УДК 044.05

[0000-0003-2007-9943] **І. В. Миронець,** *к.т.н., доцент,*
e-mail: irenmir30@gmail.com
В. М. Пономаренко, *магістр*
e-mail: vladponomarenko8@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18000, Україна

АВТОМАТИЗОВАНА СИСТЕМА ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Захист даних є необхідним атрибутом кожної людини, а захист персональних даних на смартфоні є найголовнішим, оскільки саме в них ми найбільше зберігаємо персональну інформацію. В роботі наведено реалізацію та обґрунтування актуальності використання блокування Android-додатків, що являє собою удосконалену версію звичайного використання паролей, організовуючи зміну способу деталей введення. Тобто замість того, щоб користувач щоразу бачив звичне для нього поле введення, йому буде надано можливість ввести комбінацію зі спеціально створеної таблиці, порядок елементів якої буде щоразу змінюватися, тим самим не даючи можливості легкого відтворення паролю. Надійність використання нового методу аутентифікації користувача підтверджено експериментальними дослідженнями.

Ключові слова: *пароль, Android, аутентифікація, графічний пароль, смартфон, блокування.*

Вступ. Використання смартфонів стало одним із найважливіших атрибутів сучасності, без якого неможливо уявити життя кожної людини. Нині найбільш поширеною операційною системою для мобільних гаджетів є ОС Android. Кожного дня – вдома, на роботі тощо – ми використовуємо мобільні додатки різного призначення та сфери обслуговування, і, як правило, більшість із них використовує для своєї авторизації та роботи персональну, конфіденційну інформацію. Не всі програмні продукти мають вбудовану функцію аутентифікації користувача, і тоді на допомогу приходять програми-помічники, які здатні її забезпечити. Однак надійність паролів, які відповідають за безпеку, інколи є досить низькою, тобто вони не завжди можуть забезпечити належну конфіденційність вашої персональної інформації [1, 2].

Як захист найчастіше використовуються вбудовані механізми аутентифікації користувача, такі як розблокування за допомогою PIN-коду, пароля, відбитка пальця або нової технології Face ID.

Face ID – це результат об’єднання найбільш передових апаратних і програмних компонентів Apple. Камера TrueDepth захоплює дані особи, проектуючи на неї і аналізуючи більше 30 000 невидимих точок. Таким чином пристрій визначає детальну структурну карту особи, а також її зображення в інфрачервоному спектрі. Фрагмент нейронного ядра мікропроцесорів A11, A12 Bionic, A12X Bionic і A13 Bionic, захищений модулем Secure Enclave, перетворює карту глибини та інфрачервоне зображення в математичне уявлення, яке порівнюється із зареєстрованими даними особи [1].

Проте аналіз літературних джерел [3-6] показав, що на сьогоднішній день дані більше захищені від несанкціонованого доступу за допомогою використання комп’ютера, аніж від користувачів.

Метою роботи є розробити програмний додаток захисту конфіденційної інформації користувачів для операційної системи Android та реалізувати метод двофакторної аутентифікації для захисту конфіденційної інформації від несанкціонованого доступу.

Опис об’єкта і методу дослідження. Об’єктом дослідження є процес захисту користувача від так званого the shoulder surfing (підглядання через плече). Мається на увазі, що у момент аутентифікації за користувачем може знаходитися людина, яка може підглянути пароль і запам’ятати його.

Предметом дослідження є програмна розробка, яка реалізує метод двофакторної аутентифікації, що не потребує підключення до мобільної мережі або Інтернету, і є складною для миттєвого запам’ятовування.

DOI: 10.24025/2306-4412.1.2020.185308

Найчастіше користувачі смартфонів, і не тільки, використовують один і той же пароль для доступу до різних сайтів, аутентифікації користувача на пристрої, рідше використовують два різні паролі, і дуже рідко використовують різні паролі для різних систем аутентифікації [2]. Крім цього, користувач може добровільно, не задумуючись про свої персональні дані, розблокувати телефон і віддати, наприклад, своїй дитині, другу, який попросив перевірити свою пошту, тому що його телефон розрядився, або навіть перехожому, який попросив зателефонувати. Після цього найчастіше у людини є повний доступ до даних, і, якщо є злі наміри, вона може використати у своїх цілях дані власника смартфону [3]. Навіть, якщо просто дати погратися дитині, вона може випадково видалити фотографії, копії яких знаходяться на вашому девайсі.

