УДК 004.056.5

Горбенко О. В.[1] (0000-0001-5809-6699)
Горбенко Ю. Л., канд. психол. наук, доцент[2] (0000-0002-1555-9216)
Горбенко А. Ю.[3] (0000-0002-6122-9779)
Сівоха О. М.[4] (0000-0002-8076-7425)

[1] – Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ;
[2] – Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава;
[3] – Національний університет оборони України імені Івана Черняховського, Київ;
[4] – Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ

Захист інформаційних систем за допомогою використання методів автентифікації

Резюме. У статті проаналізовано існуючі методи автентифікації користувачів інформаційних систем, визначено найбільш ефективний метод та запропоновано перспективний напрям розвитку методів автентифікації, використовуючи тест Люшера.

Ключові слова: автентифікація; інформаційні системи; тест Люшера.

Постановка проблеми. Кожна установа та підприємство у своєму розпорядженні мають комунікаційні та технологічні системи, захист яких є одним з важливих завдань для підтримання їх в ефективному та працездатному стані. Кожна така система має своє функціональне призначення, яке робить комфортним та безпечним життя суспільства. Виведення з ладу однієї із систем може призвести до колапсу: втрата навігації авіаційних сполучень або втрата контролю над банківською системою. Таких ризиків можуть зазнавати і об'єкти критичної інформаційної інфраструктури Міністерства оборони України, зважаючи ще й на російсько-український конфлікт на сході України, який веде за собою можливість завдати шкоду обороноздатності України через виведення з ладу або отримання повного чи часткового контролю над об'єктами критичної інформаційної інфраструктури Міністерства оборони України для демонстрації перед світовою спільнотою своєї переваги над Збройними Силами України та їх нездатність протистояти російським кібератакам на комунікаційні та технологічні системи.

Для недопущення неправомірних дій над інформаційними системами Збройних Сил України, заволодіння інформацією, що міститься на серверах або комп'ютерах та взагалі недопущення до приміщень сторонніх осіб, в таких установах мають використовуватися системи з процедурами автентифікації та ідентифікації користувачів.

Аналіз останніх досліджень і публікацій. Дослідженню питання автентифікації присвятили свої праці багато науковців у сфері інформаційної безпеки та захисту інформації, а саме: Я. Кісь, В. Теслюк, Н. Кошева, Н. Мазниченко та ін.

Більшість авторів у своїх працях вивчають питання застосування однофакторної та багатофакторної автентифікації, їх переваги та недоліки, а також надають поради щодо об'єктивної оцінки цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/автентифікації, яке обирається для захисту зазначеної інформації [1]. Інші автори детальніше зупиняються на конкретному методі автентифікації користувачів, найчастіше це є біометричний метод, дослідники якого вивчають його надійність використання та пріоритетність застосувань в інформаційних системах [2].

Актуальність та важливість вибору найефективнішого методу автентифікації є суттєвою з огляду на те, що все частіше метою злочинців та кіберзлочинців є об'єкти критичної інформаційної інфраструктури, втручання у роботу яких може завдати непоправних негативних наслідків як для Збройних Сил України, так і для держави загалом.

Мета статті – аналіз існуючих методів автентифікації користувачів інформаційних систем та визначення перспективного напряму розвитку методів автентифікації, використовуючи тест Люшера.

Виклад основного матеріалу. За останні два десятиліття в світі як серед приватних та державних підприємств, так і серед людей взагалі стали поширюватися інформаційні технології за допомогою

використання комп'ютерів, планшетів, смартфонів тощо. Життя людей спростилось унаслідок використання Інтернету: на сьогодні не обов'язково виходити з дому для купівлі товару, оплати послуг, отримання будь-якої інформації або замовлення квитків чи довідок. Наразі можна отримати "розумний будинок", що дасть змогу керувати з персонального гаджету системами опалення, освітлення та сигналізації, теплою підлогою, розетками та іншими комунікаціями. Також керувати за допомогою особистого гаджету дають змогу нещодавно набуті поширення дверні замки для квартир, які містять декілька методів автентифікації користувачів: пароль, IC-карту (mifare), електронний ключ (eKey) та відбиток пальця. Зазначені методи можуть використовуватися як для захисту приміщень, так і для захисту інформації, що зберігається на комп'ютерах чи серверах. Не дарма визначний британський державний та політичний діяч Бенджамін Дізраелі за час свого життя розглядав інформацію, як шлях до успіху: "Як правило, найбільшого успіху досягає той, хто має в своєму розпорядженні кращу інформацію" [3]. Отже, можна з впевненістю сказати, що заволодіння тією чи іншою інформацією, а тим паче інформацією конкурента, може заподіяти шкоди компаніям, державним установам та державам.

