МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ НАН УКРАЇНИ

ПЛАТОНЕНКО Артем Вадимович

УДК 004:004.056:004.7(043.3)

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ НА ОСНОВІ ВДОСКОНАЛЕННЯ ПАРОЛЬНИХ ПОЛІТИК

05.13.06 – «Інформаційні технології»

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2019

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційної та кібернетичної безпеки факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Бурячок Володимир Леонідович
Київський університет імені Бориса Грінченка
завідувач кафедри інформаційної
та кібернетичної безпеки
факультету інформаційних технологій та управління

Офіційні опоненти: доктор технічних наук, професор
Бараннік Володимир Вікторович
Харківський національний університет Повітряних Сил імені Івана Кожедуба, начальник кафедри бойового застосування та експлуатації АСУ

доктор технічних наук, доцент
Зибін Сергій Вікторович
Національний авіаційний університет,
професор кафедри інженерії програмного забезпечення

Захист відбудеться «29» жовтня 2019 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.255.01 при Інституті телекомунікацій і глобального інформаційного простору НАН України за адресою:
03186, м. Київ, бул. Чоколівський, 13, ауд. 601.

З дисертацією можна ознайомитись у бібліотеці Інституту телекомунікацій і глобального інформаційного простору НАН України за адресою:
03186, м. Київ, бул. Чоколівський, 13.

Автореферат розісланий «27» вересня 2019 р.

Вчений секретар
спеціалізованої вченої ради
к. т. н О. Г. Лебідь

ВСТУП

Обґрунтування вибору теми дослідження. Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається. З використанням високошвидкісних мобільних мереж, загрози інформаційної безпеки для державних та приватних установ дедалі збільшуються, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи. Отже для зловмисників відкриваються більші технічні можливості для здійснення атак, що потребує впровадження засобів захисту інформації. Зважаючи, на таке, питання щодо забезпечення функціональної безпеки (доступності та цілісності) систем бездротового зв'язку є надзвичайно актуальними.

Дослідженню проблеми захищеності бездротових мереж присвячені роботи Н. І. Битюцької, В. Л. Бурячка, О. Л. Весельської, В. І. Ніконова, С. В. Толюпи, Л.А. В. О. Хорошка, Шувалової, О. К. Юдіна, А.В. Чунарьової, L. Badman, R. Bartz, J. Doherty, F. Garzia та багатьох інших. За їх висновками встановлено, що основними проблемами захищеності систем бездротового зв'язку 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.

Способи, які використовувались для вирішення даної проблеми (парольні політики користувачів з обмеженням по кількості символів; генерування паролів на основі поєднанні декількох слів, або заміни слів іншою мовою; генерування випадкових чисел для вибору слів за таблицею, генератори випадкових значень паролів з певної множини символів і т.п.), не повною мірою відповідають викликам сьогодення. З огляду на це, розробка технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик за рахунок генерування паролю з використанням інтегрованого підходу, є **актуальною науковою задачею,** що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами.

Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», а також Стратегією кібербезпеки України від 15 березня 2016 року №96/2016. Результати роботи відображені у звітах з науково-дослідної роботи «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем (ІКС) в умовах впливу кібернетичних атак» (номер державної реєстрації 0114U000391), яка виконувалась в Державному університеті телекомунікацій й у якій здобувач брав участь у якості виконавця.

Мета і завдання дослідження. *Метою дисертаційної роботи* є забезпечення відмовостійкості систем бездротового зв'язку за рахунок підвищення стійкості парольних політик до спроб несанкціонованого доступу.

Досягнення поставленої мети вимагає вирішення таких **завдань**:

1) проведення аналізу множини існуючих актуальних загроз та уразливостей системам бездротового зв'язку, а також варіантів формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак;

2) розроблення методу обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, для забезпечення їх надійності і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих;

3) удосконалення способу або інакше методу генерування ускладнених паролів за показниками довжини та набору символів, з метою формування більш стійких паролів, у порівнянні з відомими способами-аналогами.

Зважаючи на таке **об'єктом дослідження** в роботі є процес забезпечення функціональної безпеки систем бездротового зв'язку. **Предметом дослідження** – інформаційна технологія забезпечення функціональної безпеки систем бездротового зв'язку в умовах загроз і обмежень, визначених специфічними умовами функціонування таких систем.

Методи дослідження. Проведені дослідження базуються на методах теорії множин (для формалізації процесів формування вимог до парольних політик, а також ідентифікації і визначення повноти їх забезпечення), теорії ймовірностей і математичної статистики (для розробки й дослідження алгоритмів генерування парольних множин), експертного оцінювання (для визначення коефіцієнтів стійкості, а також встановлення зв'язків між базовим способом генерування паролю та відповідними способами-аналогами), математичного моделювання (для оцінювання повноти виконання множини вимог), порівняння (для визначення оптимального способу генерування паролів), графічний (для відображення моделей атак та парольних множин), формалізації (для опису розробленого способу ускладнення паролів).

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик. Новими результатами, отриманими в дисертаційній роботі, є:

- *вперше розроблений* метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, **впровадження якого** за рахунок проведення процедури оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом **дозволило**, на відміну від подібних, серед множини існуючих способів генерування паролів обрати спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;

- *удосконалений* спосіб генерування випадкових паролів для систем бездротового зв'язку, **впровадження якого** завдяки урахуванню можливості співпадіння з паролями системи словників та використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення), **забезпечило** порівняно з аналогами підвищення рівня захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $\mathbf{3{,}73 \cdot 10^4}$ разів.

Практичне значення отриманих результатів у сукупності складає підґрунтя для реалізації програмних засобів, для захисту систем бездротового зв'язку, що застосовуються на об'єктах інформаційної діяльності.

