УДК 004.056.53

Фесьоха В.В. (ВІТІ) ORCID - 0000-0001-6612-1970
Фесьоха Н.О. (ВІТІ) ORCID - 0000-0002-9797-5589
Доброштан О.С. (ВІТІ) ORCID - 0000-0002-1527-1474

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У статті розглядається процедура визначення автентичності користувачів інформаційних систем та мереж (ІСМ) спеціального призначення на основі пред'явленого ними ідентифікатора у контексті процесу контролю доступу користувачів до ресурсів та/або сервісів ІСМ. Вибір даної процедури для дослідження обумовлено наявністю властивості формування заключного рішення щодо встановлення легітимності особистості користувача. Наведено статистику кібератак, спрямованих на отримання несанкціонованого доступу за 2019-2020 роки. Визначено вимоги до сучасних систем контролю доступу (СКД) з врахуванням умов постійного удосконалення механізмів несанкціонованих втручань, проведено відповідний аналіз існуючих методів і програмних рішень автентифікації користувачів ІСМ, описано їх переваги та недоліки. На основі проведеного аналізу обрано найперспективніший підхід до автентифікації користувачів – поведінкову біометрію та науково-методичний апарат – нечітку логіку для подальшої розробки (удосконалення) та впровадження ефективних методів визначення автентичності користувачів ІСМ спеціального призначення з метою підвищення ефективності функціонування СКД. Визначено подальший напрям наукових досліджень за даною тематикою.

Ключові слова: *несанкціонований доступ, інформаційні системи та мережі, біометрична автентифікація, нечітка логіка.*

Фесёха В.В., Фесёха Н.А., Доброштан А.С. Анализ существующих решений аутентификации пользователей информационных систем и сетей специального назначения

В статье рассматривается процедура определения подлинности пользователей информационных систем и сетей (ИСС) специального назначения на основе предъявленного ими идентификатора в контексте процесса контроля доступа пользователей к ресурсам и/или сервисам ИСС. Выбор данной процедуры для исследования обусловлено наличием свойства формирования заключительного решения по установлению легитимности личности пользователя. Приведена статистика кибератак, направленных на получение несанкционированного доступа за 2019-2020 годы. Определены требования к современным системам контроля доступа (СКД) с учетом условий постоянного совершенствования механизмов несанкционированных вмешательств, проведен соответствующий анализ существующих методов и программных решений аутентификации пользователей ИСС, описаны их преимущества и недостатки. На основе проведенного анализа избран самый перспективный подход к аутентификации пользователей – поведенческую биометрию и научно-методический аппарат – нечеткую логику для дальнейшей разработки (усовершенствования) и внедрения эффективных методов определения подлинности пользователей ИСС специального назначения с целью повышения эффективности функционирования СКД. Определено дальнейшее направление научных исследований по данной тематике.

Ключевые слова*: несанкционированный доступ, информационные системы и сети, биометрическая аутентификация, нечеткая логика.*

V. Fesokha, N. Fesokha, O. Dobroshtan. Analysis of existing solutions for user authentication of information systems and special-purpose networks

The article discusses the procedure for determining the authenticity of users of information systems and networks (ISN) for special purposes on the basis of the identifier presented by them in the context of the process of controlling user access to ISN resources and/or services. The choice of this procedure for research is due to the presence of the property of forming the final decision to establish the legitimacy of the user's identity. The statistics of cyber-attacks aimed at obtaining unauthorized access for 2019-2020 are presented. The requirements for modern access control systems (ACS) are determined, taking into account the conditions for the continuous improvement of the mechanisms of unauthorized interventions, a corresponding analysis of existing methods and software solutions for the authentication of ISN users is carried out, their advantages and disadvantages are described. On the basis of the analysis, the most promising approach to user authentication was chosen – behavioral biometrics and scientific and methodological apparatus – fuzzy logic for further development (improvement) and implementation of effective methods for determining the authenticity of users of special purpose ISN in order to increase the efficiency of ACS functioning. The further direction of scientific research on this topic has been determined.

Keywords*: unauthorized access, information systems and networks, biometric authentication, fuzzy logic.*

Актуальність та постановка завдання у загальному вигляді. Одним з основних факторів, що визначають стан кібербезпеки ІСМ спеціального призначення є ефективність функціонування їх підсистем контролю доступу до інформаційних ресурсів та/або сервісів.