Розуміючи важливість захисту інформації в теперішньому цифровому світі, в Україні в 2019 році було створено Міністерство цифрової трансформації України. Відповідно до пункту 4 "Положення про Міністерство цифрової трансформації України", затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 року № 856, Міністерство цифрової трансформації України "здійснює заходи щодо створення та забезпечення функціонування: інтегрованої системи електронної ідентифікації" [4]. Система електронної ідентифікації – це електронний майданчик, який об'єднує всіх надавачів послуг електронної ідентифікації, а саме: за електронним підписом, Bank ID, Mobile ID, тим самим гарантуючи її користувачам безпеку та захист персональних даних. Функціональні можливості зазначеної системи забезпечують "електронну ідентифікацію та автентифікацію користувачів та суб'єктів взаємодії, створення та перевірку кваліфікованого електронного підпису" [5].

Відповідно до НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу", затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22: під ідентифікацією (identification) розуміється "процедура присвоєння ідентифікатора об'єкта комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором; впізнання" [6]; під *автентифікацією* (authentication) розуміється "процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності" [6]. Об'єктами ідентифікації можуть бути людина, носії інформації, технічні засоби та документи. Отже, під час санкціонованого доступу до інформаційної системи користувач ідентифікує себе, а система зі свого боку перевіряє приналежність зазначеного користувача до ідентифікатора – проводить автентифікацію, за результатом перевірки якого відбувається допуск до потрібної інформаційної системи або відмова.

На сьогодні, залежно від кількості використовуваємих методів автентифікації користувачів, існують однофакторна та багатофакторна автентифікації.

Однофакторна автентифікація є найпростішою формою методу автентифікації, яка включає у себе лише один з перелічених нижче методів автентифікації:

парольний (логічний), під час якого можуть використовуватися паролі або ключові фрази;

ідентифікаційний – засновується на використанні унікального предмета, такого як магнітна карта, тарт-карта, штрих-кодова карта, токени, криптографічний сертифікат тощо;

біометричний – засновується на унікальних характеристиках людини, таких як голос, обличчя, відбитки пальців, геометрії руки, малюнок райдужної оболонки ока або сітчатки ока;

за географічним розташуванням – заснований на розташуванні виходу до мережі Інтернет та за допомогою GPS.

Багатофакторна автентифікація комбінує два або більше однофакторних методи автентифікації користувачів, що дає змогу ускладнити несанкціонований доступ до інформаційної системи: магнітна карта та PIN-код, пароль та клавіатурний почерк.

1. *Парольна (логічна) автентифікація*. Донедавна парольна автентифікація була чи не єдиним методом автентифікації користувачів. Парольна автентифікація заснована на порівнянні пароля, що вводиться користувачем з еталонним паролем, який зберігається в базі даних у відкритому вигляді, вигляді згорток (хешування) або в зашифрованому за деяким ключем вигляді.

Перевагами парольної ідентифікації є простота використання та доступність, оскільки зазначений метод вбудований у більшість сервісів та програмних продуктів.

Недоліком зазначеного методу є його ненадійність, яка залежить від вибору пароля або ключової фрази самим користувачем. Насамперед не рекомендується призначати пароль, який асоціюється з будь-чим: датою народження, дівочим прізвищем матері, ім'ям дітей чи дружини (чоловіка) тощо. Також, пароль не повинен складатися лише з літер чи цифр. Оптимальним варіантом є використання одночасно літер (великих та малих), цифр та символів. Важливими критеріями вибору пароля є його довжина, термін використання та обмеження кількості невдалих спроб входу в систему. Так, корпорація Microsoft рекомендує своїм користувачам використовувати не менше 8 символів у паролі та змінювати його не рідше ніж через кожні 42 доби [7]. Що є головне, так це не використовувати один і той самий пароль до різних систем, бо дізнавшись його, зловмиснику буде дуже легко поставити під загрозу усі сфери вашого життя.

