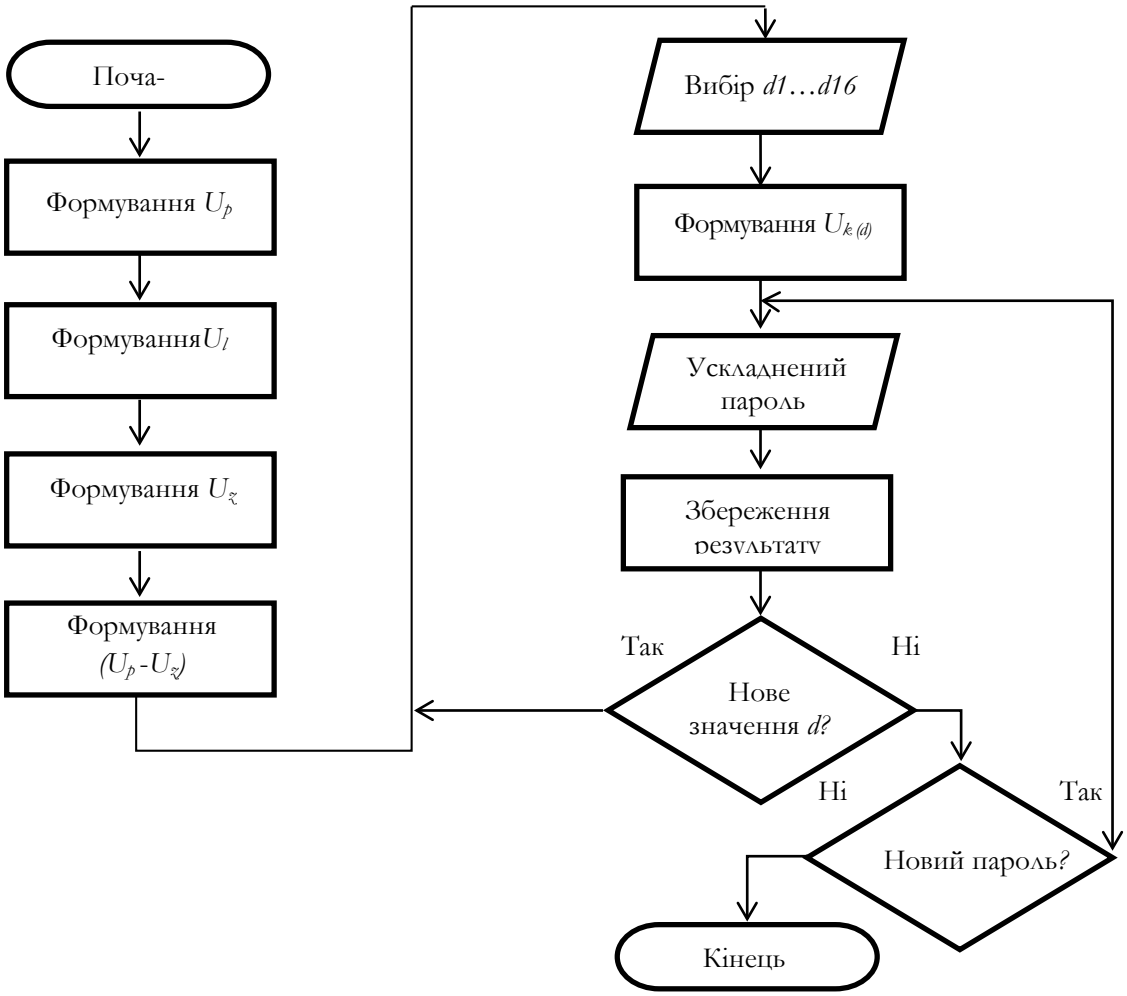

Рис. 2. Алгоритм генерування стійкого паролю зі змінним правилом ускладнення

Таблиця 4

Розрахунок кількості слів, або набору символів, що може бути частиною паролю

$U_{l(d)}$	Розрахунок	Кількість комбінацій
1	$U_{26(d1)} = C_{26}^6 \cdot C_{20}^6 \cdot C_{14}^6 \cdot C_8^6$	$7{,}50 \cdot 10^{14}$
2	$U_{26(d2)} = C_{26}^6 \cdot C_{20}^6 \cdot C_{14}^6 \cdot C_8^5 \cdot C_3^3$	$1{,}50 \cdot 10^{15}$
3	$U_{26(d3)} = C_{26}^6 \cdot C_{20}^6 \cdot C_{14}^5 \cdot C_9^5 \cdot C_4^4$	$2{,}25 \cdot 10^{15}$
4	$U_{26(d4)} = C_{26}^6 \cdot C_{20}^5 \cdot C_{15}^5 \cdot C_{10}^5 \cdot C_5^5$	$2{,}70 \cdot 10^{15}$
5	$U_{26(d5)} = C_{26}^5 \cdot C_{21}^5 \cdot C_{16}^5 \cdot C_{11}^5 \cdot C_6^5$	$1{,}62 \cdot 10^{16}$
6	$U_{26(d6)} = C_{26}^5 \cdot C_{21}^5 \cdot C_{16}^5 \cdot C_{11}^5 \cdot C_6^4$	$4{,}05 \cdot 10^{16}$
7	$U_{26(d7)} = C_{26}^5 \cdot C_{21}^5 \cdot C_{16}^5 \cdot C_{11}^4 \cdot C_7^4 \cdot C_3^3$	$6{,}75 \cdot 10^{16}$
8	$U_{26(d8)} = C_{26}^5 \cdot C_{21}^5 \cdot C_{16}^4 \cdot C_{12}^4 \cdot C_8^4 \cdot C_4^4$	$8{,}44 \cdot 10^{16}$
9	$U_{26(d9)} = C_{26}^5 \cdot C_{21}^4 \cdot C_{17}^4 \cdot C_{13}^4 \cdot C_9^4 \cdot C_5^4$	$4{,}22 \cdot 10^{17}$
10	$U_{26(d10)} = C_{26}^4 \cdot C_{22}^4 \cdot C_{18}^4 \cdot C_{14}^4 \cdot C_{10}^4 \cdot C_6^4$	$1{,}05 \cdot 10^{18}$
11	$U_{26(d11)} = C_{26}^4 \cdot C_{22}^4 \cdot C_{18}^4 \cdot C_{14}^4 \cdot C_{10}^4 \cdot C_6^3 \cdot C_3^3$	$1{,}40 \cdot 10^{18}$
12	$U_{26(d12)} = C_{26}^4 \cdot C_{22}^4 \cdot C_{18}^4 \cdot C_{14}^4 \cdot C_{10}^3 \cdot C_7^3 \cdot C_4^3$	$5{,}62 \cdot 10^{18}$
13	$U_{26(d13)} = C_{26}^4 \cdot C_{22}^4 \cdot C_{18}^4 \cdot C_{14}^3 \cdot C_{11}^3 \cdot C_8^3 \cdot C_5^3$	$1{,}12 \cdot 10^{19}$
14	$U_{26(d14)} = C_{26}^4 \cdot C_{22}^4 \cdot C_{18}^3 \cdot C_{15}^3 \cdot C_{12}^3 \cdot C_9^3 \cdot C_6^3$	$1{,}50 \cdot 10^{19}$
