appropriate means are not always effective. Therefore, the development of verification tools and experimental research of relevant technical solutions, tools and software to detect cyberattacks, abuses and anomalies in information systems to confirm the adequacy of their work is an urgent scientific task. There are a number of works, such as a tuple model of attack environments, a number of methods for detecting anomalous states, a methodology for building an intrusion detection system, and a structural model of a computer system to create cyberattacks and its algorithmic and software. To verify it, a specialized cyber threat emulator is needed, as the known ones do not support the necessary data formats used in the author's development. Based on this, the aim is to develop an emulator for experimental research to confirm the reliability of the obtained theoretical provisions, practical results and adequacy of the software module of the developed cyberattack detection system, which will improve the functional properties of modern intrusion detection systems for real time.

Keywords: attacks, cyberattacks, anomalies, intrusion detection systems, anomaly detection systems, attack detection systems, cyberattack detection systems, anomaly detection in computer networks.

Корченко Анна Олександрівна, доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net.
Orcid ID: 0000-0003-0016-1966.
Корченко Анна Александровна, доктор технических наук, доцент, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Korchenko Anna, Dr Eng (Information security), Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету, старший науковий співробітник Національної академії СБ України.
E-mail: y.dreis@nau.edu.ua.
Orcid ID: 0000-0003-2699-1597.
Дрейс Юрий Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета, старший научный сотрудник Национальной академии СБ Украины.
Yurii Dreis, PhD Eng (Information Security), Associate Professor of IT-Security Academic Department, National Aviation University, Senior Researcher of Scientific Department, National Academy of Security Service of Ukraine.

Нагорний Юрій Іванович, кандидат технічних наук, викладач спеціальних дисциплін відокремленого структурного підрозділу «Новокаховський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Моторного».
E-mail: ur.duran@gmail.com.
Orcid ID: 0000-0002-6437-3629.
Нагорный Юрий Иванович, кандидат технических наук, преподаватель специальных дисциплин обособленного структурного подразделения «Новокаховский профессиональный колледж Таврийского государственного агротехнологического университета имени Дмитрия Моторного».
Yurii Nahornyi, candidate of technical sciences, teacher of special disciplines of a separate structural subdivision «Novokakhovka vocational college of the Tavriya state agrotechnological university named after Dmitry Motorny».

Бичков Володимир Вячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
Email: bychkov.volodymyr@gmail.com.
Orcid ID: 0000-0002-1054-9182.
Бичков Владимир Вячеславович, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.
Volodymyr Bychkov, Senior Lecturer of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.23.15431
УДК 004.056.53

МОДЕЛЬ НЕЧІТКОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

Віталій Фесьоха, Надія Фесьоха

У статті розглянуто актуальне наукове завдання кіберзахисту інформаційних систем органів військового управління від несанкціонованого доступу. Запропоновано модель автентифікації користувачів інформаційних систем, яка ґрунтується на використанні поведінкової біометрії та математичного апарату теорії нечіткої логіки. Суть запропоно-

вано підходу в першу чергу полягає у побудові профілю користувача системи на основі інженерії поведінкових закономірностей (частих залежностей) з множини досліджуваних параметрів, які достатньо повно відображають притаманні йому підсвідомі характерні риси під час відтворення процесу, що підлягає автентичності. У другу чергу, завдання нечіткої автентифікації користувачів системи зводиться до визначення рівня відповідності їх поведінкових характеристик існуючому профілю на основі аналізу множини досліджуваних параметрів в умовах неповноти, нечіткості та неточності управляючої інформації. Представлена модель дозволяє виявляти притаманні конкретному користувачу підсвідомі поведінкові риси, присутні у різних психоемоційних станах, що у свою чергу дозволяє позбутися множини опису станів кожного облікового запису та зменшити кількість хибних спрацьовувань у процесі автентифікації особи, що значно підвищує ефективність кібербезпеки інформаційних систем органів військового управління.

Ключові слова: *несанкціонований доступ, інформаційні системи, біометрична автентифікація, інженерія закономірностей, нечітка логіка.*

ВСТУП

Актуальність та постановка завдання у загальному вигляді. В умовах постійного удосконалення прийомів, способів та методів здійснення несанкціонованого доступу у інформаційні системи (ІС) об'єктів критичної інфраструктури, фактичної відсутності адміністративних обмежень, а також технічних можливостей у кібернетичному просторі залишається відкритим питання ефективного забезпечення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів ІС спеціального призначення, зокрема ІС органів військового управління (ОВУ).

