

## БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ НА ОСНОВІ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ

С.О. ЄНГАЛИЧЕВ, С.Г. СЕМЕНОВ

У статті проведена оцінка стабільності клавіатурного почерку користувача. Розроблена імітаційна модель системи автентифікації користувачів на основі клавіатурного почерку. Проведені дослідження і виявлені закономірності в клавіатурному почерку різних користувачів.

*Ключові слова:* біометричні системи автентифікації, клавіатурний почерк, імітаційна модель.

**Актуальність.** Аналіз сучасного українського ринку технічних засобів забезпечення безпеки показав, що, в розвитку індустрії безпеки сьогодні позначився новий етап. На загальному фоні ринку, що стабілізувався, найдинамічніше продовжують розвиватися сучасні системи автентифікації особи і захисту інформації. Особливу увагу привертають до себе біометричні засоби захисту інформації (БСЗІ), що пояснюється їх високою надійністю автентифікації і досягнутим останнім часом значним зниженням їх вартості.

В теперішній час існує безліч методів біометричної автентифікації користувачів комп'ютерних систем, які можна розділити на дві великі групи: статичні і динамічні [1-4]. Класифікація методів біометричної автентифікації представлена на рис. 1.



Рис. 1. Класифікація методів біометричної автентифікації користувачів

Аналіз методів біометричної автентифікації показав, що статичні методи, ґрунтовані на характеристиках людини, тобто унікальній властивості, даній йому від народження і невід'ємному від нього, разом з достоїнствами (висока точність автентифікації, висока швидкість реакції та ін.) мають ряд недоліків (висока вартість устаткування, витратних матеріалів і обслуговування) [1, 3]. Методи динамічної автентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, т. е. побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Аналіз методів динамічної автентифікації показав, що, незважаючи на ряд

їх недоліків (висока імовірність помилки автентифікації і неправдивих спрацьовувань системи безпеки), в силу простоти і доступності вони залишаються затребуваними в секторі невеликих установ, підприємств і організацій [1, 2].

**Аналіз джерел** [1-4] показав, що серед динамічних методів біометричної автентифікації ряд авторів виділяє методи автентифікації користувача по клавіатурному почерку. Пов'язано це в основному з тим, що клавіатурний почерк користувача має певну стабільність, що дозволяє з високою імовірністю правильно автентифікувати користувача, працюючого з клавіатурою.

**Основна частина.** Проведені дослідження показали, що автентифікація користувачів в цих методах, як правило, ґрунтується на статистичних методах обробки початкових даних і формуванні вихідного вектору, який є ідентифікатором цього користувача. В якості початкових даних використовують часові інтервали між натисненням клавіш на клавіатурі і час їх утримання. При цьому часові інтервали між натисненням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою – різкий удар або плавне натиснення.

Дослідження показали, що автентифікація користувача по клавіатурному почерку можлива наступними способами: по набору ключової фрази; по набору довільного тексту.

Обидва способи мають на увазі два режими роботи: навчання; автентифікація.

На етапі навчання користувач вводить деяке число раз запропоновані йому тестові фрази. При цьому розраховуються і запам'ятовуються еталонні характеристики цього користувача. На етапі автентифікації розраховані оцінки порівнюються з еталонними, на підставі чого робиться висновок про збіг або неспівпадання параметрів клавіатурного почерку.

Еталонні характеристики користувача, отримані на етапі навчання системи, дозволяють зробити висновки про міру стабільності клавіатурного почерку користувача і визначити довірчий інтервал розкиду параметрів для подальшої автентифікації користувача. Щоб уникнути дискредитації роботи системи можливо відсівати користувачів, клавіатурний почерк яких не має необхідної «стабільності» [1, 2, 4]. Для цього можна користуватися даними, представленими в табл. 1.

Оценка стабильности клавиатурного почерка пользователя

Помилки, %	Аритмічність, %	Швидкість, зн./мін	Характеристика перекриттів		Оцінка
			Число перекриттів, %	Використовуване число пальців	
менш 2	менш 10	більше 200	більше 50	все	відмінно
менш 4	менш 15	більше 150	більше 30	більшість	добре
менш 8	менш 20	більше 100	більше 10	декілька	задов.
більше 8	більше 20	менш 100	менш 10	по одному	неуд.

Розробимо імітаційну модель клавіатурного введення інформації і проведемо на її основі дослідження біометричних закономірностей користувачів.

Імітаційна модель дозволяє аналізувати вектори часів утримань клавіш, а так само інтервалів часу між натисненнями клавіш.

Експеримент полягає у введенні з клавіатури спеціально підбраної кількості слів і словосполучень з реєстрацією часів утримання клавішею для покриття усього вектору часів утримань клавіш, а також з реєстрацією часів міжсимвольних інтервалів, які фіксуються у відповідній матриці. Цей набір слів кожен користувач набирає в різний час доби (вдень і уночі).