Так, процес контролю доступу користувачів до ІСМ здійснюється з врахуванням положень та вимог політики безпеки на основі класичного підходу багатоешелонованого визначення їх особистості, функціональну DFD-діаграму якого представлено на рисунку 1.

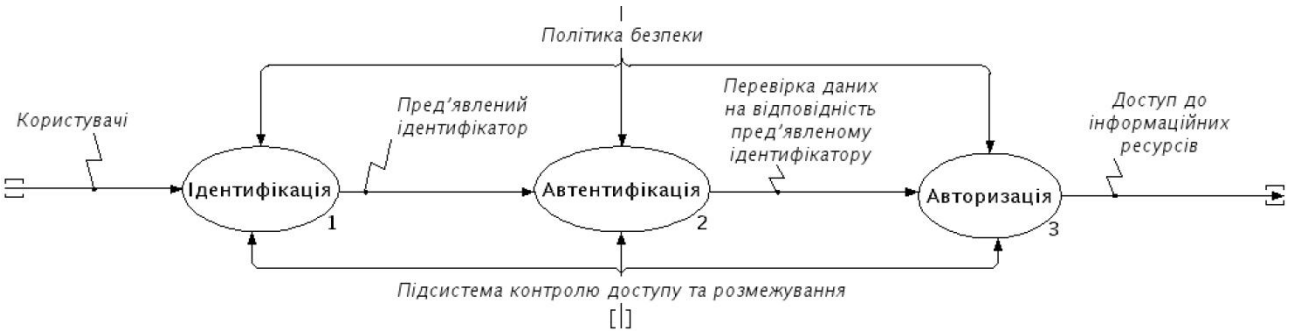

Рис. 1. Функціональна DFD-діаграма процесу контролю доступу

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором; впізнання [1].

Автентифікація (authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності [1].

Авторизація (authorization) – процедура надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створившим його користувачем або процесом) [1].

Пріоритетною процедурою із наведених є автентифікація, оскільки саме на етапі її виконання підтверджується/не підтверджується автентичність користувача на основі пред'явленого в ІСМ ідентифікатора.

Аналіз останніх досліджень і публікацій [2, 3] показав, що питання удосконалення існуючих підходів (механізмів) автентифікації останнім часом піднімається особливо гостро. Так, згідно результатів досліджень міжнародної компанії "Positive Technologies", що спеціалізується на розробці інноваційних рішень у сфері інформаційної безпеки 45% найпоширеніших вразливостей програмного забезпечення займають недоліки автентифікації (Broken Authentication) та 37% – недоліки контролю доступу. Так, для однієї програми – об'єкта тестування знадобилося лише 100 спроб, щоб успішно увійти до її оболонки з правами привілейованого користувача. За даними національного інформаційного агентства "Укрінформ" американська компанія-розробник антикоронавірусної вакцини "Moderna Inc." і Європейське агентство з дослідження вакцин "COVID-19" "Pfizer Inc." та "BioNTech" постраждали від кібератак типу отримання несанкціонованого доступу (зловмисники отримали доступ до документів, пов'язаних із розробкою вакцини), що свідчить про високий рівень загроз від інформаційно-руйнівних вторгнень такого характеру.

На основі викладеного, а також з врахуванням умов постійного удосконалення підходів здійснення несанкціонованих втручань (вторгнень) у ІСМ, фактичної відсутності адміністративних обмежень у кібернетичному просторі зростають вимоги до систем захисту інформації [4], здатних паралельно з оборонними засобами захисту ІСМ по периметру – системами виявлення кібератак забезпечувати достовірну автентичність користувачів ІСМ спеціального призначення на предмет виявлення несанкціонованої (зловмисної) діяльності [5].

Даний факт обумовлює актуальність подальших наукових досліджень, які полягають у розробці (удосконаленні) нових підходів до визначення автентичності пред'явленого користувачами ІСМ ідентифікатора з метою подальшого впровадження у функціональну архітектуру систем контролю та розмежування доступу.

