Додаток А.

Комплект графічних матеріалів

Дослідження інформативних параметрів динаміки системи "користувач-миша" для задач ідентифікації за курсорним почерком

Актуальність теми. Застосовувані на сьогоднішній день засоби розпізнавання користувачів переважно засновані на використанні паролів і (або) спеціалізованих пристроїв (наприклад, смарт-карт). Експлуатація таких систем безпеки має багато недоліків. Найчастіше паролі перехоплюються. Спеціалізовані пристрої викрадаються або підробляються. Виникають ситуації, коли один з користувачів свідомо передає свій пароль сторонній особі. Перевага біометричних систем ідентифікації у порівнянні з традиційними полягає в тому, що використовувана в цих системах біометрична характеристика є невід'ємною частиною особистості, її неможливо втратити, передати, забути.

Останнім часом велика увага приділяється методам біометричної ідентифікації особистості за динамікою підсвідомих рухів рук. Мова йде про виявлену стабільність відпрацьованих рухових навичок людини – клавіатурний та «курсорний» почерки – і можливості її розпізнавання за цією ознакою.

Метою роботи є підвищення інформаційної безпеки комп'ютерних мереж на основі аналізу динаміки системи користувач-комп'ютерна миша.

Для досягнення поставленої мети необхідно розв'язати наступні **задачі**:

1) провести аналіз принципів стабільної динамічної біометрії;

2) провести пошук відкритих датасетів параметрів курсорного почерку та обрати один з них для подальших досліджень;

3) на основі обраного датасету запропонувати інформативні параметри курсорного почерку для створення математичної моделі класифікатора користувачів за динамікою системи «користувач – комп'ютерна миша»;

4) проведення експериментальних досліджень.

Методи ідентифікації користувачів комп'ютерних мереж за інформаційним почерком

Ідентифікація користувачів комп'ютерних мереж за інформаційним почерком – сукупність методів та технологій, направлених на збір максимуму даних з системи, формування з них логічних структур, об'єднаних навколо користувачів, побудова предикативних математичних моделей, ретроспективний аналіз даних та активне використання розподілених систем зберігання даних.

Датасети динаміки системи "користувач-миша", що знаходяться у вільному доступі

1. The Balabit Mouse Challenge DataSet, компанія BalaBit IT Security (Угорщина).
https://github.com/balabit/Mouse-Dynamics-Challenge

2. ISOT Web Interactions (Mouse/Keystroke/Site Actions) Dataset, ISOT Research Lab університету Victoria (Канада).
https://www.uvic.ca/engineering/ece/isot/datasets/

3. Keystroke Free Text and Mouse Movement Coordinate Records, університет штату Нью-Йорк в Баффало (США).
https://cubs.buffalo.edu/research/datasets