15	$U_{26(d15)} = C_{26}^4 \cdot C_{22}^3 \cdot C_{19}^3 \cdot C_{16}^3 \cdot C_{13}^3 \cdot C_{10}^3 \cdot C_7^3 \cdot C_4^3$	$6{,}00 \cdot 10^{19}$
16	$U_{26(d16)} = C_{26}^3 \cdot C_{23}^3 \cdot C_{20}^3 \cdot C_{17}^3 \cdot C_{14}^3 \cdot C_{11}^3 \cdot C_8^3 \cdot C_5^3$	$1{,}20 \cdot 10^{20}$
	Всього	**$2{,}15 \cdot 10^{20}$**

Підмножина U_z складається з $2{,}15 \cdot 10^{20}$ паролів, що відповідно до формули (2) складається з суми значень $U_{l(d)}$. Відповідно до обраного d, значення $U_{l(d)}$ приєднується до множини (U_p-U_z), що в свою чергу створює ускладнену, за одним з правил, множину $U_{k(d)}$ з кількості паролів що розраховується за формулою (4).

Таким чином, загальна кількість комбі-націй можливих слів з 6, 5, 4, або 3 літер англійської мови складатиме $2{,}15 \cdot 10^{20}$ (U_z), а кількість можливих комбінацій паролів без даної комбінації слів становитиме $5{,}82 \cdot 10^{21}$ (U_p-U_z). Це на 3,57% менше, ніж у випадку комбінацій всіх можливих значень паролів (U_p), але за рахунок введення правила ускладнення d та вибірковому додаванню паролів, маємо значення $1{,}25 \cdot 10^{42}$ (U_k).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Змінний вибір правила ускладнення d, дає можливість створити пароль, ймовірність під-бору якого серед певної множини паролів U_k буде мінімальною. Розширення множини U_z за рахунок використання набору цифр, або слів іншою мовою дозволить, як результат, збільшити кількість варіантів правила ускладнення d та кількість можливих комбінацій підбору, а також рівень невизначеності для зловмисника. Для ускладненого паролю, що створений за описаним способом, отримано значне зниження ймовірності підбору паролю, оскільки на підбір потрібно у $2{,}07 \cdot 10^{20}$ разів більше часу, ніж для випадкової комбінації з 63 символів ASCII, або в $1{,}94 \cdot 10^{31}$ разів більше ніж для випадкового паролю з 8 символів.

