© Buriachok V., Platonenko A., Semko O. Selection of the rational password generation method for the expected multiples // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 1, pp. 59-64.

DOI: 10.18372/2225-5036.25.13668

ВИБІР РАЦІОНАЛЬНОГО СПОСОБУ ГЕНЕРУВАННЯ ПАРОЛІВ СЕРЕД МНОЖИНИ ІСНУЮЧИХ

Володимир Бурячок[1], Артем Платоненко [1], Олексій Семко [2]

[1]Київський університет імені Бориса Грінченка, Україна
[2] Інститут телекомунікацій і глобального інформаційного простору НАН України

БУРЯЧОК Володимир Леонідович, д.т.н., професор

Рік та місце народження: 1963 рік, м. Лутугіно Луганської обл., Україна
Освіта: Київське Вище інженерне радіотехнічне училище ППО, 1985 рік
Посада: завідувач кафедри Інформаційної та кібернетичної безпеки з 2018 року.
Наукові інтереси: системний аналіз, математичне моделювання та програмування; прийняття рішень та науково-технічне прогнозування; нові досягнення в галузі інформаційних технологій; теорія і практика інформаційної та кібернетичної безпеки
Публікації: більше 230 наукових публікацій, серед яких наукові статті у міжнародних та вітчизняних фахових журналах, підручники, монографії, тези доповідей на наукових конференціях і семінарах
E-mail: v.buriachok@kubg.edu.ua.
Orcid ID: 0000-0002-4055-1494.

ПЛАТОНЕНКО Артем Вадимович

Рік та місце народження: 1992 рік, м. Київ, Україна.
Освіта: Державний університет телекомунікацій, 2014 рік.
Посада: старший викладач кафедри Інформаційної та кібернетичної безпеки з 2018 року.
Наукові інтереси: інформаційні технології, інформаційна та кібернетична безпека.
Публікації: більше 15 наукових публікацій, серед яких колективна монографія, наукові статті, тези доповідей на наукових конференціях і семінарах
E-mail: a.platonenko@kubg.edu.ua.
Orcid ID: 0000-0002-2962-5667.

СЕМКО Олексій Вікторович

Рік та місце народження: 1993 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2015 рік.
Посада: молодший науковий співробітник відділу інформаційних та комунікаційних технологій з 2018 року.
Наукові інтереси: інформаційні технології, теорія управління.
Публікації: 18 наукових публікацій, серед яких наукові статті та свідоцтва авторського права
E-mail: semalek@meta.ua.
Orcid ID: 0000-0001-6473-1329.

Анотація. *У даній статті розглянуто метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку. Даний метод дає змогу забезпечити відмовостійкість бездротових мереж в умовах кібернетичних атак за рахунок вибору раціонального способу генерування паролів серед множини існуючих. Вибір найбільш доцільного для вдосконалення способу генерування паролів, серед сукупності можливих, здійснюється на підставі визначення та оцінки ступеня близькості між базовим способом та кожним способом-аналогом, що дозволяє генерувати паролі для парольних політик та проводиться, як за загальними вимогами, так і за сукупністю характеристик відповідних способів. Оцінка близькості між базовим способом та способом-аналогом з урахуванням характеристик дозволяє отримати оцінку невідповідності опису базового способу й кожного способу-аналога, з погляду збігу переліку їх характеристик.*

Ключові слова: *інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв.*

Вступ

Нестійкі паролі зазвичай стають причиною кібернетичних атак. Після того як зловмисник підключиться до мережі, він отримує доступ до всіх підключених пристроїв [1]. Крім того, якщо нестійкий або стандартний пароль використовується для панелі налаштувань, то всі пристрої піддаються ризику

кібернетичної атаки, яка може здійснюватися віддалено [2]. Знання звичайних користувачів в області інформаційної безпеки дуже обмежені й тому, значна кількість з них не приділяє часу для захисту своїх даних.

Третина всіх паролів, що використовуються, зламуються шляхом простого перебору варіантів зі словника [3-5]. Саме цим обумовлюється нагальна потреба застосування ускладнених паролів для забезпечення відмовостійкості систем бездротового зв'язку в умовах кібернетичних атак.