Наразі існує велика кількість шкідливих програмних забезпечень, за допомогою яких зловмисник може дізнатися пароль користувача та отримати несанкціонований доступ до конфіденційної інформації [8]:

Keylogger – різновид вірусу, який фіксує дії користувача: будь-то натискання клавіш на клавіатурі, рух і клік миші, дата і час натискання (зазначена інформація може передаватися до зловмисника в автоматичному режимі на мережевий диск, FTP-сервер або електронною поштою);

Clickjacking – спосіб, який змушує користувачів веб-сайтів натискати на невидимі або замасковані елементи для запуску і виконання ненавмисних дій;

Fishing – спосіб, у якому зловмисники підробляють оригінальні електронні листи або веб-сторінки з метою крадіжки особистої інформації користувачів, у тому числі логіни та паролі.

2. *Ідентифікаційна автентифікація*. Ідентифікаційна автентифікація відбувається за допомогою використання унікального предмета, який дає змогу забезпечити більш надійний захист, ніж парольна автентифікація.

Ці унікальні предмети, що використовуються для автентифікації поділяються на [9]:

пасивні предмети, які містять автентифікаційну інформацію, що передають в модуль автентифікації за вимогою. Зазначена інформація може зберігатися в предметі у відкритому вигляді (магнітні карти, електронні таблетки Touch Memory) та в захищеному вигляді (USB-токени);

активні предмети, які мають достатні обчислювальні ресурси та беруть активну участь під час автентифікації (мікропроцесорні смарт-карти і USB-токени).

Головною перевагою ідентифікаційної автентифікації є маленький розмір унікального предмета, який можна носити з собою. Також, більшість із зазначених предметів, таких як магнітні карти, електронні таблетки (Touch Memory) не потребують вводу логіна та пароля, що дає змогу не запам'ятовувати зайву інформацію.

До недоліків зазначеного методу можна віднести можливість втрати чи крадіжки унікального предмета, а також можливість несанкціонованого отримання його дубліката. Проте на відміну від парольного методу, у разі втрати зазначеного предмета, можливо швидко зреагувати на цю подію та заблокувати його для недопущення використання іншою особою. До недоліків зазначеного методу також можна віднести наявність спеціального зчитувача для унікального предмета (крім USB-токенів).

Такий унікальний предмет, як USB-токен відноситься до багатофакторної автентифікації. Наразі в Україні розроблено свій uaToken, який має вигляд usb-брелока та є універсальним засобом для автентифікації користувачів, захисту електронного листування, для безпечного доступу до ресурсів і додатків, для зберігання паролів і сертифікатів, ЕЦП, він також є єдиним пристроєм доступу, як у приміщення, так і до комп'ютерів. Для його використання необхідно лише підключити ідентифікатор до usb-порту, а потім набрати на клавіатурі PIN-код. [10]

3. *Біометрична автентифікація*. Біометрична автентифікація поширюється у всіх сферах життєдіяльності людей, оскільки біометричні дані та параметри кожної людини

є унікальними і не мають схожості навіть серед близнюків.

Так, відповідно до Закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус" [11]:

"біометричні дані - сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри - відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук)";

"біометричні параметри - вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу".

Існує велика різноманітність біометричної автентифікація, але не кожна організація може дозволити собі використання біометрії, яка тягне за собою залучення значних коштів до її реалізації.

Нижче наведені найвідоміші методи статичної біометричної автентифікації, які ґрунтуються на унікальності людини:

за відбитками пальців (порівнюються безпосередньо з зображенням відбитків пальців, отриманих за допомогою оптичних пристроїв, з відбитками з архіву або шляхом порівняння характерних деталей відбитка в цифровому виді, які отримують в процесі сканування зображень відбитка);

за формою кисті руки (відбувається шляхом наведення на руку яскравого світла, за допомогою якого аналізується освітленість чутливих елементів, яка залежить від довжини пальців, закругленості їх кінчиків і прозорості шкіри, за підсумком чого інформація від кожного фоторезистора перетворюється у цифровий код) [12];

за розташуванням вен на тильній стороні долоні (реалізується за допомогою інфрачервоної камери, яка зчитує малюнок вен на тильній стороні долоні або кисті руки, за результатом чого отримується картинка, що обробляється, і за схемою розташування вен формується цифрова згортка);