Розроблений спосіб підвищення захисту бездротових мереж може бути складовою для програмних та апаратних засобів захисту, а також може забезпечити підвищення рівня захисту облікових записів користувачів та інших систем захисту інформації, де необхідне використання паролів, стійких до підбору.

Тим не менш використання зловмисниками комплексного підходу для спроб несанкціонованого доступу до систем бездротового зв'язку (шляхом об'єднання соціальної інженерії та перехоплення даних з використанням зловмисного програмного забезпечення), а також нових видів кібератак, що дозволяють приховано встановлювати шкідливе програмне забезпечення на мобільні пристрої, може сприяти зниженню ефективності існуючих методів та засобів захисту бездротових мереж. Враховуючи статистику та проведені в роботі розрахунки, можна стверджувати, що впровадження способу генерування ускладнених паролів дозволить суттєво підвищити рівень захищеності бездротових мереж.

Наукова новизна. *Отримав подальшого розвитку* спосіб генерування випадкових паролів для систем бездротового зв'язку, *який* завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення), а також можливості співпадіння з паролями системи словників, *забезпечує* підвищення рівня захищеності мережі від можливого злому.

Перспективним напрямком подальших досліджень є підтримка в актуальному стані бази словників паролів, для впровадження аналізу та подальша повна автоматизація запропонованого способу.

Таблиця 5

Кількісна оцінка стійкості парольних множин

Парольна множина	**Кількість паролів у парольній множині**	**Коефіцієнти стійкості**			
Мобільний номер 10 цифр (16 кодів оператора)	$1{,}6 \cdot 10^{8}$	1	-	-	-
Телефонний номер України 10 цифр (48 кодів регіонів)	$4{,}8 \cdot 10^{8}$	3	1	-	-
Випадкова комбінація 8 символів ASCII	$6{,}43 \cdot 10^{10}$	$4{,}02 \cdot 10^{2}$	$1{,}34 \cdot 10^{2}$	1	-
Випадкова комбінація 63 символи ASCII	$6{,}03 \cdot 10^{21}$	$3{,}77 \cdot 10^{13}$	$1{,}26 \cdot 10^{13}$	$9{,}38 \cdot 10^{10}$	1
Ускладнена комбінація 63 символи ASCII	$\mathbf{1{,}25 \cdot 10^{42}}$	$\mathbf{1{,}28 \cdot 10^{34}}$	$\mathbf{2{,}60 \cdot 10^{33}}$	$\mathbf{1{,}94 \cdot 10^{31}}$	$\mathbf{2{,}07 \cdot 10^{20}}$

Примітка: коефіцієнт стійкості, що дорівнює 1, обирається для парольної множини, з якої починається порівняння.

ЛІТЕРАТУРА

[1]. А. Платоненко, "Сучасні загрози інформаційної безпеки для державних та приватних установ України", *Сучасний захист інформації*, №4, С. 86-90, 2015.

[2]. А. Платоненко, "Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту", *Сучасний захист інформації*, №1, С. 128-132, 2017.

[3]. Л. Шувалова, "Методи захисту даних у Wi-Fi мережах" *Розвиток радіотехнічного забезпечення, АСУ та зв'язку Повітряних Сил*, С. 133-135.

[4]. О. Юдін, О. Весельська, "Аналіз захищеності бездротових мереж з використанням WEP-технології" *Наукоємні технології*, №3 (15), С. 62-66, 2012.

[5]. А. Чунарьова, О. Ярмак, "Аналіз протоколів безпеки сучасних WI-FI мереж" *Nauka i studia*, Т. 33, С. 94-97, 2013.

[6]. J. Doherty, *Wireless and Mobile Device Security*, 2016, 394 p.

[7]. А. Аносов, А. Платоненко, "Модель перехоплення та захист інформації в бездротових мережах" *Сучасний захист інформації*, 2017, №2, С. 90-94.

[8]. V. Lakhno, D. Kasatkin, V. Buriachok, Y. Pa-lekha, V. Saiko, V. Domrachev, "It support in decision-making with regard to infra-red grain drying management", *Journal of Theoretical and Applied Information Technology*, Vol. 96 №22, pp. 7587-7598.

[9]. В. Бурячок, В. Толубко, В. Хорошко, С. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект: підручник,* за заг. ред. д-ра техн. наук В.Л. Бурячок, К.: ДУТ, 2015, 320 с.