Практична цінність отриманих результатів полягає в програмній реалізації:

по-перше, методу формування парольних політик, що дозволяє раціонально обрати спосіб генерування паролів серед множини існуючих;

по-друге, способу генерування ускладнених паролів в системах бездротового зв'язку, що дозволяє сформувати стійкий до підбору пароль.

Отримані результати забезпечують зменшення: витрат часу на створення паролю приблизно на 20%, а також ймовірності злому паролю шляхом збільшення часу для його можливого підбору в $3{,}73 \cdot 10^4$ разів. Результати дисертаційного дослідження впроваджено у навчальний процес Київського університету імені Бориса Грінченка (акт впровадження від 15.04.2019), а також в практику розроблення політик інформаційної безпеки ТОВ "НТК"ТЕХНОЛОГІЇ БЕЗПЕКИ (акт впровадження від 20.03.2019) та ТОВ «Квадрокоптер» (акт впровадження від 19.04.2019).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належить: в [1,12] – дослідження видів атак на бездротові мережі та види їх захисту, [2] – аналіз підходів до оцінки захищеності мережі; в [3] – оптимізація алгоритму синтезу систем захисту інформації; в [4] – перелік можливих наслідків для засобів інформатизації та аналіз можливих наслідків електромагнітного впливу в залежності від галузі використання інформаційних систем; в [5] – розгляд топології та видів розподілу, що використовуються; в [7,10] – аналіз вразливості бездротових мереж, описання та графічне зображення моделі перехоплення та захисту інформації в бездротових мережах; в [9, 11] – аналіз систем для підбору, розрахунки та графічне зображення способу.

Апробація результатів дисертації. Основні положення і результати досліджень доповідалися та обговорювалися на: Науково-технічній конференції «Актуальні проблеми забезпечення інформаційної безпеки держави» (м. Київ, ДУТ, грудень 2014); Студентській науково-технічній конференції молодих вчених присвячена Дню науки «Світ телекомунікації та інформатизації» (м. Київ, ДУТ, травень 2015); Міжнародній науково-технічній конференції «Актуальні проблеми розвитку науки і техніки» (м. Київ, ДУТ, жовтень 2015); Міжнародній науково-технічній конференції «Сучасні інформаційно-телекомунікаційні технології» (м. Київ, ДУТ, листопад 2015), Міжнародній науково-технічній конференції студентства та молоді «Світ телекомунікації та інформатизації» (м. Київ, ДУТ, грудень 2015); II Міжнародній науково-практичній конференції «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» (м. Київ, ДУТ, листопад 2016); III Міжнародній науково-технічній конференції студентства та молоді» (м. Київ, ДУТ, грудень 2016); Міжнародній конференції «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» (м. Київ, ДУТ, червень 2017).

Публікації. За результатами дисертаційної роботи опубліковано 20 наукових праць (11 статей, з них 9 – у співавторстві), серед яких: 9 наукових статей, написаних у співавторстві й опублікованих у наукових спеціалізованих фахових виданнях України та країн СНД, які включені до міжнародних наукометричних баз, 2 статті без співавторів.

Разом з тим основні наукові результати додатково відображені у 8 тезах доповідей на науково-технічних конференціях, а також видана за кордоном колективна монографія.

Із праць, що опубліковано в співавторстві, у дисертаційній роботі використано виключно ті результати, які одержано здобувачем особисто.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і має 120 сторінок основного тексту, 25 рисунків, 10 таблиць. Список використаних джерел містить 95 найменувань і займає 8 сторінок. Загальний обсяг дисертаційної роботи – 138 сторінок.

ОСНОВНИЙ ЗМІСТ

У **вступі** обґрунтовано актуальність теми, сформульовано мету і завдання досліджень, визначено наукову новизну та практичне значення роботи, наведено відомості про публікації, апробацію та впровадження результатів роботи.

У **першому розділі**:

1) проведено аналіз статистичних даних щодо наявності мобільних пристроїв та їх підключень мешканцями України, а також множини актуальних загроз та уразливостей для систем бездротового зв'язку в умовах кібернетичних атак;

2) сформовано загальну модель перехоплення та захисту інформації в бездротових мережах зображено на рис. 1 та описано в таблиці 1.