Так, функціонування ОВУ як у повсякденній діяльності, так і в умовах ведення бойових дій або ведення оборонних, наступальних/ контрнаступальних кібероперацій передбачають щоденне прийняття важливих для національної безпеки рішень на основі обробки інформації у сучасному технологічному режимі, що обумовлює необхідність захисту ІС ОВУ від зловживань у режимі реального часу [2].

Одним з основних напрямків вирішення даного завдання є забезпечення ефективного розмежування доступу користувачів до консолі управління ІС, службової (закритої) інформації, а також організація захисту від несанкціонованих втручань на основі багатоешелонованого встановлення особистості користувача (ідентифікація, автентифікація та авторизація) [1].

Оскільки саме на етапі автентифікації підтверджується/не підтверджується особистість користувача на основі пред'явленого ним в ІС ідентифікатора, тому доцільно удосконалювати існуючі (розробляти нові) підходи до контролю доступу користувачів ІС на основі процедури автентифікації у руслі підвищення захищеності від компрометації ідентифікатора/ автентифікатора.

Аналіз останніх досліджень і публікацій [1, 3-9] показав доцільність використання механізмів автентифікації, в основу яких покладено аналіз поведінкової (пасивної) біометрії, оскільки лише такий підхід дозволяє підвищити автентичність ідентифікованого користувача завдяки властивостям аналізу його поведінки протягом усієї сесії роботи з ІС, що у свою чергу дозволяє виявити факт зміни користувача в умовах відсутності статичних біометричних даних, паролю (фізичного токену), які можливо використати для компрометації. Додатково ефективність даного підходу досягається практичним унеможливленням підміни поведінкових характеристик людини та характерних підсвідомих особливостей у процесі відтворення певної дії [4].

Так, підтвердження особистості користувача після пред'явленого ним ідентифікатора здійснюється на основі аналізу його поведінки під час виконання процесу, що підлягає автентичності. Наприклад, для остаточного встановлення особи користувача передбачено отримання його особистого підпису на дігітайзері.

У даному випадку аналізу підлягає не кінцевий результат – підпис, а параметри процесу його відтворення (кут нахилу пера, швидкість відтворення, час на відтворення, сила натискання, скільки разів перо відривалося від сенсора тощо), що значно сприяє підвищенню ефективності систем контролю доступу на етапі, що передує авторизації.

Для реалізації даного підходу на практиці в сучасних умовах функціонування ІС ОВУ доцільно застосовувати підхід до автентифікації користувачів на основі клавіатурного почерку, се-

ред методів реалізації якого можна виділити метод, який найбільш повно відповідає існуючим вимогам до систем захисту інформації [1], є одночасно верифікованим, адаптивним, стійким за умов прийнятної обчислювальної складності – апарат нечіткої логіки.

Поряд з цим, застосування описаного підходу вимагає врахування динаміки психоемоційних станів користувача на етапі побудови його профілю, оскільки людині може бути властива множина станів в залежності від впливу зовнішніх факторів (самопочуття, стрес, бойові дії), які безпосередньо впливають на поведінку [5, 6].

У роботах [7-9] дане завдання справедливо намагаються вирішити шляхом застосування математичного апарату теорії нечітких множин, проте представлені підходи застосування нечіткого класифікатора не дозволяють достатньо повно вирішити вищевказану проблематику (контролювати динаміку поведінки користувача вдається лише частково, завдяки властивості аналізу параметрів профілю в умовах неповноти та нечіткості інформації).

У зв'язку з цим, виникає актуальне наукове завдання підвищення ефективності існуючих механізмів автентифікації систем контролю доступу на основі поєднання переваг підходів поведінкової біометрії та нечіткої логіки.

Метою статті є підвищення ефективності процедури автентифікації користувача ІС ОВУ шляхом розробки моделі нечіткої автентифікації на основі поведінкової біометрії.

ОСНОВНА ЧАСТИНА

Для підвищення ефективності процедури встановлення особи користувача ІС на основі визначення автентичності пред'явленого ним ідентифікатора пропонується виконання наступних часткових завдань:

- побудувати профіль поведінки користувача під час роботи з ІС;
- побудувати нечіткий класифікатор для визначення відповідності поведінки користувача ІС існуючому профілю.