4. Four HCI Tasks Dataset, Pace університет (США).
https://bitbucket.org/vmonaco/dataset-four-hci-tasks/src/master/

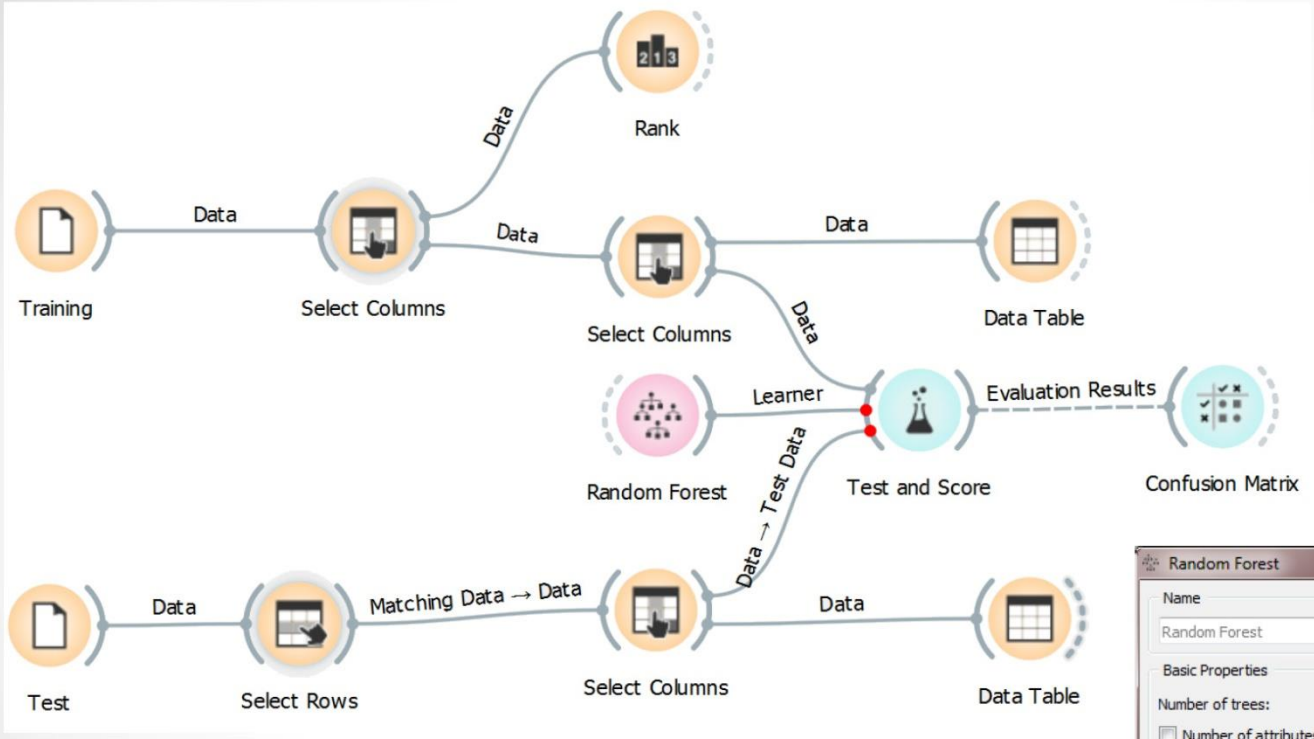
Інформативні параметри динаміки системи "користувач-миша"

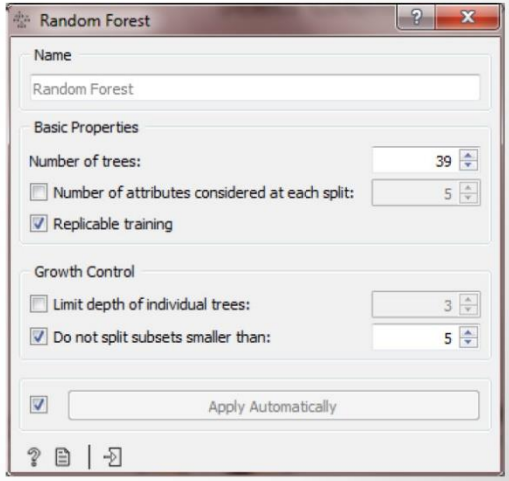
1	type_of_action	Тип дії миші: mouse movement (MM), point click (PC), drag-and-drop (DD)
2	travelled_distance_in pixels	Кількість взаємодій користувача з мишею в залежності від пройденої курсором відстані на екрані монітору впродовж даної дії миші
3	elapsed_time	Час даної дії миші
4	direction of movement	Один з восьми квадрантів, якому належить кут між віссю абсцис та відрізком, що з'єднує дві кінцеві точки траєкторії
5	dist_end_to_end_line	Довжина відрізка між двома кінцевими точками траєкторії
6	straightness	Прямолінійність траєкторії руху курсору миші
7	largest_deviation	Найбільша відстань від траєкторії до відрізка, що з'єднує дві кінцеві точки траєкторії
8	num_points	Кількість взаємодій користувача з мишею, що містяться в даній дії миші
9	sum_of_angles	Кількість кутів, що формують траєкторію курсору миші
10	mean_vx	Середнє значення горизонтальної швидкості курсору мишки впродовж даної дії миші
11	sd_vx	Середньоквадратичне відхилення горизонтальної швидкості курсору мишки впродовж даної дії миші
12	max_vx	Максимальне значення горизонтальної швидкості курсору мишки впродовж даної дії миші
13	min_vx	Мінімальне значення горизонтальної швидкості курсору мишки впродовж даної дії миші
14	mean_vy	Середнє значення вертикальної швидкості курсору мишки впродовж даної дії миші
15	sd_vy	Середньоквадратичне відхилення вертикальної швидкості курсору мишки впродовж даної дії миші
16	max_vy	Максимальне значення вертикальної швидкості курсору мишки впродовж даної дії миші
17	min_vy	Мінімальне значення вертикальної швидкості курсору мишки впродовж даної дії миші
18	mean_v	Середнє значення загальної швидкості курсору мишки впродовж даної дії миші
19	sd_v	Середньоквадратичне відхилення загальної швидкості курсору мишки впродовж даної дії миші
20	max_v	Максимальне значення загальної швидкості курсору мишки впродовж даної дії миші