Аналіз існуючих досліджень

У роботі [6] проведено аналіз актуальних загроз та уразливостей для систем бездротового зв'язку, а також варіанти формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак [6, 7].

Метою даної роботи є висвітлення розробленого авторами методу обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх відмовостійкості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих.

Основна частина дослідження

Метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх відмовостійкості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих (табл.1). Під парольною політикою в цьому сенсі будемо розуміти перелік вимог для створення паролю.

Таблиця 1

Способи генерування паролів

Назва способу	Стисла характеристика	Рівень стійкості
Спосіб заміни слів	базується на написанні паролю літерами з іншої розкладки клавіатури	*нестійкий*, оскільки більшість часто вживаних слів на певній мові використовуються для створення словників паролів
Спосіб випадкового натискання клавіш	базується на натисканні клавіш у певному порядку, не відриваючи руки	*нестійкий*, оскільки словники із «змієподібними» комбінаціями паролів (введеними затиснутим пальцем за певним маршрутом на клавіатурі) також існують
Спосіб «обчислюваних людиною» паролів	базується на формуванні матриці з символами, наприклад назви ресурсу, та подальшої заміни обраних символів, за певним правилом	може бути зручним для використання захисту онлайн-ресурсів, але генерування паролю для бездротової мережі з 63 символів таким способом не дасть необхідної стійкості та займе багато часу
Спосіб генерування паролів завдяки асоціаціям	базується на застосуванні технології асоціацій та замін певних літер символами	може бути легшим для запам'ятовування, але також не несе за собою необхідної стійкості та потребує значного часу на генерування
Спосіб створення паролів з декількох слів	базується на логічному поєднанні слів із зміною певних символів	може дати більш складний пароль, але його стійкість, також не можна вважати високою, а час на генерування може бути ще більшим
Спосіб створення паролів завдяки генеруванню випадкових чисел	базується на використанні гральних кубиків для генеруванні випадкових чисел та подальшого вибору слів за таблицею	може займати менше часу для генерування паролю, але стійкість створеного паролю важко вважати високою, оскільки можливе використання словників для підбору
Спосіб генерування випадкових паролів	базується на генеруванні паролів завдяки спеціальним командам та додаткам в операційній системі	може дати складніший результат та потребує набагато меншу часу для створення, але питання випадкового генерування такого ж самого паролю зловмисником, хоча й малоймовірне, але все ж таки можливе

Примітка: з проблемами, що відображені в табл. 1 можна зіткнутися не тільки при застосуванні онлайн-генераторів, а й при використанні відповідного ПЗ для створення паролів.

Основними умовами щодо обґрунтованого вибору найбільш доцільного для вдосконалення способу генерування паролів, серед сукупності можливих, є:

– *по-перше*, дослідження однієї із важливих якостей парольних політик, а саме стійкості до підбору та з'ясування можливості щодо її підвищення в результаті проведення вдосконалення;

– *по-друге*, проведення раціонального вибору "базового способу" серед сукупності можливих способів, що досліджуються.

При цьому, під стійкістю паролю будемо розуміти мінімальну ймовірність його підбору (чим більша стійкість паролю – тим менша ймовірність підбору і навпаки, більша ймовірність підбору – буде означати меншу стійкість паролю), а в якості базового способу обиратимемо той, що відповідатиме вимогам до перспективного (ускладненого) способу генерування паролів у системах бездротового зв'язку.

Вибір найбільш доцільного для вдосконалення способу генерування паролів, серед сукупності можливих, здійснюється на підставі визначення та оцінки ступеня близькості (відстані) між базовим способом та кожним способом-аналогом, що дозволяє генерувати паролі для парольних політик та проводиться, як за загальними вимогами, так і за сукупністю характеристик відповідних способів. Вхідними даними для цього є:

– загальні вимоги до структури базового способу та його аналогів (час генерування, довжина паролю, стійкість до підбору);

– перелік характеристик (показників), що притаманні базовому способу та способам-аналогам

(кількість символів та можливість їх повторення, множини символів та необхідність їх поєднання, частота зміни паролю);

– вимоги до ускладненого способу генерування паролів у системах бездротового зв'язку (підвищення стійкості до підбору).