Побудова профілю поведінки користувача ІС на основі запропонованого підходу окрім визначення множини досліджуваних ознак клавіатурного почерку (кількість пальців, задіяних під час набору тексту; швидкість друку – кількість введених символів розділена на час друку; тривалість натискання клавіш; час між натисканнями клавіш; динаміка друку – час між натисканням клавіш і часом їх утримання; сила натискання клавіш; частота виникнення помилок при введенні; частота використання певних комбінацій клавіш; використання основної або додаткової частини клавіатури), на основі якої формується множина правил поведінки, передбачає генерацію нових ознак засобами ефективного підходу машинного навчання – Feature Engineering (автоматизованої генерації нових ознак на основі існуючих) [11-13].

Вибір даного підходу обумовлено збільшенням показників точності встановлення відповідності на аналогічних наборах даних [12].

Так, з множини існуючих досліджуваних ознак X генеруються нові ознаки x_j^{fe} на основі виконання операцій над ними (логарифмування, піднесення до степеню), утворюючи тим самим нову додаткову множину досліджуваних ознак X_{fe} із множини усіх можливих ознак X_u:

$$X = \{x_1, \dots, x_i, \dots, x_n\}, i = \overline{1,n}, \rightarrow X_{fe} = \{x_1^{fe}, \dots, x_j^{fe}, \dots x_m^{fe}\}, j = \overline{1,m}, x \in X_u \quad . \quad (1)$$

Такий підхід хоч і дозволяє збільшити точність встановлення особистості користувача на основі поєднання досліджуваних ознак множин X та X_{fe}, проте не вирішує завдання врахування динаміки психоемоційного стану людини.

У контексті викладеного, побудову профіля користувача доцільно здійснювати на основі знайдених поведінкових частих залежностей зі статистичного набору даних його роботи з ІС за клавіатурою, оскільки саме такий підхід дозволить визначити притаманні конкретному користувачу підсвідомі поведінкові риси, присутні у різних психоемоційних станах, що у свою чергу дозволить позбутися множини опису станів кожного облікового запису та зменшити кількість

хибних спрацьовувань системою контролю доступу у процесі автентифікації користувача.

Реалізація механізму інженерії закономірностей у даному випадку передбачає застосування алгоритмів пошуку частих залежностей, асоціативних правил або закономірних послідовностей (ланцюгів подій, пов'язаних у часі) у статистичних наборах даних. Формування статистичних наборів передбачає накопичення даних за певний період часу на основі вищевказаних досліджуваних параметрів для подальшого аналізу клавіатурного почерку (стилю) користувача [14]. Ознаки $x_i^{fe} \in X_{fe}$ – представляють собою знайдені залежності між ознаками $x_i \in X$.

Аналітичний опис профілю користувача можна представити у вигляді:

$$X_{user_k} = X \cup X_{fe} = \left\{x_1, \dots, x_i, \dots, x_n, \dots, x_{1_k}^{fe}, \dots, x_{j_k}^{fe}, \dots x_{m_k}^{fe}\right\}, i = \overline{1,n}, j = \overline{1,m}, \in X_u \quad , \tag{2}$$

де X – множина параметрів досліджуваного клавіатурного почерку, X_{fe} – множина виявлених кореляцій досліджуваних параметрів конкретного користувача, k – кількість користувачів ІС, n – кількість інформативних ознак множини X, m – кількість інформативних ознак множини X_{fe}.

Побудова нечіткого класифікатора передбачає зведення завдання автентифікації користувача протягом усієї сесії роботи з ІС до ітераційного визначення рівня відповідності його поведінці попередньо побудованого профілю (2) під час використання клавіатури на основі аналізу множини вищевказаних досліджуваних ознак множини X_{user} засобами математичного апарату теорії нечітких множин.

Нечіткий класифікатор для визначення відповідності поведінки користувача ІС існуючому профілю передбачає наявність нечітких продукційних правил у базі знань, отриманих із елементів множини X_{user} у якості вхідних лінгвістичних змінних, логічного оператора «І» та ідентифікатора користувача у якості вихідної лінгвістичної змінної.