Метою статті є проведення порівняльного аналізу застосування існуючих теоретичних та програмних рішень автентифікації користувачів ІСМ.

Порівняльний аналіз існуючих методів автентифікації. Практика застосування систем контролю доступу сформувала основні методи автентифікації, які представлено на рисунку 2 [5, 6, 7]:

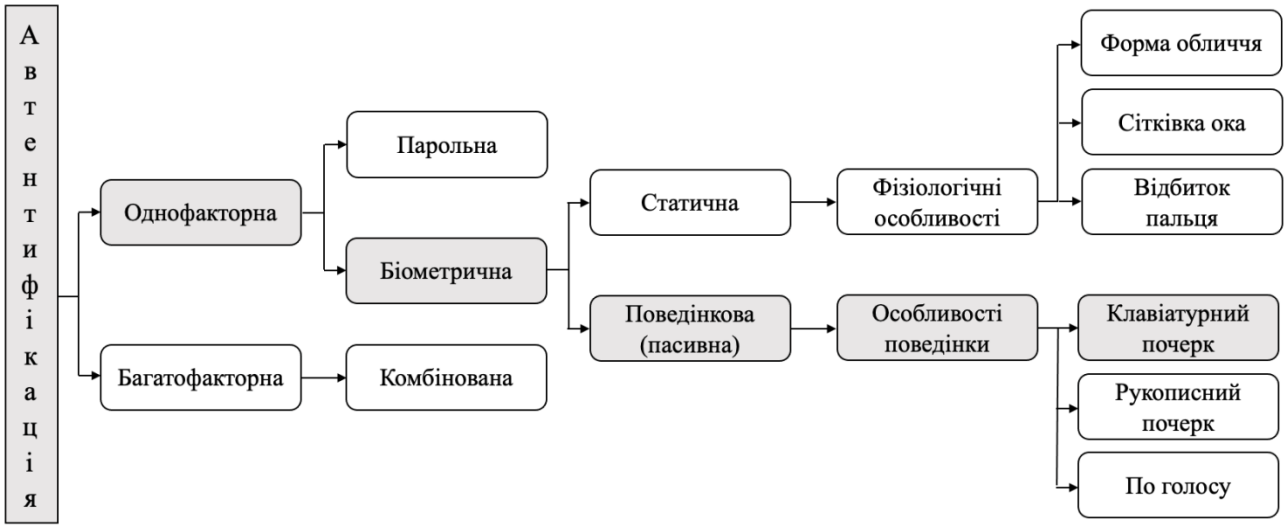

Рис. 2. Основні існуючі методи автентифікації ІСМ

парольна – використання унікального знання (наприклад, логін-пароль);

комбінована – використання різних компонентів у поєднанні (наприклад, фізичний токен і пароль);

багатофакторна – використання багатошарової перевірки (наприклад, пароль і код, відправлений на номер телефону засобами смс-повідомлень);

біометрична – використання біометричних характеристик людини.

Завдяки високій продуктивності, низькій вартості, простоті реалізації та використання парольна автентифікація стала найпоширенішим способом встановлення особи користувача. Основним недоліком такого підходу є використання користувачами ІСМ "слабких" паролів (ненадійних ключових слів), які відносно легко підбираються сучасним шпигунським програмним забезпеченням. Саме слабкість парольного захисту є однією з основних причин уразливості комп'ютерних систем кібернетичними вторгненнями, вектором яких є спроба отримання несанкціонованого доступу (Remote to Local, User to Root) [8, 9].

Комбіновані та багатофакторні методи автентифікації не забезпечують повного захисту від крадіжки облікового запису, проте надають більш надійний захист, ніж автентифікація за одним компонентом (парольна) [10].

Біометрична автентифікація (статична та динамічна/поведінкова) стає все більш прогресивним методом головного засобу захисту облікових записів користувачів і підтвердження їх автентичності. Статична полягає у перевірці унікального біологічного ідентифікатора користувача ІС (відбиток пальця, райдужна оболонка ока тощо). У даному випадку встановлення особистості користувача відбувається лише на етапі входу в систему і в подальшому не контролюється. Основною перевагою такого підходу є його швидкість, незалежність від психологічного стану користувача, і, як наслідок, можливість організації автентифікації значних потоків людей. Проте апаратна складність статичних методів призводить до значних фінансових затрат на придбання засобів для зчитування біометричних

характеристик людини. До того ж, у жовтні 2019 року команда Tencent Security X-Lab, яка займається проблемами кібербезпеки продемонструвала спосіб несанкціонованого доступу до чужого смартфону за допомогою знятих відбитків пальців зі склянки у ресторані [11,12].