Інформативні параметри динаміки системи "користувач-миша"

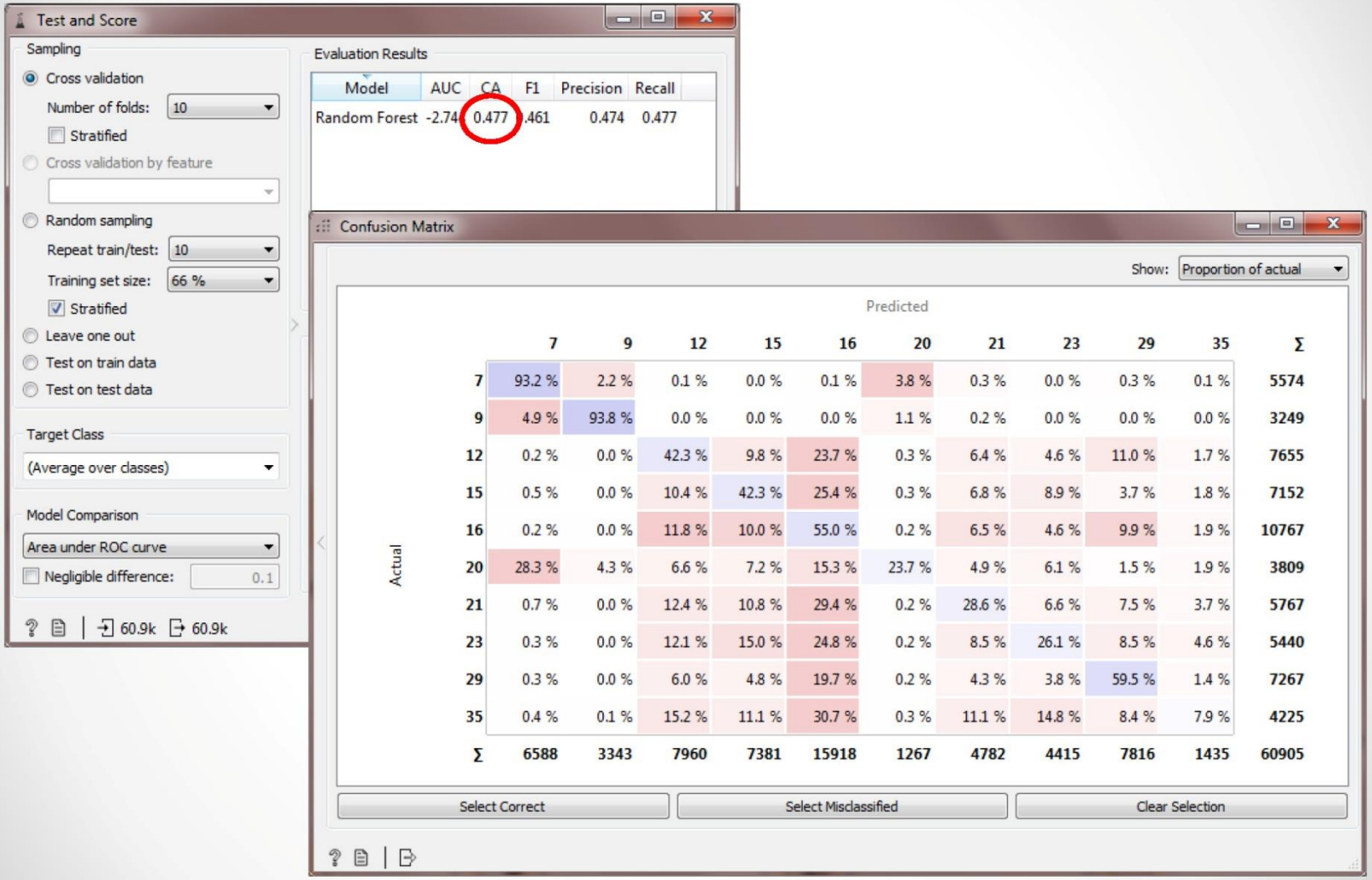
21	min_v	Мінімальне значення загальної швидкості курсору мишки впродовж даної дії миші
22	mean_a	Середнє значення прискорення курсору мишки впродовж даної дії миші
23	sd_a	Середньоквадратичне відхилення прискорення курсору мишки впродовж даної дії миші
24	max_a	Максимальне значення прискорення курсору мишки впродовж даної дії миші
25	min_a	Мінімальне значення прискорення курсору мишки впродовж даної дії миші
26	mean_jerk	Середнє значення швидкості зміни прискорення (ривку) курсору мишки впродовж даної дії миші
27	sd_jerk	Середньоквадратичне відхилення швидкості зміни прискорення (ривку) курсору мишки впродовж даної дії миші
28	max_jerk	Максимальне значення швидкості зміни прискорення (ривку) курсору мишки впродовж даної дії миші
29	min_jerk	Мінімальне значення швидкості зміни прискорення (ривку) курсору мишки впродовж даної дії миші
30	mean_omega	Середнє значення кутової швидкості курсору мишки впродовж даної дії миші
31	sd_omega	Середньоквадратичне відхилення кутової швидкості курсору мишки впродовж даної дії миші
32	max_omega	Максимальне значення кутової швидкості курсору мишки впродовж даної дії миші
33	min_omega	Мінімальне значення кутової швидкості курсору мишки впродовж даної дії миші
34	mean_curv	Середнє значення кривизни траєкторії курсору мишки впродовж даної дії миші
35	sd_curv	Середньоквадратичне відхилення кривизни траєкторії курсору мишки впродовж даної дії миші
36	max_curv	Максимальне значення кривизни траєкторії курсору мишки впродовж даної дії миші
37	min_curv	Мінімальне значення кривизни траєкторії курсору мишки впродовж даної дії миші
38	num_critical_points	Кількість критичних точок на траєкторії руху курсору мишки впродовж даної дії миші
39	a_beg_time	Прискорення курсору мишки впродовж від початку руху до першої точки часу, де прискорення стає від'ємним