Є багато різноманітних програм для вирішення цього питання, вони блокують доступ до вибраних додатків і просять щоразу при вході в ту чи іншу завчасно вибрану програму аутентифікувати користувача.

Програми для блокування додатків можуть з легкістю заблокувати всі програми для ОС Android, такі як:

– соціальні додатки: Facebook, Messenger, Vine, Twitter, Instagram тощо;

– системні програми: контакти, SMS, галерею, електронну пошту, відео тощо;

– програми електронних гаманців: Android Pay, Samsung Pay, Paypal тощо;

– будь-які інші сторонні додатки, незалежно від їх призначення.

Однак у перелічених вище додатках спосіб аутентифікації добре захищений від комп'ютерного перехоплення або перебору, але не від людини, оскільки в таких додатках найуразливішою частиною є пароль.

Так, можна встановити аутентифікацію за допомогою технологій Touch ID або Face ID, але, крім цього, все ж встановлюється звичайний текстовий пароль або графічний пароль, або пін-код, які користувач смартфону найчастіше використовує для блокування самого телефону, тим самим ці паролі є ідентичними і технології Touch ID та Face ID втрачають свій сенс.

До створення нового методу аутентифікації спонукав реальний життєвий випадок – перебуваючи у громадському транспорті, троє студентів помітили, що на смартфоні їхнього друга встановлена Face ID аутентифікація. Вони вирішили перевірити, як вона працює з різними варіантами розблокування: з заплющеними очима, з прижмуреними та з різних ракурсів. Так вони випробовували секунд 25, в результаті чого, коли власнику девайса набридло тестувати, він захотів його просто останній раз розблокувати і вимкнути, але на цей раз Face ID не спрацював. Не роздумуючи ні секунди, він вибрав ручний ввід графічного пароля та намалював його. Пароль був дуже легким для запам'ятовування, тим самим це доводить той факт, що неважливо, яку передову технологію використовувати, – вразливість буде наявною.

Тому було прийнято рішення створити таку аутентифікацію, яка буде складною для миттєвого запам'ятовування, при цьому вона буде заплутувати користувача, який захотів отримати несанкціонований доступ до персональних даних.

Проблема підглядання через плече (the shoulder surfing problem), як випливає з назви, – це спостерігання за тим, як людина вводить на гаджет певну інформацію, зазвичай з метою заволодіти персональними даними. Приклади включають спостереження за клавіатурою, коли людина вводить свій пароль, PIN-код або переглядає особисту інформацію.

Через свій графічний характер майже всі графічні схеми паролів дуже вразливі для підглядання через плече. Більшість існуючих схем просто обходять проблему, стверджуючи, що графічні паролі повинні використовуватися тільки з кишеньковими пристроями або робочими станціями, налаштованими таким чином, щоб тільки одна людина могла бачити екран під час входу в систему.

Однак зазвичай можна гарантувати, що під час входу в систему значення графічних паролів як альтернативи буквено-цифрових паролів дещо зменшується, якщо їх можна використовувати тільки в середовищах, налаштованих для запобігання підгляданню через плече [4].

У процесі дослідження було проведено аналіз існуючих систем аутентифікації користувача.

Ще до появи смартфонів користувачі персональних комп'ютерів винайшли методи створення псевдовипадкового пароля. Найпростіший із них створюється наступним чином: потрібно взяти слово і виконати з ним

DOI: 10.24025/2306-4412.1.2020.185308

певні дії. Розглянемо, наприклад, слово «Smartphone». Користувачі можуть за допомогою цього слова створити такі паролі: «enohptramS» (змінити напрямок написання, використавши зворотний варіант), «SmArTpHoNe» (верхні і нижні регістри, що чергуються), «phoneSmart» (перетасувати склади), «S1a2t4h8n16» (поєднати цифри і літери) тощо.

Проте надмірне ускладнення пароля призводить до проблем із його запам'ятовуванням самим користувачем.

Користувачі, які мають на своєму смартфоні клавіатуру з кириличним чи латинським шрифтом, можуть використовувати паролі рідною мовою з посимвольною заміною на латинські символи. Наприклад, пароль «Веселка» латинським шрифтом буде «Dtctkrf».