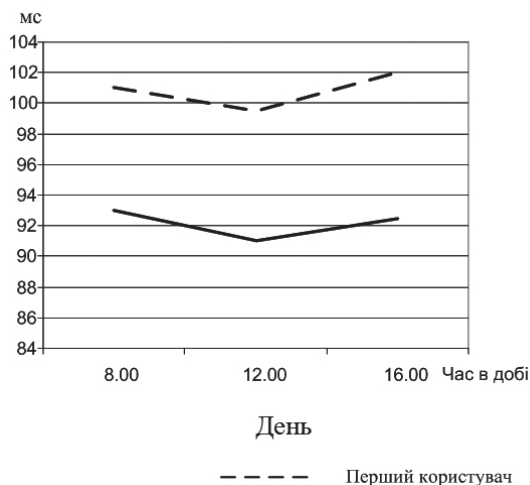
Проаналізуємо дві найбільш типових біометричних характеристики двох користувачів, які в цілому відбивають основні особливості роботи користувачів в різний час доби.

Динаміка зміни середнього часу утримання клавіш користувачами в різний час доби представлена на рис. 2.

Аналіз кривих зміни середнього часу утримання клавіш користувачами в різний час доби показав незначне (до 1,02 разів) зменшення часу натиснення клавіш в середині робочого дня, і збільшення цього часу до 1,05 разу о 5.00 годині ранку при безперервній роботі в нічний час.

Криві зміни середніх інтервалів часу між натисненнями клавіш в різний час доби представлені на рис. 3. (а – перший користувач, б – другий користувач).

Криві рис. 3. так само ілюструють результати процесу аутентифікації користувача по різниці



змін середніх інтервалів часу між натисненнями клавіш (крива Average). Як можна помітити з рисунку висунене припущення про стабільність клавіатурного почерку користувача в цілому підтверджується (відхилення даних верифікацій легального користувача тільки в 5% випадків перевищують 70%). Приведені характеристики говорять також про ритм роботи кожного користувача з клавіатурою. Окрім цього, можна виявити і ще одну важливу закономірність. У ряді випадків абстрактний користувач (тобто деякий образ усередненого користувача) стабільніше працює вдень в порівнянні з нічним часом доби. Так в прикладі, представленому на рис. 3. перший користувач «стабільніше» працює вдень майже в 1,3 разу, другий користувач в 1,051 рази. Дослідження показали, що і цей факт необхідно використати проектувальникам при розробці систем біометричної автентифікації.

**Висновки.** На основі імітаційної моделі системи біометричної автентифікації користувачів були проведені дослідження клавіатурного почерку окремих користувачів в денний і нічний час доби. Були виявлені ряд закономірностей, що підтверджують гіпотезу про можливість динамічної біометричної автентифікації користувачів по клавіатурному почерку. Крім того, результати досліджень показали можливість використання запропонованої моделі в системах захисту інформаційно-обчислювальних комплексів від несанкціонованого доступу.

**Література**

[1] Брюхомицкий Ю.А. Исследование биометрических систем динамической аутентификации пользова-

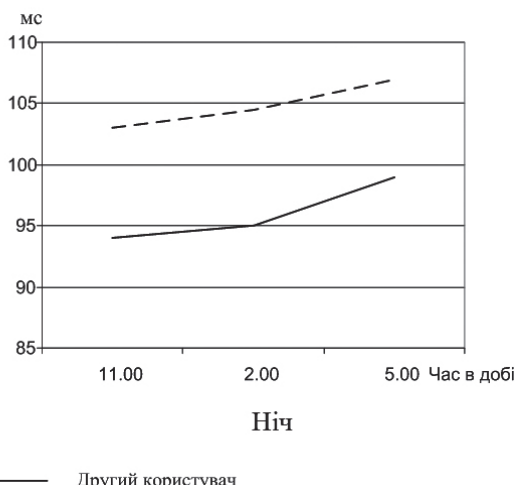


Рис. 2. Криві зміни середнього часу утримання клавіш користувачами в різний час доби