Процедура вибору найбільш доцільного для вдосконалення способу генерування паролів серед сукупності можливих, ґрунтується на модифікованому методі аналізу ієрархій Сааті та поєднує в собі такі кроки.

Крок 1. Пошук співвідношень між базовим способом і кожним способом-аналогом та розрахунок відстані між ними.

Здійснюється з урахуванням того, що:

1) вимоги до базового способу є частиною вимог до способу-аналогу:

$$p_0 = 1 - \frac{1+a_1}{2}, \text{ де } 0,3 < a_1 \le 1,5; \quad (1)$$

2) вимоги до способу-аналогу є частиною вимог до базового способу:

$$p_0 = 1 - \frac{1+a_2}{2}, \ 0 \le a_2 < 0,5; \quad (2)$$

3) перетинання вимог до способу-аналогу та вимог до базового способу (спосіб-аналог краще базового способу):

$$p_0 = 1 - \frac{b_1}{2}, \ a_1 < b_1 \le 1; \quad (3)$$

4) перетинання вимог до базового способу та вимог до способу-аналога (базовий спосіб краще способу-аналога):

$$p_0 = 1 - \frac{b_2}{2}, \ 0 \le b_2 < a_2, \quad (4)$$

де p_0 - відстань між характеристиками (показниками) базового способу та кожного із способів-аналогів за загальними вимогами; a_1, a_2 - коефіцієнти, що залежать від сумарної кількості подібних співвідношень, яких за основними характеристиками може бути, наприклад, не більше трьох. За умови, що подібні співвідношення взагалі відсутні - $a_1 = 0,25$ та $a_2 = 0,25$; b_1, b_2 - коефіцієнти, вибір значень яких здійснюється користувачем, який в даному випадку виконує роль експерта, за правилами: $b_1 \in]a_1, 1[$; $b_2 \in]0, a_2[$.

Крок 2. Оцінка близькості (відстані) між базовим способом та способом-аналогом з урахуванням характеристик.

Способи генерування паролів із сукупності однотипних, обраних для порівняння (табл. 2), розташовуються експертами в порядку убування їх значимості. В даному ряду першим номером буде фігурувати базовий спосіб.

Заповнення матриць парних порівнянь способів генерування паролів із досліджуваної сукупності - $A_j = \left[a_{11}, ..., a_{in}, ..., a_{QQ} \right]$ за кожним $j-$м показником (характеристикою): $A_j = \left| a_{in}^{(j)} \right|$, $i, n = \overline{1,Q}$, $j = \overline{1,L}$ - відбувається за методом парних порівнянь декількома незалежними експертами (групами експертів) на підставі оцінок їх характеристик, досвіду та інтуїції експертів, з використанням відповідної п'ятибальної шкали (де Q – кількість способів генерування паролів, що підлягають порівнянню).

Причому, в даному випадку елемент $a_{in}^{(j)}$ (5) матриці $\left(A_j \right)$ визначатиме вагу $i-$го способу генерування, відносно $n-$го при порівнянні їх за $j-$м показником. Пропонується таке правило, згідно з яким відбувається заповнення матриць $\left(A_j \right)$:

$$\alpha_k = \begin{cases} \alpha_1 - \textit{якщо спсооби за } j-\textit{м показником не відрізняються, тобто мають однакову важливість;} \\ \alpha_2 - \textit{якщо } i-\textit{й способи за } j-\textit{м показником має слабку перевагу над } n-\textit{м способом;} \\ \alpha_3 - \textit{якщо перевага помітна;} \\ \alpha_4 - \textit{якщо перевага } i-\textit{го способу за } j-\textit{м показником суттєва;} \\ \alpha_5 - \textit{якщо } i-\textit{й спосіб за } j-\textit{м показником має абсолютну перевагу над } n-\textit{м способом.} \end{cases} \quad (5)$$

Якщо $a_{in}^{(j)} = \alpha_k$, *де* $\alpha_k \neq 0$, $k = \overline{1,5}$ (наприклад, $\alpha_1 = 1$, $\alpha_2 = 3$, $\alpha_3 = 5$, $\alpha_4 = 7$, $\alpha_5 = 9$), то $a_{ni}^{(j)} = \frac{1}{a_k}$.

Причому $a_{ii} = 1$.