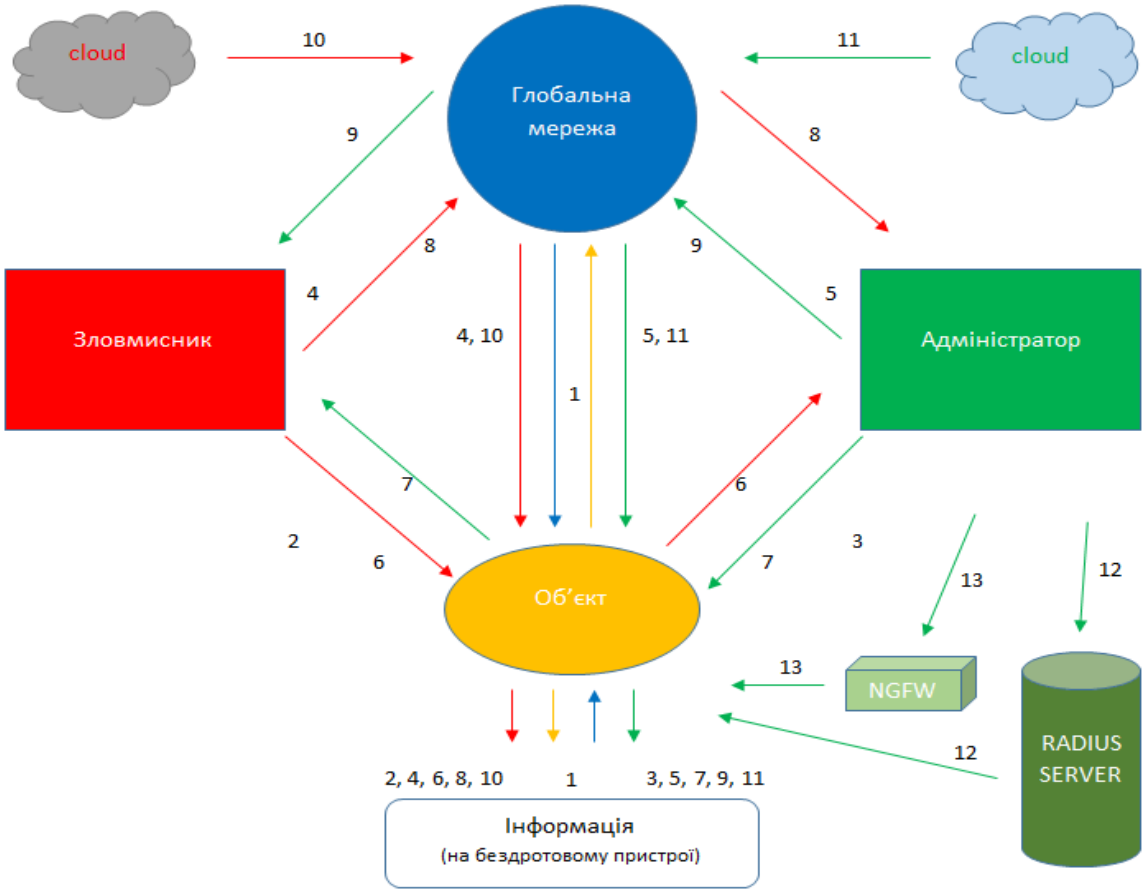

Рис. 1. Загальна модель перехоплення та захисту інформації в бездротових мережах

Таблиця 1

Опис дій та засобів, що використовуються зловмисниками/адміністраторами при перехопленні/захисті інформації в бездротових мережах

Зловмисник	Адміністратор
1. Стандартна взаємодія пристрою з глобальною мережею через точку доступу (нормальний стан).	
2. Вплив на бездротову мережу з метою перехоплення інформації з пристрою.	3. Засоби захисту адміністратора для бездротової мережі.
4. Вплив на інформацію через глобальну мережу та вразливості зв'язку між нею та точкою доступу.	5. Засоби захисту для каналу зв'язку між глобальною мережею та точкою доступу.
6. Прямий вплив на адміністратора через бездротову мережу.	7. Засоби протидії від прямого впливу зловмисника на бездротову мережу.
8. Прямий вплив на адміністратора через глобальну мережу.	9. Засоби протидії від прямого впливу зловмисника на глобальну мережу.
10. Вплив на бездротову мережу через глобальну з використанням хмарних технологій.	11. Захист бездротової мережі через глобальну з використанням хмарних технологій.
	12. Захист бездротової мережі з використанням RADIUS-SERVER.
	13. Захист бездротової мережі із застосуванням NGFW.

За отриманими результатами встановлено, що практично кожен другий мешканець нашої держави (45%) має смартфон з сенсорним екраном. Порівняно з 2015 роком простежується зростання користувачів з 26% до 45%, у випадку загального населення (рис. 2), та з 59% до 85% – у випадку осіб до 30 років. При цьому, якщо серед молоді 85% користуються смартфонами, то серед осіб літнього віку цей показник становить всього 6%. В останні два роки частка застосування смартфонів мешканцями України виросла на 26%. За прогнозами світових лідерів до 2020 року вона досягне більш ніж 70%.

Нині понад 68% користувачів смартфонів мають досвід встановлення додатків. Недосвідчені користувачі мобільних пристроїв випадково встановлюють зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Кількість мобільних підключень в Україні вже становить більш ніж 58,2 млн, з яких 26% становлять 3G-підключення. Оскільки через 5 років більших обсягів наберуть мережі 4G кількість мобільних підключень в Україні зросте майже на 6 млн. Загалом же по усьому світу до мереж мобільної передачі даних в цей період приєднається понад 2,6 млрд нових абонентів. Небезпеку для інформації несуть також і відкриті Wi-Fi мережі, адже кожен має змогу підключитись до них та виконувати певні зловмисні дії. Небезпечними також можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись, наприклад, дізнавшись пароль у працівника.