Цей спосіб дещо збільшує захищеність пароля, але він фактично безпорадний проти атаки з використанням розширеного словника, який має спеціальні правила транслітерації. Адже пари букв «кирилиця/латинь» на клавіатурах однотипні: «й/q», «я/z» тощо. Отже, цей метод створення пароля не становитиме великих проблем для злому у процесі підбору слова із словника зі зміною алфавіту.

Практика застосування складних паролів користувачами свідчить про те, що останні, як правило, або просто забувають такі паролі, або прагнуть їх зберегти «в пам'ять» записника, настільного календаря, мобільного телефону, інших предметів, які користувач найчастіше використовує. Зрозуміло, що захищеність паролів після таких записів зводиться нанівець [5].

Аналіз текстових паролів можна спростити, якщо передбачити, що паролі – це послідовність знаків, яка складається з рядкових літер (їх 26), прописних літер (ще 26), латинського алфавіту, цифр (10) і символів (10).

У простому випадку, коли пароль складається лише з n строкових літер, можливі $26n$ перестановок. Якщо пароль може мати довжину від 1 до n знаків, кількість перестановок буде наступною: пароль, що складається з восьми літер, має 208 млрд. можливих комбінацій, що для більшості користувачів здається достатньою кількістю [6].

Одним із найпростіших способів аутентифікації є PIN-код. Зазвичай він складається лише з чотирьох розрядів (із десятьма незалежними можливими значеннями в кожному з них), тому аналіз кількості унікальних комбінацій PIN-коду є дуже простим. Такий PIN-код може мати 10 000 унікальних комбінацій.

Крім цього, потрібно обрати найоптимальніше мінімальне число, яке б людина не змогла запам'ятати відразу.

У статті американського психолога Джорджа Міллера «Магічне число сім, плюс або мінус два: деякі обмеження нашої можливості для обробки інформації» написано, що людина може запам'ятати в середньому 7 (±2) символів [7].

Нельсон Коуан у своїй статті «Магічне число 4 у короткостроковій пам'яті: перегляд розумових здібностей до пам'яті» відзначив ряд інших меж пізнання, які вказують на «магічне число чотири» і які відрізняються від дослідження Джорджа Міллера.

Нельсон відзначав ще один процес, який, здається, обмежений приблизно чотирма елементами, – це субітизація (subitizing) – можливість моментально визначати невелику кількість об'єктів, які потрапляють в поле зору людини. Коли за короткий час проводиться огляд кількості об'єктів, їх кількість можна визначити дуже швидко, з першого погляду, коли число не перевищує межу субітизації, що становить приблизно чотири об'єкти [8].

Після аналізу праць Джорджа Міллера та Нельсона Коуана було прийнято рішення при виконанні власного дослідження використовувати мінімум 10 символів для встановлення коду.

Чому саме 10 символів, а не 11 чи 12? Оскільки людина може запам'ятовувати в середньому 7 (±2) символів, а у режимі субітизації – 4 символи, було вирішено використовувати найменше найбільше число, яке буде складним для миттєвого запам'ятовування. Це може видатися трохи незручним на перших етапах, але, якщо користувач, потренувавшись, запам'ятає свою комбінацію чисел, в подальшому введення пароля буде нескладним.

На першому й останньому етапах аутентифікації ідею використання таблиці було вибрано неспроста. Справа в тому, що в таблиці представлені цифри різних розмірів, а на звичайній клавіатурі для OS Android усі цифри однакового розміру. Тобто, навіть просто обравши як пароль послідовність із цифр меншого розміру, користувач збільшує надійність від випадкового запам'ятовування.

На рисунку 1 зображено звичайну таблицю з цифрами різних розмірів.

DOI: 10.24025/2306-4412.1.2020.185308

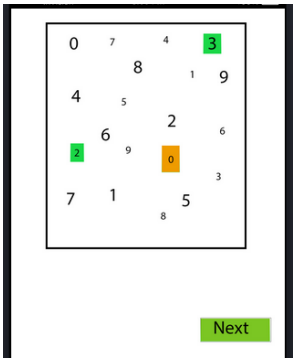

Рисунок 1 – Перша таблиця для аутентифікації

Можна поставити питання: а де ж складність у запам'ятовуванні? Крім того, що кожного разу цифри змінюють своє місцеположення, при використанні більше одного разу вони щоразу змінюють свій колір, тим самим ускладнюючи запам'ятовування, тому що не всі люди мають хороший спектральний діапазон кольорів, а це говорить про те, що звичайна зміна кольору уже може збити з пантелику. Додайте до цього ще постійну зміну елементів у таблиці. Цей метод було названо «Подвійна плутанина».