Динамічна (поведінкова) здійснює встановлення особистості користувача циклічно за певним інтервалом часу протягом усієї сесії роботи з інформаційною системою на основі побудованого профілю користувача, який складається з множини притаманних йому поведінкових характеристик. Підходи, що створені на основі динамічних характеристик автентифікації (за почерком, за клавіатурним почерком, за голосом), як правило, простіші в реалізації, оскільки не вимагають значних затрат на устаткування і можуть обмежуватися лише відповідним програмним забезпеченням, яке вимагає мінімальну підтримку фахівця у процесі експлуатації [11].

На основі проведеного аналізу існуючих методів автентифікації та виявлених в них недоліків можна зробити висновок про доцільність використання СКД в ІСМ, в основу яких покладено аналіз поведінкової біометрії, оскільки лише такий підхід дозволяє підвищити достовірність автентифікації ідентифікованого користувача завдяки властивостям аналізу його поведінки протягом усієї сесії роботи, що у свою чергу дозволяє виявити факт зміни користувача в умовах відсутності статичних біометричних даних, паролю (фізичного токену), які можливо використати для компрометації. Для впровадження даного підходу на практиці в сучасних умовах функціонування ІСМ доцільно застосувати підхід до автентифікації користувачів на основі клавіатурного почерку.

Порівняльний аналіз існуючих методів автентифікації користувачів на основі клавіатурного почерку [4, 5, 6, 7, 11, 12]. Метою даного аналізу є дослідження основних існуючих методів аналізу клавіатурного почерку на основі підходу поведінкової біометрії у руслі їх відповідності сучасним вимогам до систем захисту інформації, а також визначення їх основних переваг та недоліків для подальшого вибору найефективнішого підходу.

Рис. 3. Існуючі методи автентифікації на основі клавіатурного почерку

Найбільш поширеними методами є [4, 5, 6, 7]:

імунні системи: імунні мережі є механізмом класифікації і будуються за аналогією з імунною системою живого організму.

Основна перевага імунних систем полягає у можливості розпізнавання “своїх” унікальних особливостей в наборі досліджуваних даних. Однак, використання даного підходу дає досить велику обчислювальну складність;

нейронні мережі: мережа навчається протягом деякого часу, після чого запускається у режимі розпізнавання.

У ситуації, коли у вхідному потоці даних не вдається розпізнати профіль поведінки користувача, фіксується факт його нелегітимності.

У разі використання репрезентативної навчальної вибірки нейронні мережі дають достатню стійкість в межах заданої системи; але складання подібної вибірки є складним завданням;

геометрія відстані: модель вимірювання дистанції визначає на скільки близько чи далеко вибірка даних знаходиться від тієї, що попередньо збережена. Дистанція між профілем користувача, який зберігається у базі та новим побудованим профілем провинна бути близькою до нуля або нижчою за вказаний поріг.

кластерний аналіз: суть даної групи методів полягає у розбитті множини спостережуваних векторів клавіатурного почерку на кластери, серед яких виділяють кластери профілю поведінки користувача.

У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність спостережуваного вектору одному з кластерів або вихід за межі відомих кластерів;

статистичний аналіз: сімейство методів засноване на побудові статистичного профілю поведінки користувача протягом деякого періоду навчання.

Для кожного параметра клавіатурного почерку будується інтервал допустимих значень, з використанням певного закону розподілу. Далі система оцінює відхилення спостережуваних значень від значень, отриманих під час навчання.