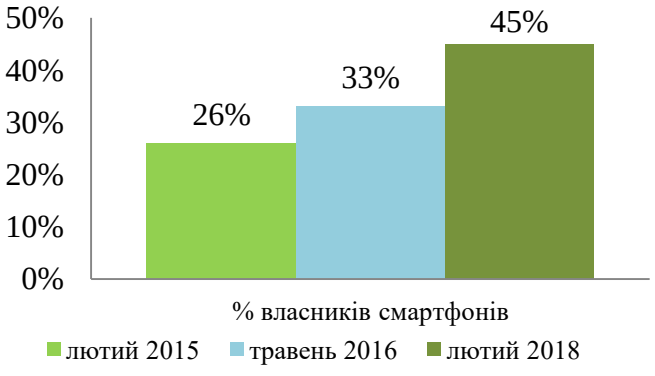

Рис. 2. Кількість власників смартфонів в Україні

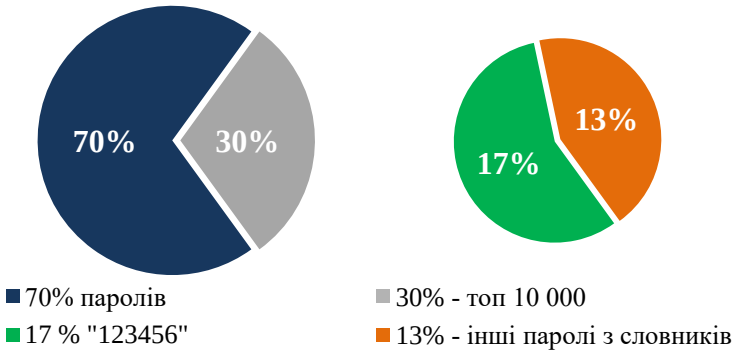

Рис. 3. Розподіл паролів користувачів

Тобто, нестійкі паролі зазвичай стають причиною кібернетичних атак. Після того як зловмисник підключиться до мережі, він отримує доступ до всіх підключених пристроїв. Крім того, якщо нестійкий або стандартний пароль використовується для панелі налаштувань, то всі пристрої піддаються ризику кібернетичної атаки, яка може здійснюватися віддалено. При цьому, наприклад, 30% користувачів використовують в якості пароля слово з топ - 10 000 паролів. З них майже 17% облікових записів банально захищені відомим паролем «123456» (рис. 3), або йому подібним. Застосування таких розповсюджених паролів як «1q2w3e4r» і «123qwe» показує, що деякі користувачі намагаються використовувати поєднання символів для створення захищених паролів, проте їх зусилля є недостатніми, оскільки програми для злому паролів, засновані на словниках, в першу чергу аналізують такі поширені варіанти. Це призводить до того, що:

- зловмисник (атакуючий), використовуючи для проникнення в мережу зламані облікові записи користувачів, що не були захищені стійким паролем (76% вдалих атак на мережу), може знаходитись в мережі компанії в середньому 243 дні, перш ніж його несанкціоноване підключення буде виявлено;

- основні загрози інформаційній безпеці організацій приносить застосування співробітниками мобільних пристроїв (51%) та Інтернет речей (21%);

- збиток, нанесений зловмисником (атакуючим) в результаті кібератаки, буде виражатись переважно у збоях систем (58,4%), втраті даних (25,2%) і несанкціонованому доступі (14,9%) та може привести до репутаційних втрат компаній, обумовлених невиправданими втратами часу на відновлення режиму нормального функціонування системи.

Таким чином, за результатами проведеного аналізу множини актуальних загроз та уразливостей для систем бездротового зв’язку в умовах кібернетичних атак можна зробити наступні висновки:

по-перше, знання звичайних користувачів в області інформаційної безпеки дуже обмежені й тому, значна кількість з них не приділяє часу для захисту своїх даних;

по-друге, третина всіх паролів, що використовуються, зламуються шляхом простого перебору варіантів зі словника;

по-третє, саме цим обумовлюється нагальна потреба застосування ускладнених паролів для забезпечення відмовостійкості систем бездротового зв’язку в умовах кібернетичних атак.

У **другому розділі** розроблено метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв’язку, для забезпечення їх надійності функціональної безпеки і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих (табл.2). Під парольною політикою в цьому сенсі будемо розуміти перелік вимог для створення паролю. 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.

Таблиця 2

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. 2, можна зіткнутися не тільки при застосуванні онлайн-генераторів, а й при використанні відповідного ПЗ для створення паролів.

При цьому, під стійкістю паролю будемо розуміти мінімальну ймовірність його підбору (чим більша стійкість (надійність) 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 генерування паролів 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 генерування паролів 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 - $A_j = [a_{11}, ..., a_{in}, ..., a_{QQ}]$ 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 (A_j) 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 (A_j):

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

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 (A_j) та притаманного йому власного вектору відбувається формування набору локальних пріоритетів способів генерування за кожною характеристикою:

$$k_j = \lambda_{\max_{A_j}}^{(j)} x_{Вл_j}. \tag{6}$$

Зі значень $x_{Вл_j}$ формується узагальнена власна матриця:

$$A_{Вл_{ij}} = \left[x_{Вл_1}, ..., x_{Вл_j}, ... x_{Вл_L} \right], \quad j = \overline{1,L}, \tag{7}$$

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

$$A_{Вл_{ij}}^{нор} = A_{Вл_{ij}} \Big/ \sum_{i=1}^{Q} A_{Вл_{ij}}, \quad i = \overline{1,Q}, \quad j = \overline{1,L}. \tag{8}$$

Формування матриці вагових коефіцієнтів важливості кожної характеристики - $B = \lfloor b_{11}, b_{jh}, ..., b_{LH} \rfloor$, 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: $\beta_1 = 1$, $\beta_2 = 3$, $\beta_3 = 5$, $\beta_4 = 7$, $\beta_5 = 9$):

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

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:

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

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:

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

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 генерування паролів 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 способами-аналогами за характеристиками (p_T) знаходиться за формулою:

$$p_T = \gamma_{сп}^{баз} - \gamma_{ан}, \quad (12)$$

– 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 генерування паролів 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):

$$\text{якщо} \quad \left| \frac{p_0 - p_T}{p_{\max}} \right| \le 0.1 \quad \text{то} \quad p = \frac{p_0 + p_T}{2}; \quad (13)$$

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:

$$\text{якщо} \quad \frac{p_T - p_0}{p_{\max}} > 0.1 \quad \text{то} \quad p = p_0 + k_1 p_T \text{, де} \quad k_1 = \left| \frac{p_T - p_0}{p_{\max}} \right|. \tag{14}$$

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:

$$\text{якщо} \quad \frac{p_0 - p_T}{p_{\max}} > 0.1 \quad \text{то} \quad p = p_T + k_2 p_0 \text{, де} \quad k_2 = \left| \frac{p_0 - p_T}{p_{\max}} \right|. \tag{15}$$

де p_{max} - максимальне значення коефіцієнта p_T;

p_T - відстань 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 генерування паролів із всіх можливих пар «базовий спосіб – спосіб-аналог» із досліджуваної сукупності, для якого коефіцієнт комплексної (узагальненої) оцінки буде найбільшим (табл. 3).

Таблиця 3

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

Таким чином, за коефіцієнтом переваг γ та показником комплексної узагальненої оцінки ступеня близькості (відстані) між базовим способом генерування паролів і кожним способом-аналогом (табл. 2) найбільш раціональним для забезпечення функціональної безпеки систем бездротового зв'язку, за рахунок вдосконалення парольних політик, є спосіб генерування випадкових паролів (табл. 3).