Для формулювання та вирішення задачі нечіткої автентифікації користувача ІС ОВУ на основі поведінкової біометрії пропонується підхід, згідно з яким процес прийняття рішення системою контролю доступу про автентичність користувача у режимі реального часу, і як наслідок встановлення факту легітимного або несанкціонованого доступу (на основі вищеописаних інформативних ознак множини X_{user}) за умови наявності причинно-наслідкової залежності [10]:

$$y = f_y\left\{x_1, \dots, x_i, \dots, x_n, \dots, x_{1_k}^{fe}, \dots, x_{j_k}^{fe}, \dots x_{m_k}^{fe}\right\}, i = \overline{1,n}, j = \overline{1,m} \quad . \tag{3}$$

зводиться до задачі знаходження виразу після упорядкування елементів множини X_{user}:

$$X_{user}{}^* = (x_1^*, \dots, x_i^*, \dots, x_n^*) \to y = d_j \in D = \left(d_1^*, \dots, d_j^*, \dots, d_m^*\right), i = \overline{1,n}, j = \overline{1,m} \quad . \tag{4}$$

В якості досліджуваного об'єкта, для якого буде визначатись поняття несанкціонованого доступу до ІС буде виступати профіль користувача, побудований на основі (2).

Для встановлення залежності (3) між аналізованим профілем користувача та результатом аналізу, вхідні і вихідну змінні розглядаємо як лінгвістичні [17], що задані в наступних універсальних множинах для кількісних параметрів:

$$X_i = \underline{x_i}, \overline{x_i}, i = \overline{1,n}; \tag{5}$$

$$Y = \left[\underline{y}, \overline{y}\right], \tag{6}$$

де X_i – множина всіх можливих параметрів досліджуваного клавіатурного почерку, Y – множина усіх зареєстрованих користувачів, $\underline{x_i}(\overline{x_i})$ та $\left(\underline{y}, \overline{y}\right)$ – нижні (верхні) границі значень вхідних та вихідної змінної якісних параметрів:

$$X_i = \left\{v_i^1, v_i^2, \dots, v_i^{q_i}\right\}, i = \overline{1,n}; \tag{7}$$

$$Y = \{y^1, y^2, \dots, y^{q_m}\}, \tag{8}$$

де $v_i^1\left(v_i^{q_i}\right)$ та $y^1(y^{q_m})$ – бальна оцінка, що

відповідає мінімальному (максимальному) значенню x_i/y, де $q_i, i=\overline{1,n}$ та q_m – потужності множин (6) і (7).

Для оцінки лінгвістичних змінних $x_i, i=\overline{1,n}$ та y використовуються якісні терми з наступних терм-множин:

$A_i=\{a_i^1, a_i^2, \ldots, a_i^{l_i}\}$ – терм-множина $x_i, i=\overline{1,n}$,

$D=\{d_1, d_2, \ldots, d_m\}$ – терм-множина y,

де a_i^p – p-й лінгвістичний терм $x_i, p=\overline{1,l_i}$, $i=\overline{1,n}$; d_j – j-й лінгвістичний терм y, m – кількість можливих значень змінної y у встановленій області її значень.

Оскільки лінгвістичні терми $a_i^p \in A_i$, $d_j \in D$, $p=\overline{1,l_i}, i=\overline{1,n}$, $j=\overline{1,m}$ можливо представити як нечіткі множини a_i^p і d_j на основі досвіду у [10,11], що задані на універсальних множинах X_i і Y та визначаються виразами (5) – (6), то у випадку наявності кількісних $x_i, i=\overline{1,n}$ та y вони будуть визначатися співвідношеннями:

$$a_i^p=\int_{\underline{x_i}}^{\overline{x_i}} \mu^{a_i^p}(x_i)/x_i \quad ; \tag{9}$$

$$d_j=\int_{\underline{y}}^{\overline{y}} \mu^{d_j}(y)/y \quad , \tag{10}$$

де $\mu^{a_i^p}(x_i)$ – функція належності значення $x_i \in \left[\underline{x_i}, \overline{x_i}\right]$ терму $a_i^p \in A_i, p=\overline{1,l_i}, i=\overline{1,n}$;

$\mu^{d_j}(y)$ – функція належності значення вихідної змінної $y \in \left[\underline{y}, \overline{y}\right]$ терму $d_j \in D, j=\overline{1,m}$.