Якщо відхилення перевищують деякі задані значення, то фіксується факт нелегітимності користувача;

методи класифікації: дозволяють побудувати функцію, яка вирішує задачу класифікації клавіатурного почерку, при цьому, для визначення профілю користувача формується вектор ознак, а далі – здійснюється навчання та побудова класифікатора, в результаті чого отримана функція здійснює класифікацію векторів-ознак і, таким чином, розпізнає приналежність динаміки клавіатурного почерку певному профілю користувача;

фрактальний аналіз: даний метод аналізує клавіатурний почерк користувача системи на основі властивості самоподібності, ключовими поняттями в якому є параметр Херста – H і фрактальна Хаусдорфова розмірність.

Для властивості самоподібності виконується співвідношення $0,5 < H < 1$;

нечітка логіка: метод на основі теорії нечіткої логіки використовується для формалізації неточних знань для подальшого аналізу клавіатурного почерку.

Дозволяє визначити проміжні значення для загальноприйнятих оцінок (так | ні, істинно | хибно).

Метод є ефективним для дослідження об’єктів, ідентифікація яких занадто трудомістка, розмита, у слабоструктурованих задачах, а також у випадках, коли за умовами задачі необхідно використовувати знання експерта.

Дослідження вказаних методів аналізу клавіатурного почерку на основі підходу поведінкової біометрії у руслі їх відповідності сучасним вимогам до систем захисту інформації представлено у таблиці 1.

Вимоги до систем контролю доступу представлено наступними критеріями [4]:

верифікованість – критерій, який дозволяє оцінити, чи може адміністратор з кібербезпеки відтворити послідовність кроків щодо прийняття рішення системою про автентичність користувача на основі пред’явленого ідентифікатора, оперуючи вхідними та вихідними даними, що дозволяє оцінити коректність моделі;

адаптивність – здатність системи оперативно реагувати на динаміку процесу функціонування або на зміни в множині ознак клавіатурного почерку.

Дана властивість дозволяє системі захисту визначати профіль користувача з врахуванням певної поведінкової динаміки користувача;

стійкість – в незалежності від об’єкта захисту для одних і тих же вхідних даних модель повинна видавати один і той же результат (глобальна стійкість). У противному випадку стійкість називається локальною;

обчислювальна складність – теоретична оцінка складності методу у процесі прийняття рішення щодо виявлення кібератак. Результати порівняльного аналізу методів автентифікації на основі клавіатурного почерку показують, що для більшості із них характерним недоліком є слабка верифікованість та стійкість.

Таблиця 1

Існуючі методи автентифікації на основі клавіатурного почерку

	Верифікованість	Адаптованість	Стійкість	Обчислювальна складність
Імунні системи	–	+	–	> O(n)
Нейронні мережі	–	+	–	> O(n)
Геометрія відстані	–	+	–	P
Кластерний аналіз	–	+	–	> O(n)
Статистичний аналіз	–	+	–	> O(n)
Методи класифікації	–	+	–	ln(n)
Фрактальний аналіз	–	+	–	> O(n)
Нечітка логіка	+	+	+	> O(n)

З іншого боку, основною їх перевагою є адаптивність до незначної динаміки поведінки користувача ІСМ. Проте, серед них можна виділити метод, який демонструє найбільш повну відповідність критеріям аналізу, є одночасно верифікованим, адаптивним, стійким за умов прийнятної обчислювальної складності – апарат нечіткої логіки.

Порівняльний аналіз існуючих програмних рішень автентифікації користувачів на основі клавіатурного почерку [13, 14, 15, 16]. Метою даного аналізу є дослідження існуючих відкритих програмних рішень на предмет визначення методів, покладених в їх основу функціонування. Аналіз динаміки натискання клавіш у більшості випадків використовується для процесу автентифікації разом з ідентифікатором або паролем користувача у формі багатофакторної автентифікації. Проте, існує спосіб застосування даного підходу у вигляді форми спостереження. Такого роду програмні рішення, часто, без усвідомлення користувачів про їх наявність, відслідковують динаміку роботи з клавіатурою. Зібрані дані з такого трекінгу використовуються для аналізу та визначення їх належності легітимному обліковому запису користувача.У таблиці 2 наведено коротку інформативну довідку про існуючі програмні рішення встановлення особистості користувача, використовуючи підхід пасивної біометрії на основі аналізу динаміки натискання клавіш.