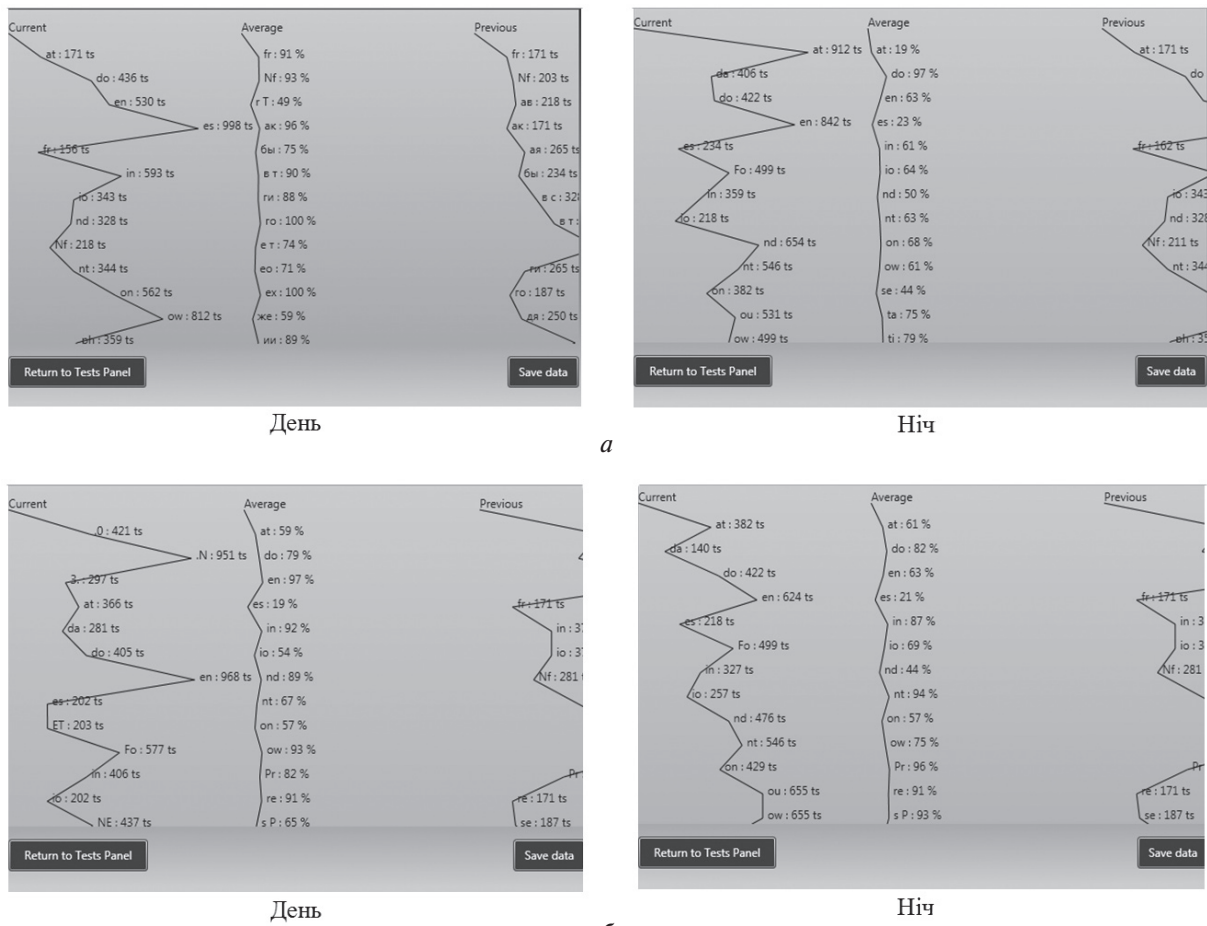


Рис. 3. Криві зміни середніх інтервалів часу між натисненнями клавіш в різний час доби

телей ПК по рукописному и клавиатурному почеркам / Ю.А. Брюхомицкий, М.Н. Казарин – Таганрог: Изд-во ТРТУ, 2004. – 38 с.

- [2] *Кобиелус Д.* Информационная безопасность: идентификация и аутентификация / Джеймс Кобиелус – М.: Связь, 1997. – 252 с.
- [3] *Карабутов Н.Н.* Структурная идентификация систем: анализ динамических структур / Н.Н.Карабутов. – М.: МГИУ, 2008. – 160 с.
- [4] *Расторгуев С.П.* Программные методы защиты информации в компьютерах и сетях / С.П. Расторгуев – М.: Изд-во Агентства «Яхтсмен», 1993. 188 с.

Поступила в редколлегию 24.04.2012



**Семенов Сергій Геннадійович**, к.т.н. доцент кафедри обчислювальної техніки і програмування, Національний Технічний університет «ХПІ». Галузь наукових інтересів: Захист інформації в інформаційно-телекомунікаційних системах.



**Єнгалічев Сергій Олександрович**, магістр, Харківський національний університет радіоелектроніки. Галузь наукових інтересів: Захист інформації в комп'ютерних системах.

УДК 621.34

**Биометрическая аутентификация на основе анализа клавиатурного почерка** / С.А.Енгалычев, С.Г. Семенов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 309–311.

В статье проведенная оценка стабильности клавиатурного почерка пользователя. Разработана имитационная модель системы аутентификации пользователей на основе клавиатурного почерка. Проведенные исследования и выявленные закономерности в клавиатурном почерке различных пользователей.

*Ключевые слова:* биометрические системы аутентификации, клавиатурный почерк, имитационная модель

Табл. 01. Ил.02. Библиогр.: 04 назв.

UDC 621.34

**Biometric authentication on the basis of analysis of keyboard handwriting** / S.A. Engalychev, S.G. Semenov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 309–311.

Estimation of the stability of a user keyboard handwriting is conducted in the paper. A simulation model of a user authentication system on the keyboard handwriting basis is developed. Research is done and regularities in different users' keyboard handwriting are revealed.

*Keywords:* biometric systems of authentication, keyboard handwriting, simulation model.

Tab. 01. Fig. 03. Ref.: 04 items.