У випадку наявності якісних $x_i, i=\overline{1,u}$ та y нечіткі множини a_i^p і d_j будуть визначатися співвідношеннями:

$$a_i^p=\sum_{k=1}^{q_i} \mu^{a_i^p}\left(v_i^k\right)/v_i^k; \tag{11}$$

$$d_j=\sum_{r=1}^{q_m} \mu^{d_j}\left(y^r\right)/y^r \quad , \tag{12}$$

де $\mu^{a_i^p}\left(v_i^k\right)$ – ступінь належності елемента $v_i^k \in U_i$ терму $a_i^p \in A_i$, $p=\overline{1,l_i}, i=\overline{1,n}$, $k=\overline{1,q_i}$; $\mu^{d_j}\left(y^r\right)$ – ступінь належності елемента $y^r \in Y$ терму $d_j \in D, j=\overline{1,m}$.

Лінгвістична оцінка усіх (вхідних/вихідної) змінних і необхідних для їх формалізації функцій приналежності є першим етапом побудови нечіткої моделі автентифікації користувача ІС ОВУ на основі поведінкової біометрії, оскільки дозволяє визначити тільки показник їх належності терму відповідної терм множини.

Для реалізації наступного етапу для нечіткої системи логічного виводу необхідно інтерпретувати отримані на основі (2) асоціативні правила з множини досліджуваних параметрів (вхідних лінгвістичних змінних) у нечіткі продукційні правила.

Так, шукане відношення (3) формалізується у вигляді системи нечітких логічних тверджень типу „ЯКЩО-ТО, ІНАКШЕ”:

ЯКЩО $(x_1=a_1^{11})$ І $(x_2=a_2^{11})$ І…І $(x_n=a_n^{11})$
АБО
$(x_1=a_1^{12})$ І $(x_2=a_2^{12})$ І…І $(x_n=a_n^{12})$ АБО
$(x_1=a_1^{1k_1})$ І $(x_2=a_2^{1k_1})$ І…І $(x_n=a_n^{1k_1})$
ТО
$y=d_1$, ІНАКШЕ
ЯКЩО $(x_1=a_1^{21})$ І $(x_2=a_2^{21})$ І…І $(x_n=a_n^{21})$
АБО
$(x_1=a_1^{22})$ І $(x_2=a_2^{22})$ І…І $(x_n=a_n^{22})$ АБО
$(x_1=a_1^{2k_2})$ І $(x_2=a_2^{2k_2})$ І…І $(x_n=a_n^{2k_2})$ ТО
$y=d_2$, ІНАКШЕ
ЯКЩО $(x_1=a_1^{m1})$ І $(x_2=a_2^{m1})$ І…І $(x_n=a_n^{m1})$
АБО
$(x_1=a_1^{m2})$ І $(x_2=a_2^{m2})$ І…І $(x_n=a_n^{m2})$ АБО
$(x_1=a_1^{mk_m})$ І $(x_2=a_2^{mk_m})$ І…І $(x_n=a_n^{mk_m})$ ТО
$y=d_m$.

З використанням операцій $\cup$ (АБО) $\cap$ (І) представлена система логічних висловлювань приводиться до наступного вигляду:

$$\bigcup_{p=1}^{k_j}\left[\bigcap_{i=1}^{u}\left(x_i=a_i^{jp}\right)\right] \rightarrow y=d_j, i=\overline{1,n}, j=\overline{1,m} \tag{13}$$

Таким чином, шукане відношення (3), що встановлює взаємозв'язок між параметрами профілю користувача та відповідними їм користувачами, формалізовано у вигляді системи нечітких логічних висловлювань (13).

Для розрахунку значення функцій належності різних рішень при фіксованих значеннях вхідних змінних, зв'язок між функціями належності вхідного параметра x_i та вектора $\langle x_1^*, x_2^*, \dots, x_n^* \rangle$ рішенню y може бути представлений у вигляді наступних рівнянь:

$$\begin{aligned}
&\mu^{d_1}(x_1, x_2, \dots, x_n) = \mu^{11}(x_1) \wedge \mu^{11}(x_2) \wedge \dots \wedge \mu^{11}(x_n) \vee \\
&\vee \mu^{12}(x_1) \wedge \mu^{12}(x_2) \wedge \dots \wedge \mu^{12}(x_n) \vee \dots \\
&\dots \vee \mu^{1k_1}(x_1) \wedge \mu^{1k_1}(x_2) \wedge \dots \wedge \mu^{1k_1}(x_n), \\
&\mu^{d_2}(x_1, x_2, \dots, x_n) = \mu^{21}(x_1) \wedge \mu^{21}(x_2) \wedge \dots \wedge \mu^{21}(x_n) \vee \\
&\qquad \vee \mu^{22}(x_1) \wedge \\
&\qquad \mu^{22}(x_2) \wedge \dots \wedge \\
&\qquad \mu^{22}(x_n) \vee \dots \\
&\dots \vee \mu^{2k_2}(x_1) \wedge \mu^{2k_2}(x_2) \wedge \dots \wedge \mu^{2k_2}(x_n), \\
&\mu^{d_m}(x_1, x_2, \dots, x_n) = \mu^{m1}(x_1) \wedge \mu^{m1}(x_2) \wedge \dots \wedge \mu^{m1}(x_n) \vee \\
&\vee \mu^{m2}(x_1) \wedge \mu^{m2}(x_2) \wedge \dots \wedge \mu^{m2}(x_n) \vee \dots \\
&\dots \vee \mu^{mk_m}(x_1) \wedge \mu^{mk_m}(x_2) \wedge \dots \wedge \mu^{mk_m}(x_n),
\end{aligned} \tag{14}$$

де $\wedge$ – логічне І, $\vee$ – логічне АБО.

Нечіткі логічні рівняння отримано шляхом заміни в них лінгвістичних термів відповідними функціями належності, а операції $\bigcap$ та $\bigcup$ – на $\wedge$ та $\vee$. В загальному вигляді система нечітких логічних висловлювань про рішення виглядає наступним чином:

$$\mu^{d_j}(x_1, \dots, x_i, \dots, x_n) = \bigvee_{p=1}^{k_j} \left[\bigwedge_{i=1}^{n} \mu^{jp}(x_i) \right], i = \overline{1,n}, j = \overline{1,m} \quad . \tag{15}$$

На основі (15) у якості прийнятого рішення обирається результат з найбільшим значенням функції належності.

Узагальнено функціональне ядро запропонованої моделі представлено на рис. 1.

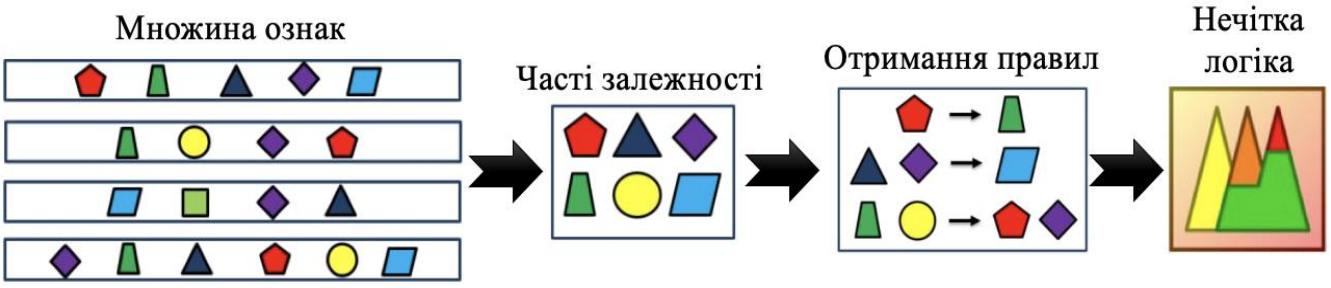

Рис. 1 Функціональне ядро запропонованої моделі

ВИСНОВКИ

Таким чином, розроблено модель нечіткої автентифікації користувача ІС ОВУ на основі поведінкової біометрії, яка на відміну від існуючих, передбачає побудову профіля користувача ІС на основі інженерії поведінкових закономірностей з множини досліджуваних параметрів клавіатурного почерку, які достатньо повно відображають притаманні йому підсвідомі характерні риси під час відтворення досліджуваного процесу, що у свою чергу дозволяє:

- зберегти прийнятну обчислювальну складність на процедуру автентифікації користувача;
- здійснювати прийняття ефективних рішень в умовах неповноти, неточності та нечіткості управляючої інформації;
- доповнити існуючі системи керування доступом властивістю верифікації поточної ситуації щодо процедури автентифікації;
- виявити притаманні конкретному користувачу підсвідомі поведінкові риси, присутні у різних психоемоційних станах, і як наслідок, позбутися множини опису станів кожного облікового запису та зменшити кількість хибних спрацьовувань системою контролю доступу у процесі автентифікації особи;

- підвищити ефективність процедури автентифікації ідентифікованого користувача завдяки властивостям аналізу його поведінки протягом усієї сесії роботи з ІС, що надає можливість виявляти факт зміни користувача в умовах відсутності статичних біометричних даних, паролю (фізичного токену), які можливо використати для компрометації.