В результаті для кожного способу генерування паролів, серед тих, що порівнюються, формуються відповідні квадратні матриці, елементи яких задовольняють умові оберненої симетричності. На підставі знайдених: максимального власного значення $\lambda_{\max_{A_j}}$ кожної з матриць $\left(A_j \right)$ та притаманного йому власного вектору відбувається формування набору локальних пріоритетів способів генерування за кожною характеристикою:

$$k_j = \lambda_{\max_{A_j}}^{(j)} x_{B_{\text{л}j}}. \quad (6)$$

Зі значень $x_{B_{\text{л}j}}$ формується узагальнена власна матриця:

$$A_{B_{\text{л}ij}} = \left[x_{B_{\text{л}1}}, ..., x_{B_{\text{л}j}}, ... x_{B_{\text{л}L}} \right], \quad j = \overline{1,L}, \quad (7)$$

а потім проводиться нормування елементів кожного з її стовпчиків (вміщують в собі коефіцієнти важливості способу генерування за однією з характеристик):

$$A_{B_{\text{л}ij}}^{нор} = A_{B_{\text{л}ij}} \Big/ \sum_{i=1}^{Q} A_{B_{\text{л}ij}}, \quad i = \overline{1,Q}, \quad j = \overline{1,L}. \quad (8)$$

Формування матриці вагових коефіцієнтів важливості кожної характеристики - $B = \left[b_{11}, b_{jh}, ..., b_{LH} \right]$, де $b_{jh} = \beta_k$; $\beta_k \neq 0$; $k = \overline{1,5}$; $h = \overline{1,H}$; $j = \overline{1,L}$, для способу генерування паролів, відбувається за способом безпосередньої оцінки в межах заданої п'ятибальної шкали на підставі врахування

значимості даних характеристик під час вирішення однієї й тієї ж задачі, згідно з міркуваннями H експертів-спеціалістів. Правило, згідно з яким кожній характеристиці надається свій бал, вибираємо таке (при цьому, наприклад: $\beta_1 = 1$, $\beta_2 = 3$, $\beta_3 = 5$, $\beta_4 = 7$, $\beta_5 = 9$):

$$\beta_k = \begin{cases} \beta_1 & - \textit{ можливо не враховувати} \\ \beta_2 & - \textit{ бажано враховувати} \\ \beta_3 & - \textit{ враховувати обов'язково} \\ \beta_4 & - \textit{ важливий} \\ \beta_5 & - \textit{ дуже важливий} \end{cases}. \qquad (9)$$

Нормована вага $j-$ї характеристики, визначена $h-$м експертом, при цьому становить: $b_{jh}^{нор} = b_{jh} \Big/ \sum_{j=1}^{L} b_{jh}$, де $h = \overline{1,H}$. Середнє значення вагового коефіцієнта (коефіцієнта значимості) для $j-$ї характеристики, визначене H експертами, обчислюється за такою формулою:

$$b_j^{середнє} = \sum_{h=1}^{H} b_{jh}^{нор} \Big/ \sum_{h=1}^{H}\sum_{j=1}^{L} b_{jh}^{нор}, \quad h = \overline{1,H}, \quad j = \overline{1,L}. \qquad (10)$$

При цьому, якщо виникає ситуація коли декілька характеристик способу-аналога відповідають одній вимозі базового способу, або ж навпаки - декілька вимог базового способу відповідають одній характеристиці способу-аналога, вирішується задача щодо приведення кількості вимог базового способу, що розглядаються та способу-аналога до однакової кількості. Це реалізується шляхом підсумовування середніх значень їх вагових коефіцієнтів (коефіцієнтів значимості) - $b_j^{середнє}$:

$$b^p = \sum_{j=1}^{p} b_j^{середнє}.$$

За умови відсутності даних про вимоги до перспективного (ускладненого) способу генерування паролів, аналогічні характеристики способів-аналогів виключаються з подальшого розгляду.