Таблиця 2

Існуючі програмні рішення автентифікації на основі пасивної біометрії

Найменування продукту	Розробник	Офіційний сайт
TypingDNA	Raul Popa, Cristian Tamas et al.	https://www.typingdna.com/
BehavioSec	ForgeRock organization	https://www.behaviosec.com/
Banking System with Keystroke authentication	Saksham Saini	https://github.com/saqsham/Banking-System-with-Keystroke-authentication
BioCatch-Auth	ForgeRock organization	https://www.biocatch.com/

TypingDNA – вбудований механізм на основі елементів штучного інтелекту, здатний розрізняти два паттерни вводу з безпрецедентною точністю. Пропонується інтерфейс для використання автентифікації на основі аналізу клавіатурного вводу, що забезпечує: безпеку під час входу до системи або вимушеного скидання паролю; виявлення зловмисників; здійснення біометричної онлайн-автентифікації для аналітики поведінки користувачів; виконання багатофакторної автентифікації; здійснення ідентифікації користувача; запобігання діям шахраїв.

BehavioSec – продукт шведської компанії, яка спеціалізується на системах тривалої автентифікації. Дане програмне забезпечення здійснює моніторинг активності користувача, щоб упевнитися в тому, що за цим комп'ютером працює саме власник. Використовується не тільки аналіз динаміки натискання на клавіш, але і використання комп'ютерної миші (тачпаду).

Banking System with Keystroke authentication – відкрита реалізація пасивної біометрії, представлена звичайною сторінкою банківського веб-сайту та аналізу динаміки натискання на клавіші. Посилаючись на фактор, що характеристики вводу різних людей є унікальними, здійснюється автентифікація користувачів на основі вилучення паттернів їхнього стилю вводу паролю.

BioCatch-Auth – програмне рішення, розроблене на основі підходу пасивної біометрії. Платформа формує поведінкові профілі користувачів для розпізнавання широкого кола загроз кібербезпеки різного роду, включаючи шкідливе програмне забезпечення, трояни віддаленого доступу (remote access Trojan – RAT) та роботизовану діяльність (боти).

BioCatch-Auth забезпечує наступними можливостями:

перевірка особистості – аналіз різних вимірів способів введення інформації (вільне користування додатками, навігаційними можливостями) та зіставлення даних для виявлення використання викрадених або синтетичних ідентифікаційних даних при заповненні онлайн-заявок;

тривала автентифікація – вибірка 20 унікальних характеристик із бази вимірів користувальницьких профілів для аналізу поведінки протягом сеансу;

запобігання шахрайству – використовуючи підхід "скритного моніторингу" відбувається ідентифікація можливих загроз та оповіщення про виявлені підозри в режимі реального часу з мінімальною кількістю помилкових тривог.

У таблиці 3 представлено порівняльний аналіз функціонування та можливостей описаних рішень автентифікації на основі поведінкової біометрії.

Таблиця 3

Порівняльний аналіз існуючих програмних рішень автентифікації

	TypingDNA	BehavioSec	BioCatch-Auth	Banking System with Keystroke authentication
Сумісність	Мобільні пристрої, ПК	Мобільні пристрої, ПК	Мобільні пристрої, ПК	ПК
Метод автентифікації	Статистичні метричні методи	Методи машинного навчання	Конфігурація дерева автентифікації та політики прав для користувачів	Метод опорних векторів
Відкритий доступ	+	+	+	+
Точність результатів	90%	95%	90%	90%

Проведений порівняльний аналіз існуючих рішень автентифікації користувачів ІСМ на основі застосування підходу пасивної біометрії показав досить високі результати за показником точності встановлення автентичності пред'явленого ідентифікатора. Поряд з цим, виявлено наступні недоліки, що знижують практичну цінність їх застосування:

залежність від зміни психоемоційного стану користувача, що обумовлює в подальшому наявність хибних спрацювань системою;

відсутність можливості верифікації процесу встановлення автентичності користувача на основі заявленого ним ідентифікатора;

відсутність можливості встановлення факту зміни користувача на робочому місці.

Проведений аналіз основних існуючих як теоретичних, так і практичних рішень автентифікації користувачів ІСМ із використанням підходу пасивної біометрії, зокрема методу аналізу клавіатурного почерку дозволяє зробити висновок про відсутність СКД, функціонал яких забезпечує вирішення вищеописаних недоліків.