Перспективним напрямком подальших наукових досліджень є розробка методики автентифікації користувачів ІС, в основу якої буде імплементовано запропоновану у статті модель.

ЛІТЕРАТУРА

[1] Фесьоха В. В., Фесьоха Н. О., Доброштан О. Д. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення. *Збірник наукових праць ВІТІ.* 2020. №3. С. 129-136.

[2] 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, 5 квіт. 2017 р. Бережани, 2017. С. 236-246.

[3] Мороз А.О. Биометрические технологии идентификации человека. Обзор систем. *Математические машины и системы*. 2011. № 1. С. 39–45.

[4] Брагина Е. К., Соколов С. С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития. *Вестник АГТУ*. 2016. №1. С. 40–43.

[5] Чалая Л. Э. Сравнительный анализ методов аутентификации пользователей компьютерных систем по клавиатурному почерку. *Системи обробки інформації*. 2008. №1. С. 108–116.

[6] Тушканов Е. В., Гатчин Ю. А., Сухостат В. В. Метод аутентификации при использовании клавиатурного почерка на основе нечеткой логики. *Научное обозрение*. 2014. №12. С. 171–175.

[7] Аникин И. В., Анисимова Э. С. Распознавание динамической рукописной подписи на основе нечёткой логики. *Информатика, вычислительная техника и управление. 2016. С. 48-64. URL:* https://cyberleninka.ru/article/n/raspoznavanie-dinamicheskoy-rukopisnoy-podpisi-na-osnove-nechyotkoy-logiki/viewer.

[8] Полякова А.С. *Коллективные методы интеллектуального анализа данных на основе нечеткой логики*: дис. … канд. техн. наук: 05.12.01. Красноярск, 2019. 136 с.

[9] Fesokha V.V., Subach I.Y., Kubrak V.O., Mykytiuk A.V., Korotaiev S.O. Zero-day polymorphic cyberattacks detection using fuzzy inference system. *Austrian Journal of Technical and Natural Sciences: scientific journal*. Vienna, 2020. № 5-6. pp. 8-13.

[10] Ротштейн А. П. *Медицинская диагностика на нечеткой логике*. Континент– ПРИМ. 1996. – 142 с.

[11] Субач І.Ю., В.В. Фесьоха Модель виявлення аномалій в інформаційно – телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу. *Збірник наукових праць ВІТІ*. 2017. № 3. С.158-164.

[12] Искусство Feature Engineering в машинном обучении. URL: https://habr.com/ru/company/mlclass/blog/248129.

[13] Пример Feature Engineering в машинном обучении. URL: https://habr.com/ru/company/mlclass/blog/249759.

[14] Feature Generation I: Data Transformation and Dimensionality Reduction. URL: https://www.sciencedirect.com/topics/computer-science/feature-generation.

[15] Data Mining –интеллектуальный анализ данных URL: http://www.olap.ru/basic/dm2.asp#3.%20Типы%20закономерностей.

МОДЕЛЬ НЕЧЕТКОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ПОВЕДЕНЧЕСКОЙ БИОМЕТРИИ

В статье рассмотрена актуальная научная задача защиты информационных систем сектора критической инфраструктуры от несанкционированного доступа. Предложена модель аутентификации пользователей информационных систем, основанная на использовании поведенческой биометрии и математического аппарата теории нечеткой логики. Суть предложено подхода в первую очередь заключается в построении профиля пользователя системы на основе инженерии поведенческих закономерностей (частых зависимостей) из множества исследуемых параметров, которые достаточно полно отражают присущие ему подсознательные характерные черты во время воспроизведения процесса, подлежащего подлинности. Во вторую очередь, задача нечеткой аутентификации пользователей системы сводится к определению уровня соответствия их поведенческих характеристик существующему профилю на основе анализа множества исследуемых параметров в условиях некоторой нечеткости и неточности управляющей информации. Представленная модель позволяет выявлять присущие конкретному пользователю подсознательные поведенческие черты, присутствующие в разных психоэмоциональных состояниях, в свою очередь позволяет избавиться множества описания состояний каждой учетной записи и уменьшить количество ложных срабатываний в процессе аутентификации

личности, что значительно повышает эффективность кибербезопасности информационных систем сектора критической инфраструктуры.