Третій розділ дисертації присвячено вдосконаленню обраного в другому розділі способу генерування випадкових паролів. Процедура (послідовність) вдосконалення полягає в такому.

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 4.

Таблиця 4

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

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.

Як результат, логічним, хоча і доволі тривіальним, 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.

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 символів, можливі різні значення кількості паролів. В таблиці 5 розглянуто можливі множини паролів для парольних політик, залежно від варіанту захисту бездротових мереж Wi-Fi з використанням WPA/WPA2.

Таблиця 5

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**	$\mathbf{6.03\cdot10^{21}}$	$1.19\cdot10^{109}$	$3.18\cdot10^{122}$
+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 5, 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 (табл. 2) 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.

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

Із сполучення множини паролів U_p відбирається множина U_z (рис. 4), що складається з паролів, які мають в собі 2 або 3 числа від двох до восьми цифр.

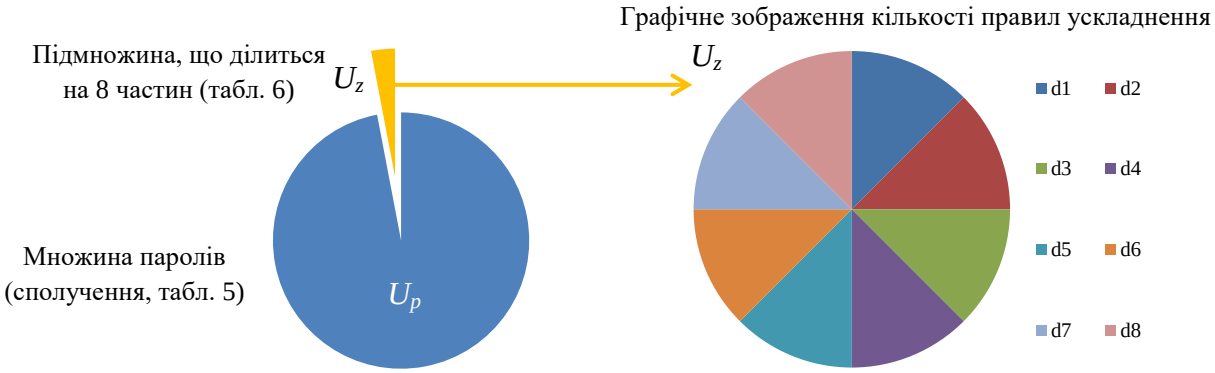

Рис.4. Кількість чисел, що можуть бути частиною паролю

До U_z потрапляють паролі, які містять 2 або 3 числа, довжиною від 2 до 8 цифр, або комбінацій набору символів, що можуть бути в словниках.

Із множини U_z за певним правилом *d (d1…d8)*, що визначається кількістю та довжиною чисел, виділяються 8 підмножин $U_{l(d)}$, (від 2 до 8 цифр), що прописуються в кожному рядку таблиці 6.

Таблиця 6

Кількість чисел, що можуть бути частиною паролю

$U_{l(d)}$	Кількість чисел у паролі	Кількість цифр у числі				Кількість комбінацій
d1	3	**3**	**3**	**3**	**1**	$U_{l\,(d1)}$
d2	3	**4**	**3**	**2**	**1**	$U_{l\,(d2)}$
d3	3	**4**	**3**	**3**		$U_{l\,(d3)}$
d4	3	**4**	**4**	**2**		$U_{l\,(d4)}$
d5	2	**5**	**5**			$U_{l\,(d5)}$
d6	2	**6**	**4**			$U_{l\,(d6)}$
d7	2	**7**	**3**			$U_{l\,(d7)}$
d8	2	**8**	**2**			$U_{l\,(d8)}$

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.4. Даний підхід забезпечує трирівневе ускладнення паролю, оскільки:

по-перше, при додаванні паролів обираються лише ті, що складаються з певної кількості цифр (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 такої ж процедури генерування паролів зловмисником.

Етап 4. Розрахунок кількості паролів для можливих парольних множин.

Формула розрахунку кількості можливих комбінацій паролів матиме вигляд:

$$U_{l(d)} = C_l^m \cdot C_{l-m}^m \cdot C_{l-2m}^m \cdot \ldots \cdot C_{l-(r-1)m}^m \cdot C_{l-rm}^m \quad (16)$$

де l – кількість літер алфавіту;

m – кількість літер в слові (3…6);

r = 1…m, при умові: $m<rm<l$.

В даному випадку добуток комбінацій означає поєднання значень паролів, кількість цифр у яких, сумарно дорівнює 10. Для кожної довжини чиста та поєднання отримаємо певне значення комбінацій, що може бути використане для розрахунку. Отже, для кожного $U_{l(d)}$ в таблиці 6 буде обчислене певне значення за формулою (16). Загальна кількість паролів для парольної множини U_z буде сумою значень підмножин $U_{l(d)}$, розрахованих за формулою (17):

$$U_z = U_{l(d1)} + \ldots + U_{l(d16)} \quad (17)$$

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 (18):

$$U_k = (U_p - U_z) \cdot U_z \quad (18)$$

де U_k – кількість паролів для кінцевої, ускладненої, множини паролів;

U_p – початкове значення кількості паролів (сполучення з таблиці 5);

U_z – значення кількості комбінацій чисел, з різної кількості цифр, формула (17).

Формула (18) 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 (19):

$$U_{k(d)} = (U_p - U_z) \cdot U_{l(d)} \quad (19)$$

де $U_{k(d)}$ – ускладнена комбінація за обраним правилом d,

U_p – початкове значення кількості паролів (сполучення з таблиці 5),
U_z – значення комбінацій чисел, з різної кількості цифр з формули (17),
$U_{l(d)}$ – кількість комбінацій чисел, з кількості цифр за правилом, формула (16).