за сітківкою ока (заснований на підсвічуванні очного дна, яке сканується спеціальною камерою під час направлення зору людини на віддалену світлову точку);

за райдужною оболонкою ока (реалізується за наявністю спеціальної камери і відповідного програмного забезпечення, яке виділяє з отриманого зображення малюнок райдужної оболонки ока, за якою будується цифровий код);

за формою обличчя (реалізується за допомогою камери і спеціалізованого програмного забезпечення, що виділяють контури очей, брів, носа, губ та обчислюють відстань між ними, за результатом чого будується образ, що перетворюється в цифрову форму для порівняння);

за термограмою особи (заснований на використанні спеціальної камери інфрачервоного діапазону, яка розпізнає на обличчі артерії, що постачають кров'ю шкіру і виділяють тепло) [13];

Серед динамічних методів біометричної автентифікація, які ґрунтуються на поведінці людини, найвідомішими є:

за допомогою автоматичного аналізу підпису (візуальне сканування і дослідження динамічних характеристик руху руки у процесі виконання підпису). Другий спосіб є більш точним, оскільки підпис людини не може бути ідентичним, таким чином, порівняння підпису відбувається за допомогою застосування спеціальних вимірювальних авторучок з датчиками, чутливими до прискорення, швидкості, тиску, тривалості пауз під час підпису;

за характером голосу (реалізуються за трьома напрямками: аналізуючи короткочасні сегменти мови, тривалістю до 20 мс (вибираються короткі фрагменти, що обробляються, складаються в статистичний образ, який і порівнюється з еталоном); контурний аналіз мови (з фрагмента мови виділяється деяка характеристика голосу, для них визначається характеристична функція, яка порівнюється з еталонною; статистична оцінка голосу, тривалістю приблизно 12 с (протягом звучання якого збирається інформація про деякі параметри голосу, на основі якої створюється цифровий образ і порівнюється з еталоном) [12];

за клавіатурним почерком (заснований на вивченні основних параметрів: часу утримання клавіші (ЧУК) та часу між натиснутими клавішами (ЧМК), що визначаються під час введення з клавіатури контрольної фрази (статична), або постійного моніторингу системою під час набору (постійна)) [14].

Перевагами біометричної автентифікації є те, що самим ідентифікатором є людина, що ускладнює процес доступу до системи та вилучає необхідність носити з собою пристрої

для автентифікації та запам'ятовувати паролі. До переваг більшості методів біометричної автентифікації можна віднести високу швидкодію та точність, а також відсутність безпосереднього контакту з обладнаннями (окрім автентифікації за відбитками пальців), що дає змогу проводити процес автентифікації на відстані від декількох сантиметрів до декількох метрів.

До недоліків біометричної автентифікації відносяться її висока вартість, у зв'язку зі складністю побудови алгоритмів, залежність більшості пристроїв сканування від природного та штучного освітлення (автентифікація за формою кисті руки, за райдужною оболонкою ока), залежність від змін у зовнішності (автентифікація за формою обличчя) або пошкодження папілярного візерунка пальців (автентифікація за відбитками пальців).

4. *Автентифікація за географічним розташуванням*. Зазначений метод є новим напрямом автентифікації, що встановлює справжність користувача на основі його місцезнаходження. Він поділяється на:

розташуванні виходу до мережі Інтернет, що заснований на використанні інформації про місцезнаходження серверів, точок доступу бездротового зв'язку, через які здійснюється підключення до мережі Інтернет. Недоліком зазначеного методу є те, що інформацію про розташування можна змінити, використовуючи, так звані, проксі-сервери або системи анонімного доступу;

за допомогою GPS, що заснований на використанні системи космічної навігації, типу GPS (Global Positioning System). Зазначений метод є досить надійним завдяки нестабільності орбіти супутників, передбачити які досить важко. Також, перевагою є те, що координати постійно змінюються, що не дає змоги їх перехопити [15].

Багатофакторна автентифікація набуває все більшої популярності серед методів автентифікації користувачів, оскільки вона набагато дієвіша проти несанкціонованого отримання інформації. Серед них можливе комбінування біометричних, парольних, ідентифікаційних методів, що дає змогу збільшити ймовірність того, що під час захоплення зловмисником паролю, йому буде потрібні ваші біометричні дані або ваш ідентифікатор. Заволодіти одночасно паролем та ідентифікатором буде значно важче, на цім втрату ідентифікатора ви зможете одразу помітити та заблокувати його.