Висновок. У контексті викладеного, перспективним підходом до вирішення даного завдання є створення інтелектуальних СКД ІСМ, в основу функціонування яких необхідно покласти математичний апарат теорії нечіткої логіки. Реалізація такого підходу дозволить:

створити механізм побудови нечіткого профілю облікового запису користувача ІСМ;

зберегти прийнятну обчислювальну складність на процедуру автентифікації користувача; здійснювати прийняття ефективних рішень в умовах неповноти та нечіткості управляючої інформації; доповнити СКД властивістю верифікації поточної ситуації щодо процедури автентифікації; доповнити СКД властивістю адаптивності до динаміки поведінки користувача. Окрім того, досвід дослідної експлуатації систем виявлення кібератак, що реалізовані на основі застосування наведеного підходу дозволяє досягнути більше 96% ефективності виявлення кібератак за показником точності [17]. Перспективними напрямками подальших наукових досліджень є розробка моделі автентифікації користувача ІСМ на основі теорії нечіткої логіки.

ЛІТЕРАТУРА

1. НД ТЗІ 1.1-003-99 : 1999. Системи технічного захисту інформації. [Чинний від 1999-07-01]. Київ, 1999. 22 с. (Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу).

2. Уязвимости и угрозы веб-приложений в 2019 году [Електронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020/#id4

3. Хакери отримали доступ до даних компаній-розробника вакцини Moderna [Електронний ресурс]. Режим доступу: https://www.ukrinform.ua/rubric-world/3154639-hakeri-otrimali-dostup-do-danih-kompaniirozrobnika-vakcini-moderna.html.

4. Субач І.Ю., Фесьоха В.В., Фесьоха Н.О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій. Information Technology and Security. 2017. № 1. С. 29 – 41.

5. Еременко Ю.И., Олюнина Ю.С. Об определении метода обработки потока данных с целью выявления скрытых характеристик клавиатурного почерка. Прикладная математика и вопросы управления. 2017. № 3. С. 69 – 78.

6. Сабанов А.Г., Смолина С. Г. Сравнительный анализ методов биометрической идентификации личности. Труды ИСА РАН. Том 66. 3/2016. С. 11 – 20.

7. Чалая Л.Э. Сравнительный анализ методов аутентификации пользователей компьютерных систем по клавиатурному почерку. Системи ОБРОБКИ информации, 2008, випуск 1 (68). С. 108 – 116.

8. Парольна ідентифікація [Електронний ресурс]. Режим доступу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-identifikaciu/parolna-identifikacia.

9. Слабые пароли стали предпосылкой 76% кибератак на компании [Електронный ресурс]. Режим доступа: https://www.anti-malware.ru/news/2014-07-17/14402.

10. Мазниченко Н. І. Підвищення захищеності інформаційних ресурсів комп'ютерних систем на основі систем ідентифікації користувачів / Актуальні питання сучасної науки: матер. Всеукр. наук.-практ. інтернет-конф., м. Бережани, 2017 р., – Вип. 1. – С. 236-246.

11. Технологии биометрической идентификации [Електронный ресурс]. Режим доступа: https://www.tadviser.ru/index.php.

12. Маркелов К. С. Биометрические информационные технологии: актуальные и перспективные методы / К. С. Маркелов, В. В. Нечаев // Информационные и телекоммуникационные технологии. 2013.№ 18. С. 24 – 42.

13. Typingdna [Online]. Access: Режим доступа: https://www.typingdna.com/.

14. BehavioSec [Online]. Access: https://www.behaviosec.com/.

15. Banking-System-with-Keystroke-authentication [Online]. Access: https://github.com/saqsham/Banking-System-with-Keystroke-authentication.

16. BioCatch [Online]. Access: https://www.biocatch.com/.

Fesokha Vitalii Viktorovich, Subach Ihor Yuriiovych, Kubrak Volodymyr Oleksandrovych, Mykytiuk Artem Viacheslavovych, Korotaiev Stanislav Oleksandrovych. Zero-day polymorphic cyberattacks detection using fuzzy inference system. Austrian Journal of Technical and Natural Sciences. № 5 – 6 2020. P. 8 – 13.