Таким чином, зазначена процедура (послідовність) вдосконалення випадкового паролю завдяки використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (використовуючи змінний вибір правила ускладнення *d*), а також урахуванню можливостей співпадіння з паролями системи словників та розширення множини U_z (за рахунок використання набору букв/символів, або слів іншою мовою) дозволяє:

по-перше, створити пароль, ймовірність підбору якого серед певної множини паролів U_k буде мінімальною;

по-друге, збільшити кількість варіантів правила ускладнення *d* та кількість можливих комбінацій підбору, а також рівень невизначеності для зловмисника.

Четвертий розділ присвячено дослідженню вдосконаленого способу генерування ускладнених паролів, а також формуванню рекомендацій щодо його застосування на базі існуючих засобів захисту систем бездротового зв'язку стандарту IEEE 802.11. 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.

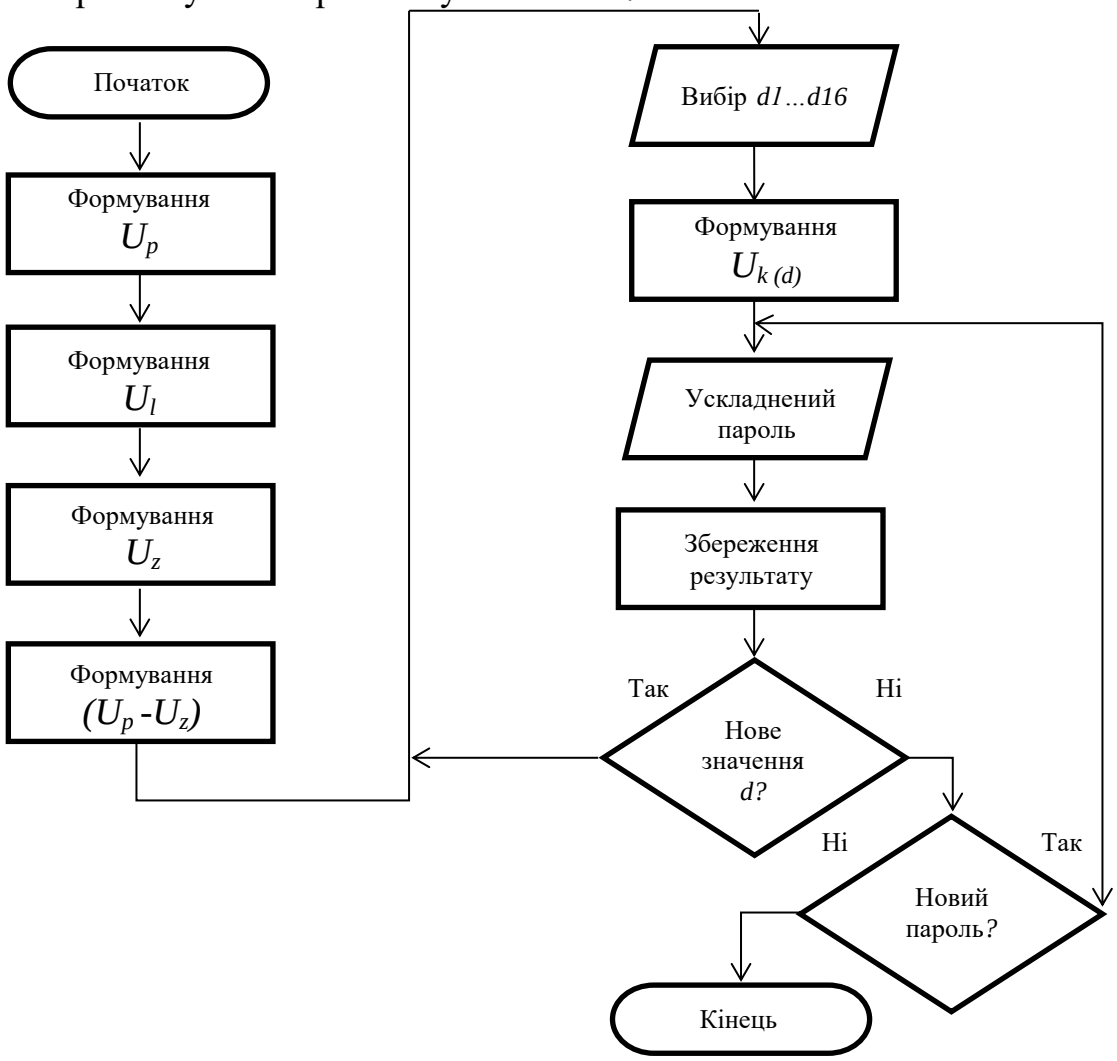

Рис. 5. Алгоритм генерування стійкого паролю зі змінним правилом ускладнення

На рис. 5 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 $6{,}03 \cdot 10^{21}$.

Відповідно до таблиці 6, 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 $U_{l(d)}$ наведено в таблиці 7.

Таблиця 7

Розрахунок кількості чисел, що можуть бути частиною паролю

$U_{l(d)}$	Розрахунок	Кількість комбінацій
1	$U_{10(d1)} = C_{10}^3 \cdot C_7^3 \cdot C_4^3$	16 800
2	$U_{10(d2)} = C_{10}^4 \cdot C_6^3 \cdot C_3^2$	12 600
3	$U_{10(d3)} = C_{10}^4 \cdot C_6^3 \cdot C_3^3$	4 200
4	$U_{10(d4)} = C_{10}^4 \cdot C_6^4 \cdot C_3^2$	3 150
5	$U_{10(d5)} = C_{10}^5 \cdot C_5^5$	252
6	$U_{10(d6)} = C_{10}^6 \cdot C_4^4$	210
7	$U_{10(d7)} = C_{10}^7 \cdot C_3^3$	120
8	$U_{10(d8)} = C_{10}^8 \cdot C_2^2$	45
	Всього	**37 377**

Підмножина U_z складається з $3{,}73 \cdot 10^4$ паролів, що відповідно до формули (17) 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 (19).