Значення вектору переваг для способів генерування паролів з досліджуваної сукупності визначаються шляхом перемноження узагальненої власної матриці (кореляційної функції способів генерування за всіма характеристиками) на вектор усереднених коефіцієнтів значимості кожної характеристики:

$$\gamma = A_{Вл_{ij}}^{нор} \cdot b_j^{середнє} = \begin{bmatrix} x_{11} & \dots & x_{1j} & \dots & x_{1L} \\ \dots & \dots & \dots & \dots & \dots \\ x_{i1} & \dots & x_{ij} & \dots & x_{iL} \\ \dots & \dots & \dots & \dots & \dots \\ x_{Q1} & \dots & x_{Qj} & \dots & x_{QL} \end{bmatrix} \cdot \begin{bmatrix} b_1^{середнє} \\ \dots \\ b_j^{середнє} \\ \dots \\ b_L^{середнє} \end{bmatrix} = \left(\gamma_{сп}^{баз}, \gamma_{ан_1}, \dots, \gamma_{ан_i}, \dots, \gamma_{ан_Q}\right). \qquad (11)$$

При цьому, зважаючи на те, що попередньо способи генерування паролів із сукупності однотипних, обраних для порівняння, були розташовані експертами в порядку убування їх значимості, отриманий вектор переваг також відповідатиме даній закономірності. Причому на першому місці буде знаходитись показник, що характеризуватиме базовий (перспективний або ускладнений) спосіб.

Оцінка близькості (відстані) між базовим способом та способом-аналогом з урахуванням характеристик дозволяє отримати оцінку невідповідності опису базового способу й кожного способу-аналога, з погляду збігу переліку їх характеристик. При аналізі формули (11) можливі такі варіанти зіставлення:

– існує однозначна відповідність між способом та його аналогом. Відстань між базовим способом та способи-аналогами за характеристиками (p_T) знаходиться за формулою:

$$p_T = \gamma_{сп}^{баз} - \gamma_{ан}; \qquad (12)$$

– спосіб-аналог не відповідає базовому способу. У даному випадку робиться висновок про те, що опис способу-аналога обтяжений зайвими характеристиками, які доцільно викреслити з процесу порівняння.

Крок 3. Формування комплексної (узагальненої) оцінки для кожної пари базовий спосіб – спосіб-аналог із досліджуваної сукупності.

В даному випадку можливі такі співвідношення:

а) отримані оцінки відстані близькі за значеннями. При цьому показник комплексної узагальненої оцінки ступеня близькості базового способу та способів-аналогів (p) знаходимо шляхом усереднення значень оцінок відстані за загальними вимогами характеристиками (показниками):

якщо $\left|\dfrac{p_0 - p_T}{p_{\max}}\right| \le 0{,}1$, то $p = \dfrac{p_0 + p_T}{2}$; (13)

б) оцінка відстані за загальними вимогами суттєво менша оцінки відстані за характеристиками (відповідає неповній кореляції між оцінками, що згадувались). При цьому показник p знаходимо з формули:

якщо $\dfrac{p_T - p_0}{p_{\max}} > 0{,}1$, то $p = p_0 + k_1 p_T$, (14)

де $k_1 = \left|\dfrac{p_T - p_0}{p_{\max}}\right|$.

в) оцінка відстані за характеристиками суттєво менша оцінки відстані за загальними вимогами (відповідає неповній кореляції між згадуваними оцінками). При цьому показник p знаходимо з формули:

якщо $\dfrac{p_0 - p_T}{p_{\max}} > 0{,}1$, то $p = p_T + k_2 p_0$, (15)

де $k_2 = \left|\dfrac{p_0 - p_T}{p_{\max}}\right|$,

де p_{max} - максимальне значення коефіцієнта p_T; p_T - відстань за між базовим способом та способами-аналогами; p_0 - відстань між характеристиками (показниками) базового способу та кожного із способів-аналогів за загальними вимогами; k_1, k_2 - коефіцієнти, що відображують невідповідність оцінок та вибираються за допомогою експертного аналізу.

Для проведення заходів з вдосконалення обирається той спосіб із всіх можливих пар «базовий спосіб – спосіб-аналог» із досліджуваної сукупності, для якого коефіцієнт комплексної (узагальненої) оцінки буде найбільшим (табл. 2).