Схема експерименту у Orange





Результати проведених досліджень



Результати проведених досліджень

Користувач	Точність класифікації, CA	Відсоток True Positive	Відсоток True Negative
7	96.8	97.9	96.3
9	98.4	97.1	98.8
12	75.9	64.5	83.8
15	76.4	65.9	83.2
16	73.3	78.1	68.6
20	83.1	47.1	95.5
21	76.0	52.2	88.3
23	75.0	46.4	89.1
29	81.7	70.2	98.2
35	74.5	24.7	93.7
Середнє значення	**81.1**	**64.4**	**89.6**

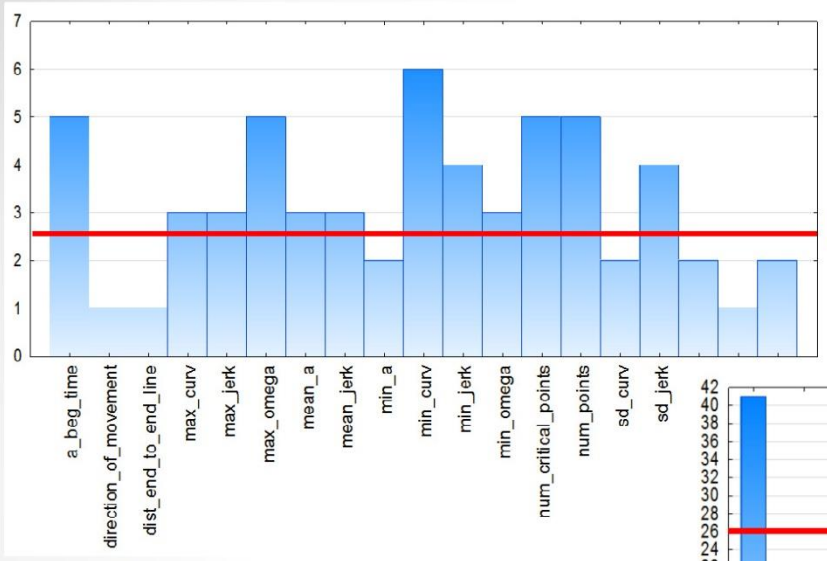
Користувач	Точність класифікації, CA	Відсоток True Positive	Відсоток True Negative
7	92.7	85.6	99.9
9	96.2	89.2	100
12	54.6	10.9	99.4
15	65.5	8.1	97.9
16	39.6	8.3	96.9
20	47.6	13.4	99.9
21	36.7	2.9	99.1
23	53.7	1.6	99.5
29	53.6	39.3	89.4
35	68.0	0.4	99.9
Середнє значення	**60.8**	**26.0**	**98.2**