Наразі реалізовані такі пристрої багатофакторної автентифікації [16]:

1. Термінал для багатофакторної ідентифікації ZK Software IFace202: мультимедійний біометричний термінал контролю доступу та обліку робочого часу, який заснований на розпізнаванні по обличчю, відбитку пальця, проксіміті-карти (опція) і кодом. Дає змогу запам'ятати 400 осіб, 3000 відбитків, 100 000 подій, час ідентифікації менше 1,5 с.

2. Багатофакторний біометричний термінал IFace302 компанії ZKSoftware: заснований на методах ідентифікації по обличчю і за відбитками пальців, введення коду і зчитування карт доступу. Дає змогу запам'ятати 700 осіб і 3000 відбитків пальців, а також зчитувачем карток доступу Em Marine. До комплекту входять 2 камери: кольорова і чорно-біла з інфрачервоним підсвічуванням, а також TFT кольоровий сенсорний дисплей з меню. Для завантаження і зчитування даних термінали дають змогу використовувати USB-порт.

3. Пристрій Fujitsu PalmSecure ID Match: дає змогу проводити автентифікацію за допомогою сканування малюнка кровоносних судин долоні і перевірки PIN-коду до смарт-карти. До комплекту пристрою входить датчик PalmSecure, сенсорний екран, плата на базі процесора ARM і пристрій для читання карт різного формата.

Зазначені пристрої автентифікації є дієвими проти несанкціонованого доступу до інформаційних систем, але мають досить велику вартість.

Унікальність кожної людини може розглядатися як її біометричний або психологічний автентифікатори, які неможливо повторити будь-кому іншому. На фоні цього можна розглядати розпізнавання людиною кольорів або їх психологічне сприйняття для можливості автентифікації користувачів інформаційних систем.

Таким прикладом автентифікації користувачів інформаційних систем можна визначити тест Люшера, що особа яка проходить службу або працює в певній установі, проходить лише один раз при першому вході до інформаційної системи. Тест Люшера заснований на припущенні про те, що вибір кольору відображає спрямованість кожної людини на певну діяльність, настрій, функціональний стан і найбільш стійкі її риси.

Закордонні психологи іноді використовують зазначений тест під час

підбору кадрів на роботу у ту чи іншу сферу діяльності.

Характеристика кольорів (за Максом Люшером) містить у собі 4 основних та 4 додаткових кольори. Основні кольори: синій – спокій; синє-зелений – впевненість, іноді упертість; поморанчево-червоний – наступальні тенденції, агресивність; світло-жовтий – активність, прагнення до спілкування. Під час відсутності конфлікту в оптимальному стані основні кольори мають займати перші п'ять позиції. Додаткові кольори: фіолетовий, коричневий, чорний, нульовий символізують негативні тенденції: тривожність, стрес, відчуття страху, засмучення. Значення цих кольорів більшою мірою визначаються їх взаємним розміщенням, розподілом за позиціями [17].

Результатом проходження зазначеного тесту буде послідовність з 8 кольорів. Під час наступних входів до системи запитуватиметься лише певна послідовність 4-х кольорів. Їх послідовність має бути рандомною для ускладнення злому алгоритму. Так система генерує колір, який є найбільш сприятливий, 2 нейтральні та негативний. В інших випадках ця послідовність може бути змінена, проте загальний результат залишиться сталим.

До переваг методу можливо віднести його простоту реалізації та зрозумілість входження для користувачів. Крім того, від користувача системи вимагається відповідь, що не є логічною для людей, які можуть бачити його пароль, а поведінковою – зрозумілою тільки для нього. Як результат його відповіді матимуть низький часовий показник, що може стати додатковим фактором автентифікації.

Недоліком методу є те, що він не дає змоги ідентифікувати користувача на 100 %, отже його використання можливе лише як елемент багатофакторної автентифікації.

Висновки та перспективи подальших досліджень. Підсумовуючи, зазначимо, що багатофакторна автентифікація все більше витісняє однофакторну автентифікацію, що обґрунтовується складністю отримання зловмисником одразу двох чи трьох ключів (паролів, пристроїв) від інформаційної системи, а ще складніше буде підробити ще й біометричний автентифікатор. Використання будь-якого паролю чи пристрою автентифікації разом з унікальністю рис характеру та зовнішності кожної людини дає можливість створити найкращий захист інформаційних систем.