Таким чином, загальна кількість комбінацій можливих слів з 2 або 3 чисел від 2 до 8 цифр складає $3{,}73 \cdot 10^4$ (U_z), а кількість можливих комбінацій паролів без даних комбінації чисел, практично не зміниться, та становитиме $6{,}03 \cdot 10^{21}$ (U_p-U_z). За рахунок введення правила ускладнення d та вибірковому додаванню паролів, маємо кінцеве значення $2{,}25 \cdot 10^{26}$ (U_k).

Порівняння стійкості парольних множин до підбору розглянуті в таблиці 8.

Таблиця 8

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	$\mathbf{2{,}25 \cdot 10^{26}}$	$\mathbf{1{,}40 \cdot 10^{18}}$	$\mathbf{4{,}68 \cdot 10^{17}}$	$\mathbf{3{,}50 \cdot 10^{15}}$	$\mathbf{3{,}73 \cdot 10^4}$

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

Як видно з таблиці 8, для перебору випадкової комбінації з 63 символів ASCII знадобиться в $3{,}77 \cdot 10^{13}$ разів більше часу, ніж на підбір мобільного номеру, а для підбору паролю з множини сформованої ускладненим способом необхідно у $3{,}73 \cdot 10^{4}$ разів більше часу, ніж обраним у другому розділі базовим способом генерування паролів, що підтверджує правильність його вибору для вдосконалення.

Таким чином, за результатами четвертого розділу можливо зробити такі висновки:

по-перше, спосіб генерування ускладнених паролів в системах бездротового зв'язку з введенням змінного правила дозволяє зменшити витрати часу на створення паролю приблизно на 20%;

по-друге, для ускладненого паролю, що створений за вдосконаленим способом, отримано значне зниження ймовірності підбору паролю, оскільки на підбір потрібно у $3{,}73 \cdot 10^{4}$ разів більше часу, ніж для випадкової комбінації з 63 символів ASCII, або в $3{,}50 \cdot 10^{15}$ разів більше ніж для випадкового паролю з 8 символів;

по-третє, спосіб генерування ускладнених паролів може використовуватись не тільки як частина парольних політик, а і як додаткова складова для програмних та апаратних засобів захисту, облікових записів користувачів, а також в інших системах захисту інформації, де необхідне використання стійкого до підбору паролю.

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 ПЗ 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.

ВИСНОВКИ

У дисертації вирішено актуальне **наукове завдання**, що полягає *в створенні технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик*, яка за рахунок впровадження оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом та урахування можливості співпадіння з паролями системи словників, а також використання інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення) *дозволяє:*

- обрати серед множини існуючих способів генерування паролів спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;
- підвищити рівень захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $3{,}73 \cdot 10^{4}$ разів;
- зменшити витрати часу на створення паролю приблизно на 20%.

З цією метою в роботі, як результат:

1) проведено аналіз множини актуальних загроз та уразливостей системам бездротового зв'язку, а також варіанти формування та застосування парольних політик для забезпечення функціональної безпеки таких систем в умовах кібернетичних атак;

2) вперше розроблений метод обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку для забезпечення їх надійності і живучості в умовах кібернетичних атак, за рахунок вибору раціонального способу генерування паролів серед множини існуючих;

3) удосконалений спосіб генерування випадкових паролів для систем бездротового зв'язку, за показниками довжини та набору символів, з метою формування більш стійких до підбору паролів;

4) досліджено стан можливого злому (спроб несанкціонованого доступу) на прикладі систем бездротового зв'язку стандарту IEEE 802.11.

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

Таким чином, поставлене актуальне наукове завдання розв'язане у повному обсязі. Усі визначені часткові завдання вирішено, мету досліджень досягнуто.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Колективна монографія в іноземному науковому виданні:

1. Opirskyy Ivan. Use of near field communication technology for automated profile replication/ Opirskyy Ivan, Ivanchenko Ihor, **Platonenko Artem**, Skladannyi Pavlo, Roshchuk Mariia. // Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko-Biala, Poland.

Статті в іноземних наукових виданнях:

2. Odiyanenko H. V. Evaluation of parameters and compensation of noises in protected telecommunication systems / H. V. Odiyanenko, G. N. Rozorynov, **A. V. Platonenko**. // Научно-практический журнал Западно-Казахстанского аграрно-технического университета имени Жангир хана "Наука и образование". – 2014. – С. 91–94.

3. Одияненко Е. В. Синтез оптимальной структуры системы защиты информации / Е. В. Одияненко, Г. Н. Розоринов, **А. В. Платоненко**. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Часть I. – 2014. – С. 443–445.

Статті у наукових фахових виданнях України:

4. Розорінов Г. М. Захист інформаційних систем від потужних електромагнітних випромінювань / Г. М. Розорінов, **А. В. Платоненко**. // Сучасний захист інформації. – 2014. – №3. – С. 16–20.

5. Розоринов Г. Н. Пассивная оптическая сеть с кодовым разделением каналов / Г. Н. Розоринов, **А. В. Платоненко**. // Телекомунікаційні та інформаційні технології. – 2014. – №4. – С. 20–26.

6. **Платоненко А. В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

7. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, **А. В. Платоненко.** // Сучасний захист інформації. – 2017. – №2. – С. 90–94.

8. **Платоненко А. В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

9. Аносов А. О. Генерування унікального паролю зі змінним правилом ускладнення / А. О. Аносов, **А. В. Платоненко**. // Сучасний захист інформації. – 2017. – №3. – С. 82–86.