На рисунку 2 можна побачити звичайний повзунок (slider), який усі бачили в різноманітних відеоплеєрах та музичних плеєрах, коли користувач може пересувати повзунок пальцем на екрані. Повзунок також можна рухати за допомогою клавіш-стрілок, якщо вони є на клавіатурі. Повзунки можуть бути багатьох видів: круглі, наполовину круглі, горизонтальні, вертикальні, і навіть із емодзі-знаками.

На другому етапі аутентифікації використовується вертикальний повзунок. Іноді, навіть знаючи значення, яке необхідно ввести, це буває надзвичайно важко зробити.

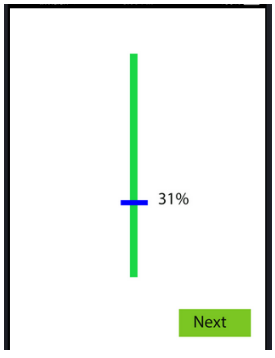

Рисунок 2 – Другий етап аутентифікації

Зазвичай це пов'язано з тим, що екран користувача чимось забруднений або, як буває у деяких випадках, просто великі пальці. Погодьтеся, такого способу аутентифікації ви не зустрічали в жодній програмі, принаймні за весь час користування смартфоном жодного разу не було знайдено.

Діапазон значень можна вибрати довільно, але цей діапазон не повинен бути меншим за 50 % від усього повзунка. Це значення вибрано з міркувань безпеки.

Нову революцію в безпеці паролів зробив Грег Блондер (Greg Blonder), розробивши графічні схеми паролів [9].

Графічний пароль є однією із систем аутентифікації користувача. Він відрізняється від інших систем тим, що потрібно з'єднати послідовно набір точок на довільному зображенні або ж на певно обраному наборі точок, такі, які зазвичай використовують за замовчуванням для аутентифікації, наприклад на Android системах.

Існує два типи графічних парольних технік: на основі розпізнавання та на основі відгуку. У режимі розпізнавання користувачу надані різні зображення, і користувач повинен розпізнати потрібні зображення в правильній послідовності. На основі відгуку користувач повинен відтворити те, що було вибрано під час авторизації.

Одними з технік на основі розпізнавання є техніка Draw-a-Secret (DAS) і техніка підпису.

Техніка Draw-a-Secret – користувач може намалювати картинку на двовимірній сітці розміром $n \times n$. Кожний елемент позначений дискретними прямокутними координатами (x, y).

Значення сенсорних сіток зберігаються в порядку малювання. Для аутентифікації користувач повинен перемалювати ту ж картинку, торкаючись тих же координат сітки. При цьому користувачі можуть малювати пароль стільки, скільки побажають.

Простір пароля набагато кращий, ніж текстовий пароль [10]. Обмеження – користувачі можуть забути свій порядок штрихів, тому іноді легше запам'ятати текстовий пароль, ніж пароль DAS. Також користувачі іноді вибирають слабкий пароль, який є вразливим для атаки з використанням графічного словника і повторної атаки.

Техніка підпису – користувач аутентифікується шляхом малювання підпису за до-

DOI: 10.24025/2306-4412.1.2020.185308

помогою миші. Немає необхідності запам'ятовувати підпис, а також його важко підробити, однак важко намалювати підпис в тому ж периметрі, що і під час реєстрації.

Одним із рішень цієї проблеми є використання ручки введення, а з появою планшетів – можна підписуватись за допомогою пальця [11].

Найчастіше ця техніка використовується у банках, наприклад, коли відкриваєте кредитний рахунок і вам пропонують зробити підпис на планшеті.

При спробі виконання аутентифікації за допомогою графічного пароля введені на екрані маніпуляції порівнюються з еталонним зразком, збереженим при налаштуванні графічного пароля. При цьому аналізується різниця між кожним рухом і автоматично приймається рішення про успішність перевірки достовірності на основі сумісності з еталоном або виявленої кількості помилок. Якщо маніпуляція неправильна (наприклад, має бути лінія, а замість неї вводиться коло), перевірка достовірності ключа буде заблокована. Якщо ж види таких рухів, їх порядок введення і напрями збігаються, то система аналізує, наскільки вони відповідають еталонним, і надає доступ користувачу до системи.

