

# **ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ КЛАВІАТУРНОГО ТА КУРСОРНОГО ПОЧЕРКУ ДЛЯ ВИРІШЕННЯ ЗАДАЧ ІДЕНТИФІКАЦІЇ СТУДЕНТІВ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ**

Зозуля О.С.

Науковий керівник – к.т.н., доц. Горелов Д.Ю.

Харківський національний університет радіоелектроніки  
(61166, Харків, пр. Науки, 14, навчально-наукова лабораторія «Систем  
технічного захисту інформації (відеоспостереження, охоронні сигналізації  
і контроль доступу)», тел. (057) 702-14-78.

The objective of the work is to research the effectiveness of the background keyboard and mouse monitoring applications in the automatically-controlled distance education systems.

Однією з ключових проблем дистанційного навчання є забезпечення спостереження за контрольними заходами (тестами, екзаменами). У більшості сучасних систем дистанційної освіти цю задачу досить успішно вирішує система прокторингу, тобто віддаленого відстеження поведінки слухача online-курсу під час складання іспиту спеціально навченими викладачами (прокторами). Однак даний метод контролю має свої обмеження, і насамперед низьку пропускну здатність. Крім того, актуальним є питання про захист особистих даних користувача. Вирішенням зазначених проблем бачиться розвиток автоматизації ідентифікації особистості у процесі проведення контрольних заходів – автопрокторингових системах. У якості ідентифікатора можуть застосовуватися не тільки контрольна пара логін пароль, але й біометричні характеристики людини.

На даний момент метод біометричної ідентифікації вбачається найбільш ефективним, оскільки мінімізує можливість здійснення обману або підробки з боку слухача online-курсу, а також працює на контроль нормативності поведінки на екзамені, а саме забезпечують захист від наступних загроз достовірності результатів контролю знань. Для розв'язання задачі розпізнавання користувачів у системах ДН необхідно проводити ідентифікацію не тільки в момент входу користувача в систему, але й регулярно з деякою періодичністю протягом усього сеансу користування системою. Таким чином, слід використовувати біометричні технології, які забезпечують можливість неперервної та непомітної для користувача ідентифікації. Останній вимозі відповідають методи розпізнавання за клавіатурним та курсорним почерком користувача.

Клавіатурний почерк – унікальний стиль роботи на клавіатурі, що залежить від таких параметрів як: кількість пальців, задіяних під час набору тексту; тривалість натискання клавіш; час між натисканнями клавіш; використання основної або додаткової частини клавіатури; характер здвоєних або строєних натискань; улюблені комбінації гарячих клавіш і т.д. Курсорний

почерк описує особливості роботи з комп'ютерною мишею за допомогою параметрів взаємодії з маніпулятором на рівні інтерфейсу (динаміка переміщення курсору) і параметрів взаємодії з маніпулятором як з фізичним об'єктом (тривалість натискання клавіш миші). Перевагами даних методів ідентифікації є дешевизна, простота реалізації й впровадження (реалізація винятково програмна); можливість повністю легальної схованої ідентифікації протягом усього сеансу користування; простота інтеграції в мультимодальні біометричні системи (клавіатурний почерк плюс голос, клавіатурний почерк плюс геометрія обличчя і т.д.).

Окрім успішного вирішення задачі ідентифікації студентів під час контролю знань методи розпізнавання за клавіатурним та курсорним почерком також дозволяють підвищити інформаційну безпеку систем дистанційного навчання шляхом захисту від наступних загроз.

Для захисту від загрози підміни користувача можливе використання методу ідентифікації за клавіатурним почерком або більш складний метод мультимодальної ідентифікації за інформаційним почерком – клавіатура плюс комп'ютерна миша.

Для захисту від загрози використання програмних ботів і скриптів можливе використання методу ідентифікації за інформаційним почерком. Проблема використання програмного бота, що автоматично вставляє відповіді у відповідні вікна, вирішується, наприклад, за перевіркою на текст, який було вставлено, – шаблон клавіатурного почерку порожній або занадто малий у порівнянні з кількістю символів у тексті. Для захисту від скриптів, які безпосередньо взаємодіють з елементами web-сторінки, можливе використання динаміки курсору мишки, тобто необхідно провести аналогічну перевірку на «повноту шаблону почерку» – якщо всі рухи миші проводилися миттєво, то необхідно відмовити в авторизації.

Для захисту від загрози використання лекцій і електронних довідників під час виконання тестів і завдань у web-орієнтованій системі навчання можна відслідковувати наступні параметри: чи розгорнуто вікно браузера на повний екран; чи є активною сторінка браузера з іспитом; чи використовує студент клавіатуру або мишу в момент, коли вікно браузера є активним, а сторінка з іспитом ні; чи відрізняється середній час на одну відповідь від аналогічного, який затрачував студент впродовж поточних контролів знань.

#### **ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ:**

1. Sinytsa YU.O., “Authentication subjects by keystroke dynamics using digraphs”, International conference Internet technologies and computer programming mobile systems, 2013, pp. 167-168.4. Md Liakat Ali, John V. Monaco, Charles C. Tappert, Meikang Qiu. Keystroke Biometric Systems for User Authentication. Journal of Signal Processing Systems, vol. 86, pp.175-190, 2017. 2. V.O. Aliksieiev, YU.O. Sinytsa, D.YU. Gorelov. “Modified digraphs method in the problem of authenticating users using keystroke dynamics”. Ukrainian Information Security Research Journal (Zahist informacii), vol. 18(4), pp. 252-261, 2016.