Отже, метод автентифікації користувачів за допомогою тесту Люшера також є перспективним для можливості використання його під час входу до системи та отримання максимального захисту системи, використовуючи лише поведінкові особливості людини. Подальша робота буде направлена на створення алгоритму входження до системи за допомогою тесту Люшера та можливості використання на практиці зазначеного методу.

Окремо слід виділити питання зберігання ключової інформації в інформаційних системах. Розподіленість баз даних, що зберігають ідентифікатори, а також способи одночасного безпечного доступу до кожної бази ідентифікаторів у режимі онлайн потребують окремого вивчення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кошева Н. А., Мазниченко Н. І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. *Системи обробки інформації*. Київ, 2013. Вип. 6. С. 215–223.
2. Кісь Я. П., Теслюк В. М. Методи і засоби автентифікації біометричних даних в інформаційних системах. *Актуальні проблеми економіки*. 2012. № 12. С. 174–182.
3. Высказывания, афоризмы и цитаты об информации. URL: http://www.wisdoms.one/tsitati_pro_informatsiy.html (дата звернення: 15.04.2020).
4. Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18.09.2019 р. № 856. *Офіційний вісник України*. 2019. № 80. Ст. 2736.
5. Про затвердження Положення про інтегровану систему електронної ідентифікації : Постанова Кабінету Міністрів України від 19.06.2019 р. № 546. *Офіційний вісник України*. 2019. № 52. Ст. 1790.
6. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999-07-01]. Київ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).
7. Пароль должен соответствовать требованиям к сложности. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements (дата звернення: 16.04.2020).
8. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома. URL: https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma (дата звернення: 16.04.2020).

9. Панасенко С. Методы аутентификации. URL: http://www.panasenko.ru/Articles/69/69.html (дата звернення: 16.04.2020).
10. Украинское средство аутентификации. URL: http://www.uatoken.kiev.ua/ (дата звернення: 17.04.2020).
11. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 р. № 5492-VI. *Відомості Верховної Ради України*. 2013. № 51. Ст. 716.
12. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Одеса, 2018. 228 с.
13. Мороз А. О. Біометричні технології ідентифікації людини. Огляд систем. *Математические машины и системы*. 2011. № 1. С. 39–45.
14. Чалая Л. Э. Модель идентификации пользователей по клавиатурному почерку. *Штучний інтелект*. 2004. №4. С. 811–817.
15. Аутентификация с помощью sms. URL: https://studfile.net/preview/7883128/page:4/ (дата звернення: 20.04.2020).
16. Багатофакторна ідентифікація. URL: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-identifikaciu/bagatofaktorna-identifikacia (дата звернення: 20.04.2020).
17. Тест Люшера – описание и интерпретация. URL: https://psyfactor.org/lib/lusher.htm (дата звернення: 20.04.2020).

Стаття надійшла до редакційної колегії 03.06.2020

Protection of information systems through the use of authentication methods

Annotation

Each institution and enterprise has communication and technological systems, the protection of which is one of the important tasks to keep them in an efficient and functional condition. Failure of one of the systems can lead to collapse, namely: loss of air communications or loss of control over the banking system. So, critical information infrastructure facilities of the Ministry of Defense of Ukraine may be exposed to the same risks, considering the Ukrainian conflict in eastern Ukraine with Russia.

In order to prevent illegal actions over the Information Systems of the Armed Forces of Ukraine, the seizure of information contained on servers or computers and to prevent unauthorized access, systems with authentication and user identification procedures should be used.

Currently, depending on the number of user authentication methods, there is single-factor and multi-factor authentication is used. Multifactor authentication is increasingly displacing one-factor authentication, which is justified by the difficulty of an attacker obtaining two or three keys from the Information System at once but biometric authenticator will be more difficult to counterfeit. The use of any password or authentication devices along with the uniqueness of each person's appearance makes it possible to create the best protection for information systems.

The method of user authentication using the Luscher test is promising for use when logging in and maximizing its protection, using only human’s characteristics. Further work will be focused to the creation an algorithm for entering the system using the Luscher test and the possibility use to use this method in practice.

Keywords: authentication; information systems; Luscher test.