На рисунку 3 зображено останній етап аутентифікації – введення ключа-слова, яке також може зайняти певний час, що дасть змогу власнику девайса вчасно звернути на це увагу та забрати його, аби не трапилося незворотних дій.

Здебільшого ця аутентифікація схожа на введення графічного ключа. Але відмінність полягає в тому, що тут потрібно вибрати слово. Недолік звичайного графічного ключа – в тому, що це просто набір точок, зв'язаних між собою.

Рисунок 3 – Введення ключа-слова

Опис результатів. В експериментальному тестуванні взяли участь 17 добровольців. Це були особи віком від 14 до 28 років. За даними дослідження було виявлено, що при використанні 8-числового пароля та слова 95 % учасників було складно відразу запам'ятати та відтворити паролі і лише 5 % змогли відразу запам'ятати введені паролі.

Для того щоб випадкова людина змогла запам'ятати паролі, 6 % знадобилося від 5 до 8 спроб, іншим учасникам навіть після 10 повторювань було важко відтворити аутентифікацію.

Висновки. В статті наведено реалізацію блокування Android-додатків, яка являє собою удосконалену версію звичного використання паролей, використовуючи зміну способу деталей введення. Тобто, замість того, щоб користувач щоразу бачив звичайне для нього поле введення, йому буде надано можливість ввести комбінацію зі спеціально створеної таблиці, порядок елементів якої буде щоразу змінюватися, тим самим не даючи можливості легкого відтворення пароля.

За допомогою реалізації цього методу блокування додатків можна бути впевненим у тому, що будь-хто з вашого оточення або просто випадкові люди, які забажали дізнатися вашу конфіденційну інформацію, доки ви ненадовго відійшли від вашого смартфону, не зможуть відразу отримати доступ простим вводом легкого пароля. Крім цього, проведене тестування надало обґрунтовані результати щодо надійності розробленого методу аутентифікації.

Список використаних джерел

[1] Сведения о передовой технологии Face ID. [Электронный ресурс]. Режим доступа: https://support.apple.com/ru-ru/HT208108.

[2] Моделі системи безпеки ОС ANDROID. 2018. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.

[3] Искусство защиты и взлома информации. 2004. [Электронный ресурс]. Режим доступа: https://www.e-reading.club/ bookreader.php/133669/Sklyarov_-_Iskusstvo_zashchity_i_vzloma_informacii.pdf

[4] L. Sobrado, and J. Birget, "Graphical passwords", Department of Computer Science,

DOI: 10.24025/2306-4412.1.2020.185308

Rutgers University, 2003. [Online]. Available: https://rutgersscholar.libraries.rutgers.edu/ volume04/sobrbirg/sobrbirg.htm.

[5] Є. Завальнюк, "Простота і захищеність графічного пароля для користувача", *Вісник Національного банку України*, № 6, с. 37-41, 2013. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/ Vnbu_2013_6_23.

[6] В. Безмалый, и Д. Нефедов, "Применение графического пароля в Windows 8", *Windows IT Pro/RE*, № 10, с. 45-47, 2012.

[7] G. A. Miller, "The magical number seven, plus or minus two some limits on our capacity for processing information", *Psychological Review*, 1956. [Online]. Available: http://www2.psych.utoronto.ca/users/peterson /psy430s2001/Miller%20GA%20Magical%20Seven%20Psych%20Review%201955.pdf.

[8] N. Cowan, "The magical number 4 in short-term memory: a reconsideration of mental storage capacity", *Behavioral and Brain Sciences*, 2001. [Online]. Available: https://www.researchgate.net/publication/11830840_The_Magical_Number_4_in_Short-Term_Memory_A_Reconsideration_of_Mental_Storage_Capacity.

[9] G. E. Blonder, "Graphical password", *U.S. Patent 5 559 961*, Sept. 24, 1996.

[10] Ian Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords", in *Proc. Eighth USENIX Security Symposium.* Aug. 23-26, 1999. USENIX Association 1-14, 1999.