Ключевые слова: несанкционированный доступ, информационные системы, биометрическая аутентификация, инженерия закономерностей, нечеткая логика.

FUZZY AUTHENTICATION MODEL FOR USERS OF SPECIAL PURPOSE INFORMATION SYSTEMS BASED ON BEHAVIORAL BIOMETRICS

The article deals with the urgent scientific problem of protecting information systems of the critical infrastructure sector from unauthorized access. The author proposes a model for the authentication of users of information systems based on the use of behavioral biometrics and the mathematical apparatus of the theory of fuzzy logic. The essence of the proposed approach is, first of all, to construct a user profile of the system based on the engineering of behavioral patterns (frequent dependencies) from a set of investigated parameters, which quite fully reflect its inherent subconscious characteristics during the reproduction of the process to be authenticated. Secondly, the problem of fuzzy authentication of system users is reduced to determining the level of compliance of their behavioral characteristics with the existing profile based on the analysis of a set of investigated parameters in conditions of some fuzziness and inaccuracy of control information. The presented model makes it possible to identify subconscious behavioral traits inherent in a particular user that are present in different psychoemotional states, in turn, it allows you to get rid of many descriptions of the states of each account and reduce the number of false positives in the process of identity authentication, which significantly increases the efficiency of cybersecurity of information systems in the critical infrastructure sector.

Keywords: unauthorized access, information systems, biometric authentication, engineering of laws, fuzzy logic.

Фесьоха Віталій Вікторович – доктор філософії у галузі Інформаційні технології, старший викладач кафедри Комп'ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут.
E-mail: vitaliifesokha@gmail.com.
Orcid ID: 0000-0001-6612-1970.

Фесёха Виталий Викторович – доктор философии в области Информационные технологии, старший преподаватель кафедры Компьютерных информационных технологий Военного института телекоммуникаций и информатизации имени Героев Крут.

Vitalii Fesokha – PhD in Information Technologies, Senior lecturer of the Department of Computer Information Technologies of the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty.

Фесьоха Надія Олександрівна – викладач кафедри Комп'ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут.
E-mail: nadya_viti@i.ua.
Orcid ID: 0000-0002-9797-5589.

Фесёха Надежда Александровна – преподаватель кафедры Компьютерных информационных технологий Военного института телекоммуникаций и информатизации имени Героев Крут.

Nadiia Fesokha – lecturer of the Department of Computer Information Technologies of the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty.

DOI: 10.18372/2410-7840.23.15431
УДК 004.056.53

АНАЛІЗ ДОСЛІДЖЕНЬ З РОЗГОРТАННЯ DNSSEC В ІНТЕРНЕТІ

Тетяна Приходько

Система доменних імен є невід'ємною частиною адресації в мережі Інтернет. Недоліки в реалізації протоколу DNS дозволяють використовувати його для зловмисних дій, підчас яких може бути порушено цілісність і доступність даних при обміні даними між DNS-клієнтом та DNS-сервером. Для захисту цілісності при обміні даними DNS призначена технологія DNSSEC, яка запобігає отриманню фальшивих даних DNS-клієнтами. В статті досліджується сучасний стан використання технології розширення безпеки системи доменних імен DNSSEC та розглядаються питання попиту на вивчення показників з розгортання протоколу DNSSEC і проблеми, що наразі існують з отриманням максимально повного уявлення про масштаби розгортання даного протоколу в Інтернеті. DNSSEC дозволяє власникам доменних імен використовувати метод цифрового підпису інформації, яку вони вносять в систему доменних імен DNS. Це забезпечує захист споживачів, так як дані DNS, які піддалися спотворенню, випадково або зі злим умислом, до них не доходять. Питання, яке вирішує DNSSEC: Чи можна довірятися відповіді DNS? З 2010 року була забезпечена можливість використання підпису DNSSEC на самому верхньому рівні DNS,