Таблиця 2

Порівняння способів генерування паролів за загальними вимогами

Назва способу	Час генерування	Довжина паролю	Стійкість паролю
Спосіб генерування випадкових паролів	**0,950**	**0,980**	**0,935**
Спосіб створення паролів завдяки генеруванню випадкових чисел	0,720	0,715	0,750
Спосіб створення паролів з декількох слів	0,318	0,529	0,597
Спосіб генерування паролів завдяки асоціаціям	0,210	0,312	0,389
Спосіб «обчислюваних людиною» паролів	0,152	0,214	0,247
Спосіб випадкового натискання клавіш	0,368	0,390	0,189
Спосіб заміни слів	0,169	0,369	0,125

Висновки

Таким чином, за коефіцієнтом переваг γ та показником комплексної узагальненої оцінки ступеня близькості (відстані) між базовим способом генерування паролів і кожним способом-аналогом (табл. 1) найбільш раціональним для забезпечення функціональної безпеки систем бездротового зв'язку, за рахунок вдосконалення парольних політик, є спосіб генерування випадкових паролів (табл. 2).

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]. Программы для создания словарей. [Електронний ресурс]. Режим доступу: https://hackware.ru/?p=2661.

[4]. Взлом пароля методом грубой силы. Изучаем bruteforce атаку. [Електронний ресурс]. Режим доступу: https://geekmaze.ru/2016/03/04/izuchaem-bruteforce-ataku/.

[5]. Грубая сила против паролей. [Електронний ресурс]. Режим доступу: https://geektimes.ru/company/amd/blog/277068/.

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

[7]. А. Платоненко, А. Аносов, "Средства защиты современных мобильных устройств в сетях нового поколения", *Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите»*. Київ: ДУТ, 2017.

УДК 004.62

Бурячок В., Платоненко А. Выбор рационального способам генерирования паролей среди множества существующих

Аннотация. *В данной статье рассмотрен метод обоснования решения на совершенствование парольных политик в системах беспроводной связи. Данный метод позволяет обеспечить отказоустойчивости беспроводных сетей в условиях кибернетических атак за счет выбора рационального способа генерирования паролей среди множества существующих. Выбор наиболее целесообразного для совершенствования способа генерирования паролей, среди совокупности возможных, осуществляется на основании определения и оценки степени близости между базовым способом и каждым способом-аналогом, что позволяет генерировать пароли для парольных политик и проводится, как по общим требованиям, так и по совокупности характеристик соответствующих способов. Оценка близости между базовым способом и способом-аналогом с учетом характеристик позволяет получить оценку несоответствия описания базового образа и каждого способа-аналога, с точки зрения совпадения перечня их характеристик.*

Ключевые слова*: информационная безопасность, угрозы информационной безопасности, беспроводные сети, защита сетей от несанкционированного доступа, защита мобильных устройств.*

Buriachok V., Platonenko A., Semko O. Selection of the rational password generation method for the expected multiples

Abstract. *This article discusses the method of justification of the decision to improve the password policies in wireless communication systems. This method allows to provide deflection of wireless networks in the conditions of cybernetic attacks by choosing a rational way of generating passwords among the set of existing ones. The most expedient choice to improve the method of generating passwords, among the possible set, is based on the determination and evaluation of the proximity between the base method and each analogue method, which allows you to generate passwords for passwords policies and conducted in accordance with the general requirements and the set of characteristics appropriate methods. The procedure for choosing the most expedient way to improve the method of generating passwords among a set of possible ones, is based on a modified Saati hierarchy analysis method. In the absence of data on the requirements for a promising (complicated) method of generating passwords, similar characteristics of analogue methods are excluded from further consideration. Estimation of the proximity between the basic method and the analogue method taking into account the characteristics allows to obtain an assessment of the inconsistency of the description of the base method and each analogue method in terms of the coincidence of the list of their characteristics. In order to carry out improvement activities, the method is chosen from all possible pairs "Base method - method-analogue" from the population under study for which the coefficient of the*

integrated (generalized) estimation will be the largest. Thus, there is a way of generating random passwords based on the benefit coefficient and the indicator of an integrated generalized assessment of the proximity (distance) between the basic method of generating passwords and each method analogue most rational for ensuring the functional security of wireless systems, due to the improvement of the password policies.

Keywords: *information security, information security threats, wireless networks, unauthorized access network protection, protection of mobile devices.*

Отримано 3 *лютого 2019 року*, затверджено редколегією *15 березня 2019 року*