10. Бурячок В.Л. Генерування паролю для бездротових мереж з використанням змінного правила ускладнення/ В.Л. Бурячок, А. О. Аносов, **А.В Платоненко**. // Захист інформації. – 2019. – Том 21, №1. – С. 52–59.

11. Бурячок В.Л. Вибір раціонального способу генерування паролів серед множини існуючих / В.Л. Бурячок, **А.В Платоненко**, О.В. Семко. // Безпека інформації. – 2019. – Том 25, № 1. – С. 59–64.

Публікації у наукометричних базах Scopus і Web of Science:

12. Vladymyrenko Maksym. Analysis of implementation results of the distributed access control system. / Maksym Vladymyrenko, Sokolov Volodymyr, Buriachok Volodymyr, **Platonenko Artem**. // Preprint. PIC S&T`2019 IEEE conference, Kyiv.

Тези наукових доповідей:

13. **Платоненко А.В.** Захист інформації у безпроводових мережах WI-FI./ Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.

14. **Платоненко А.В.** Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. / Платоненко А.В. // Науково-технічна конференція «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.34-35.

15. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для пристроїв у корпоративних мережах. Матеріали Міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.128.

16. **Платоненко А.В.** Сучасні загрози інформаційної безпеки для державних та приватних установ України. / Платоненко А.В. // ІІ Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» – Київ: ДУТ, 2015 – С.137-138.

17. **Платоненко А.В.** Сучасні загрози інформаційної безпеки та засоби захисту від них. / Платоненко А.В. // Міжнародна науково-технічна конференція студентства та молоді «Світ телекомунікації та інформатизації» – Київ: ДУТ, 2015 – С.159-160.

18. **Платоненко А.В.** Актуальні загрози інформаційної безпеки сучасних мобільних пристроїв у мережах нового покоління. / Платоненко А.В. // ІІ Міжнародна науково-практична конференція «Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G та 5G» – Київ: ДУТ, 2016 – С.182-183.

19. **Платоненко А.В.** Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв в Україні. / Платоненко А.В. // ІІІ Міжнародна науково-технічна конференція студентства та молоді» – Київ: ДУТ, 2016 – С.134-136.

20. **Платоненко А.В**. Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // 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.

АНОТАЦІЯ

Платоненко А. В. Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, Київ, 2019.

Дисертація присвячена розв'язанню актуального наукового завдання, що полягає в розробленні технології забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик.

Об'єкт дослідження – процес забезпечення функціональної безпеки систем бездротового зв'язку. *Предмет дослідження* – інформаційна технологія забезпечення функціональної безпеки систем бездротового зв'язку в умовах загроз і обмежень, визначених специфічними умовами функціонування таких систем.

Новизна роботи полягає в подальшому розвитку теоретичних і практичних методів та моделей забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик, за рахунок:

- розробки та обґрунтування рішення на вдосконалення парольних політик в системах бездротового зв'язку, на відміну від подібних, шляхом оцінки ступеня близькості між базовим способом генерування паролів і кожним способом-аналогом, що дозволяє на відміну від подібних, серед множини існуючих способів генерування паролів обрати спосіб, найбільш раціональний з точки зору його вдосконалення та забезпечити функціональну безпеку систем бездротового зв'язку в умовах впливу кібернетичних атак;

- удосконалення способу генерування випадкових паролів для систем бездротового зв'язку, завдяки урахуванню можливості співпадіння з паролями системи словників та використанню інтегрованого підходу для генерування більш стійких паролів за показниками довжини та набору символів (обраних за правилом комбінації з введенням певного ускладнення), що забезпечує, порівняно з аналогами, підвищення рівня захищеності систем бездротового зв'язку стандарту IEEE 802.11 від можливого злому (спроб несанкціонованого доступу) в $3{,}73 \cdot 10^4$ разів.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв, пароль, генерування паролів, стійкі паролі, парольні політики.

ANNOTATION

A. Platonenko. Techodology of providing functional security for wireless communication systems based on the improvement of the password policies. - On the manuscript basis. Qualification scientific work on the rights of manuscript.

The technique of ensuring the functional safety of wireless communication systems based on the analysis of password policies

The dissertation is for the degree of a candidate of technical sciences in specialty 05.13.06 - Information technologies. - Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2019.

The dissertation is devoted to the solution of the actual scientific problem, which consists in providing functional security for wireless communication systems on the basis of improvement passwords corporate policies.

Object of study is the process of ensuring the functional security of wireless communication systems. The subject of the research is information technology for ensuring the functional security of wireless systems in the conditions of threats and restrictions determined by the specific conditions of such systems operation.

The novelty of the work lies in the further development of theoretical and practical methods and models for ensuring the functional security of wireless systems based on the improvement of password policies through:

- developing and validating solutions to improve password policies in wireless systems, as opposed to similar ones, by assessing the degree of closeness between the basic method of password generation and each unlike any of the many existing password-generating methods, choose the method that is most streamlined in terms of improving it and ensure the functional security of wireless systems in the face of cyber-attack;

- improving the method of generating random passwords for wireless systems by taking into account the ability to match the passwords of the vocabulary system and using an integrated approach to generate more stable passwords by length and character set (chosen by the combination rule with some complication), compared to its counterparts, the IEEE 802.11 wireless security system is increased by $3.73 \cdot 10^4$ times from possible hacking (unauthorized access attempts).

Keywords: information security, threats of information security, wireless networks, protection of networks from unauthorized access, protection of mobile devices, password, password generation, stable passwords, password policies

Підписано до друку 16.09.2019. Папір офсетний. Ум.-др. арк. 0,9.
Формат 60×90/16. Наклад 110 прим. Замовлення №1560.

Суб'єкт видавничої діяльності занесено до державного реєстру №620049 13.10.2008,
ПРІНТЦЕНТР, м.Київ, вул. Політехнічна, 16