[11] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse", in *Third Australasian Conf. on Information Security and Privacy (ACISP):* Springer-Verlag lecture notes in comp. science, (1438), 1998, pp. 403-441.

References

[1] Information on the advanced technology Face ID. [Online]. Available: https://support.apple.com/ru-ru/HT208108.

[2] The models of ANDROID security system. 2018. [Online]. Available: https://www.researchgate.net/publication/328775065_MODELI_SISTEMI_BEZPEKI_OS_ANDROID.

[3] The art of protecting and hacking information. 2004. [Online]. Available: https://www.e-reading.club/bookreader.php/133669/Sklyarov_-_Iskusstvo_zashchity_i_vzloma_informacii.pdf.

[4] L. Sobrado, and J. Birget, "Graphical passwords", Department of Computer Science, Rutgers University, 2003. [Online]. Available: https://rutgersscholar.libraries.rutgers.edu/ volume04/sobrbirg/sobrbirg.htm.

[5] E. Zavalnyuk, "Simplicity and security of the graphic password for the user", *Visnyk Natsionalnoho banku Ukrayiny*, no. 6, pp. 37-41, 2013. [Online]. Available: http://nbuv.gov.ua/UJRN/Vnbu_2013_6_23.

[6] V. Bezmalyy, and D. Nefedov, "Application of graphic password in Windows 8", *Windows IT Pro/RE*, no. 10, pp. 45-47, 2012 [in Russian].

[7] G. A. Miller, "The magical number seven, plus or minus two some limits on our capacity for processing information", *Psychological Review*, 1956. [Online]. Available: http://www2.psych.utoronto.ca/users/peterson /psy430s2001/Miller%20GA%20Magical%20Seven%20Psych%20Review%201955.pdf.

[8] N. Cowan, "The magical number 4 in short-term memory: a reconsideration of mental storage capacity", *Behavioral and Brain Sciences*, 2001. [Online]. Available: https://www.researchgate.net/publication/11830840_The_Magical_Number_4_in_Short-Term_Memory_A_Reconsideration_of_Mental_Storage_Capacity.

[9] G. E. Blonder, "Graphical password", *U.S. Patent 5 559 961*, Sept. 24, 1996.

[10] Ian Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords", in *Proc. Eighth USENIX Security Symposium.* Aug. 23-26, 1999. USENIX Association 1-14, 1999.

[11] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Third Australasian Conf. on Information Security and Privacy (ACISP):* Springer-Verlag lecture notes in comp. science, (1438), 1998, pp. 403-441.

DOI: 10.24025/2306-4412.1.2020.185308

I. V. Myronets, *Ph. D., associate professor,*
e-mail: irenmir30@gmail.com
V. M. Ponomarenko, *master*
e-mail: vladponomarenko8@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy,18006, Ukraine

AUTOMATED SYSTEM OF SOFTWARE PROTECTION FOR ANDROID OPERATION SYSTEM

The article pays the attention to the authentication of data on mobile devices running the Android operation system. We use smartphones and applications which are installed on them, every day. We can use personal information in some applications, that we do not wish to disclose. Such built-in user authentication mechanisms as unlocking with a PIN code, password, fingerprint, or with the new Face ID technology are most commonly used.

Most often, smartphone users, and not only use the same password to access different sites, authenticate a user to the device, rarely they use two different passwords, and very rarely use different passwords for different authentication systems. These systems are well protected from computer hacking, but not from humans. What does it mean? At the time of authentication, another person may be present, and he can look at the password (it's called the shoulder surfing) and remember it after that. That's why it has been decided to create an authentication that would be difficult to remember and would confuse the user who wanted to gain unauthorized access to personal data.

The article introduces the implementation of Android application lock, which is an improved version of the usual use of passwords, using a change in the way details are introduced. That is, instead of the user seeing the usual input field every time, the user will be able to enter a combination from a specially created table, whose order of elements will be changed every time, thus not allowing easy password reproduction.

Using this method of blocking apps, you can be sure that nobody in your environment, or just random people who wanted to know your sensitive information when you have just left your smartphone, would be able to access by simple typing of easy password right away. In addition, the testing has provided valid results regarding the reliability of the developed authentication method.

Keywords: *password, Android, authentication, graphic password, smartphone, lock.*

Стаття надійшла 28.11.2019
Прийнято 26.12.2019

DOI: 10.24025/2306-4412.1.2020.185308