Результати проведених досліджень

Користувач	Тип дії миши	Точність класифікації, CA	Відсоток True Positive	Відсоток True Negative
7	MM	92.2	82.5	100
9	MM	96.3	88.8	100
12	MM	55.7	9.8	98.8
15	MM	75.2	11.5	97.9
16	MM	44.3	7.9	97.1
20	MM	48.1	4.3	100
21	MM	29.2	4.9	99.0
23	MM	62.7	0.4	100
29	MM	45.8	23.2	92.2
35	MM	63.2	0.0	100
Середнє значення		**61.27**	**23.33**	**98.5**
7	DD	87.2	77.7	98.2
9	DD	87.9	60.5	100
12	DD	60.1	32.3	99.0
15	DD	74.8	26.4	95.5
16	DD	49.2	26.9	89.0
20	DD	56.1	19.3	99.0
21	DD	30.7	8.2	90.5
23	DD	55.8	1.4	100
29	DD	64.6	52.9	92.9
35	DD	63.7	2.5	97.9
Середнє значення		**63.01**	**30.81**	**96.2**

Користувач	Тип дії миши	Точність класифікації, CA	Відсоток True Positive	Відсоток True Negative
7	PC	92.2	85.1	99.8
9	PC	97.0	91.7	100
12	PC	53.8	8.9	99.2
15	PC	61.9	7.9	97.6
16	PC	37.8	7.6	97.4
20	PC	46.0	14.6	100
21	PC	40.5	1.3	99.7
23	PC	51.6	3.3	99.0
29	PC	53.4	39.9	89.0
35	PC	69.9	0.0	100
Середнє значення		**60.41**	**26.03**	**98.17**

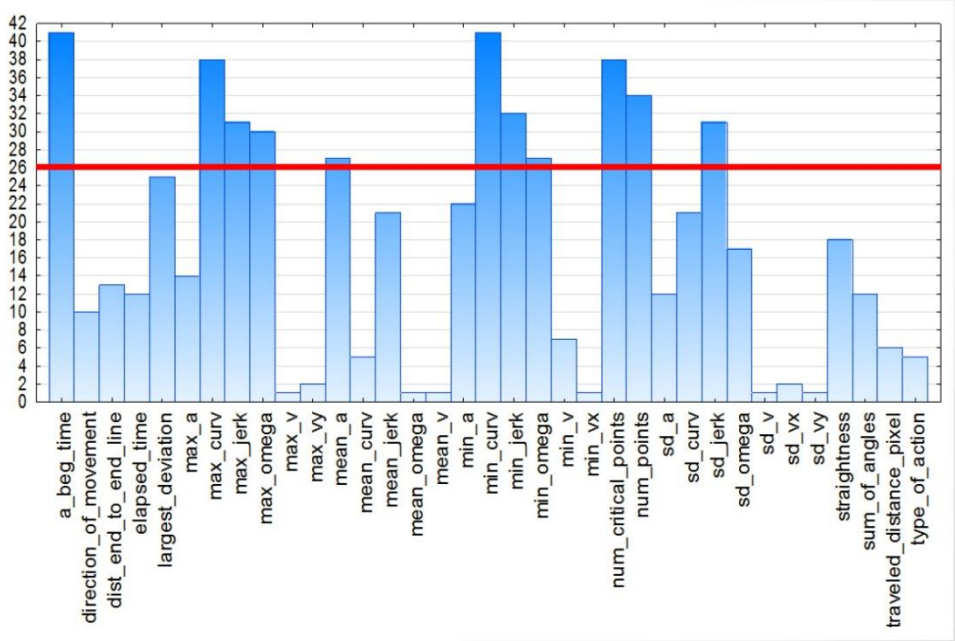
Результати проведених досліджень



1	a_beg_time
2	max_curv
3	max_jerk
4	max_omega
5	mean_a
6	mean_jerk

7	min_curv
8	min_jerk
9	min_omega
10	num_critical_points
11	num_points
12	sd_jerk