ГЕНЕРИРОВАНИЕ ПАРОЛЯ ДЛЯ БЕСПРОВОДНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ПЕРЕМЕННОГО ПРАВИЛА УСЛОЖНЕНИЯ

Наибольшую опасность для информации в последнее время несут открытые Wi-Fi сети. Любой человек может подключиться к ним и выполнить определенные злонамеренные действия. Опасными можно считать также и условно защищенные сети в публичных местах или организациях, к которым можно подключиться узнав, например, пароль у сотрудника. Одной из причин кибернетических атак на ресурсы таких сетей являются неустойчивые к подбору пароли. Их применение позволяет злоумышленникам подключаться к указанным сетям и получать доступ ко всем подключенных к сетям устройствам. Кроме того, если неустойчивый или стандартный пароль используется для панели настроек, то все устройства также подвергаются риску кибератаки, которая может осуществляться удаленно. Использование злоумышленниками комплексного подхода для несанкционированного доступа к системам беспроводной связи (путем объединения социальной инженерии и перехвата данных с использованием вредоносных программ), а также новых видов кибератак, позволяющего скрыто устанавливать вредоносное программное обеспечение на мобильные устройства может способствовать снижению эффективности существующих методов и средств защиты беспроводных сетей. Во избежание таких и подобных им проблем в статье предложен способ повышения защиты беспроводных сетей от перехвата информации и воздействия на нее, путем создания пароля, устойчивого к подбору с переменным правилом сложности. Данный способ может быть использован при создании программно-аппаратных средств защиты, а также для повышения защиты учетных записей пользователей и других систем защиты, где необходимо использование надежного пароля. Учитывая статистику и проведенные в работе расчеты, можно утверждать, что внедрение способа генерирования усложненных паролей позволит существенно повысить уровень защищенности беспроводных сетей.

Ключевые слова: информационная безопасность; угрозы информационной безопасности; беспроводные сети; защита сетей от несанкционированного доступа; защита мобильных устройств; устойчивость паролей; уменьшение вероятности подбора пароля.

PASSWORD GENERATION FOR WIRELESS NETWORK WITH USING VARIABLE COMPLICATION RULE

The most dangerous information lately are open Wi-Fi networks. Anyone can connect to them and perform certain malicious actions. Conditionally protected networks in public places or organizations that you can connect to can be considered dangerous, for example, know the password from an employee. One of the causes of cybernetic attacks on the resources of such networks are unsustainable passwords. Their use allows attackers to connect to specified networks and gain access to all devices connected to networks. In addition, if an unstable or standard password is used for the settings panel, then all devices are also at risk of a cyber attack, which can be carried out remotely. The use of an integrated approach by attackers for unauthorized access to wireless communication systems (by combining social engineering and data interception with the use of malware), as well as new types of cyber attacks, which allow to install malicious software on mobile devices can reduce the effectiveness of existing methods and means of protecting wireless networks. In order to avoid such and similar problems, the article proposes a way to increase the protection of wireless networks from intercepting information and influencing it by creating a password that is resistant to selection with a varying complexity rule. This

method can be used to create software and hardware security tools, as well as to enhance the protection of user accounts and other security systems where a strong password is required. Considering the statistics and the calculations carried out in the work, it can be argued that the introduction of a method for generating complicated passwords will significantly increase the level of security of wireless networks.

Keywords: information security; threats of information security; wireless networks; protection of networks from unauthorized access; mobile devices protection; password resilience; reduce the likelihood of password cracking.

Бурячок Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.
E-mail: v.buriachok@kubg.edu.ua.
Orcid ID: 0000-0002-4055-1494.
Бурячок Владимир Леонидович, доктор технических наук, профессор, заведующий кафедрой информационной и кибернетической безопасности Киевского университета имени Бориса Гринченко.
Buriachok Volodymyr, Doctor of Technical Sciences, Professor, Head of the Department of Information and cyber security of Borys Grinchenko Kyiv University.

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.
E-mail: a.anosov@kubg.edu.ua.
Orcid ID: 0000-0002-2973-6033.
Аносов Андрей Александрович, кандидат военных наук, доцент, доцент кафедри информационной и кибернетической безопасности Киевского университета имени Бориса Гринченко.
Anosov Andii, PhD in military Sciences, Associate Professor, Associate Professor of the Department of Information and cyber security of Borys Grinchenko Kyiv University.

Платоненко Артем Вадимович, старший викладач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.
E-mail: a.platonenko@kubg.edu.ua.
Orcid ID: 0000-0002-2962-5667.
Платоненко Артем Вадимович, старший преподаватель информационной и кибернетической безопасности Киевского университета имени Бориса Гринченко.
Platonenko Artem, Senior Lecturer of the Department of Information and cyber security of Borys Grinchenko Kyiv University.