1	a_beg_time
2	max_curv
3	max_jerk
4	max_omega
5	mean_a
6	min_curv
7	min_jerk
8	min_omega
9	num_critical_points
10	num_points
11	sd_jerk



Результати проведених досліджень

Користувач	Точність класифікації, CA	Відсоток True Negative	Точність класифікації, CA	Відсоток True Negative
	12 інформативних параметрів		41 інформативний параметр	
7	91.2	99.8	92.7	99.9
9	95.0	100	96.2	100
12	54.8	99.4	54.6	99.4
15	74.1	99.4	65.5	97.9
16	42.0	97.8	39.6	96.9
20	48.3	100	47.6	99.9
21	28.6	99.0	36.7	99.1
23	62.5	100	53.7	99.5
29	44.6	94.8	53.6	89.4
35	63.1	99.9	68.0	99.9
Середнє значення	**60.4**	**99.0**	**60.8**	**98.2**

Висновки

1. Одночасне виконання вимог по безперервності й зручності використання в комп'ютерних мережах не може забезпечити ніякий спосіб ідентифікації, крім динамічного. Крім того, динамічна біометрія дешевше статичної, так як може використовувати стандартні пристрої введення інформації.

2. Аутентифікація користувачів за курсорним почерком є досить перспективним напрямком досліджень і може широко застосовуватись для забезпечення безпеки як домашніх комп'ютерів, так і комп'ютерів найбільших корпорацій, а також для запобігання несанкціонованому доступу зловмисників до web-ресурсів.

3. У роботі проаналізовано 41 інформативну ознаку курсорного почерку десяти користувачів з датасету «Balabit Mouse Challenge Data Set».

4. Аутентифікацію за курсорним почерком слід використовувати для користувачів з добре сформованим «курсорним почерком».

5. Аутентифікацію за курсорним почерком слід використовувати для сценарію двійкової класифікації, тобто для випадків, коли на комп'ютері зареєстровано тільки одного користувача.

6. Аутентифікацію за курсорним почерком слід використовувати для сценарію двійкової класифікації, причому класифікатор повинен перевіряти користувача на приналежність до класу «зловмисники».

7. Найінформативнішим параметром з трьох типів дій миші для задач аутентифікації за курсорним почерком є «mouse movement» дії миші (для сценарію перевірки класифікатором користувача на приналежність до класу «зловмисник»).

9. Найінформативнішими параметрами курсорного почерку є a_beg_time, max_curv, max_jerk, max_omega, mean_a, min_curv, min_jerk, min_omega, num_critical_points, num_points, sd_jerk, що пов'язані з ривками та формою траєкторії курсору миші.

Додаток Б.

Публікації за темою атестаційної роботи

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 24-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

7 – 9 квітня 2020 р.

Том 3

КОНФЕРЕНЦІЯ «ІНФОРМАЦІЙНІ РАДІОТЕХНОЛОГІЇ ТА ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

Харків 2020

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, email: f_re@nure.ua.

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. Курсор-

ний 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. Alieksieiev, 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.

Номер документу	Позначення	Найменування	Прим.
		Текстові документи	
1	ГЮІК ХХХХХХ.001 ПЗ	Пояснювальна записка	100 с.
		Графічний матеріал	
2		Дослідження інформативних параметрів	А4 ел.ф.
		динаміки системи "користувач-миша"	
		для задач ідентифікації за курсорним	
		почерком	
3		Методи ідентифікації користувачів	А4 ел.ф.
		комп’ютерних мереж за інформаційним	
		почерком	
4		Датасети динаміки системи	А4 ел.ф.
		"користувач-миша",	
		що знаходяться у вільному доступі	2х А4 ел.ф.
5-6		Інформативні параметри динаміки	
		системи "користувач-миша"	
7		Схема експерименту у Orange	А4 ел.ф.
8-12		Результати проведених досліджень	5х А4 ел.ф.
13		Висновки	А4 ел.ф.

					ГЮІК ХХХХХХ.001 Д1			
Из	Лист	№ докум.	Підпис	Дата				
Розроб.		Зозуля			*Дослідження інформативних параметрів динаміки системи "користувач-миша" для задач ідентифікації за курсорним почерком*	Літера	Лист	Листів
Перев.		Горелов				Д		
						ХНУРЕ Кафедра КРіСТЗІ		
Н.контр.		Милютченко			Відомість атестаційної роботи магістра			
Затв.		Антіпов						