розмежуванні виявлення та реагування, а також визначенні перевірюваних вимог до коректності роботи.

Список використаних джерел

1. Amazon Web Services. Amazon S3 Event Notifications. AWS Documentation. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html
2. Shuffle. Workflows. Shuffle Documentation. URL: https://github.com/Shuffle/shuffle-docs/blob/master/docs/workflows.md
3. VirusTotal. Writing YARA Rules. YARA Documentation. URL: https://yara.readthedocs.io/en/stable/writing_yara_rules.html

УДК 004.056.5

Колєснік Ігор Олександрович,

здобувач другого (магістерського) рівня вищої освіти
Харківського національного університету радіоелектроніки

Городецький Сергій Леонідович,

старший викладач кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки

ПОВЕДІНКОВА БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ НА ОСНОВІ АНАЛІЗУ ДИНАМІКИ РУХІВ КОМП'ЮТЕРНОЇ МИШІ

Анотація. Розглянуто підхід до додаткової перевірки користувача протягом активного комп'ютерного сеансу за характеристиками рухів миші. Описано програмний прототип реєстрації подій, формування статистичних поведінкових ознак, навчання класифікатора Random Forest та періодичного оцінювання відповідності дій еталонному профілю. Визначено вимоги до перевірки якості моделі на незалежних сеансах, оцінювання хибних рішень та оброблення ситуацій відсутності даних. Показано, що поведінкова біометрія може доповнювати початкову автентифікацію.
Ключові слова: поведінкова біометрія, динаміка комп'ютерної миші, автентифікація, Random Forest, машинне навчання, захист сеансу.

Традиційна автентифікація підтверджує особу переважно в момент входу до інформаційної системи, однак не встановлює, чи залишився власник облікового запису за робочою станцією протягом наступної роботи. Якщо активний сеанс залишається розблокованим, стороння особа

може отримати доступ до ресурсів без повторного введення облікових даних. Тому актуальним є застосування додаткових поведінкових механізмів контролю, які оцінюють дії користувача в процесі взаємодії з комп'ютером [1].

Метою дослідження є обґрунтування та реалізація підходу до поведінкової біометричної автентифікації на основі динаміки рухів комп'ютерної миші із застосуванням машинного навчання. На відміну від ідентифікації серед багатьох осіб, розглянуто бінарну перевірку відповідності поточної поведінки профілю заявленого власника сеансу. Така постановка дає змогу інтегрувати результат класифікатора в політику додаткової перевірки доступу.

Для отримання первинних даних у роботі використано програмний модуль мовою Python та бібліотеку pynput, що реєструє часові мітки, координати курсора і типи подій. Дані легітимного та стороннього користувачів зберігаються в окремих CSV-файлах. Попереднє оброблення передбачає відбір подій переміщення, контроль коректності часових інтервалів і перетворення послідовностей координат на числові характеристики поведінки.

Для розрізнення поведінки власника й сторонньої особи використано Random Forest - ансамбль дерев рішень, придатний для класифікації табличних ознак і врахування нелінійних зв'язків між ними [2]. У практичній реалізації передбачено поділ даних на навчальну і тестову частини у співвідношенні 80:20, навчання моделі засобами scikit-learn та збереження класифікатора для повторного використання без перенавчання під час кожного запуску. Програмну реалізацію доповнено модулем guard.py, який періодично формує поведінкові ознаки та порівнює їх з еталонним профілем.

Окремої уваги потребують загрози відтворення записаних подій, підміни навченої моделі, відключення агента та відсутності рухів миші. За

таких умов політика доступу повинна розрізняти впевнений результат класифікації, підозрілу поведінку, недостатність даних і технічний збій. Доцільно зберігати в аудиті часові мітки, версію моделі, значення порога та підставу прийнятого рішення, мінімізуючи збереження необроблених біометричних траєкторій [3].

Таким чином, у межах дослідження сформовано й програмно реалізовано послідовність збору подій, побудови поведінкових ознак, навчання Random Forest і періодичного контролю активного сеансу. Практичне значення підходу полягає в можливості створення додаткового сигналу виявлення потенційної підміни користувача без спеціалізованого біометричного обладнання. Подальше оцінювання на незалежних сеансах, із вимірюванням FAR, FRR та системних реакцій, є необхідною умовою обґрунтування його надійності та придатності до впровадження.

Список використаних джерел

1. Shen C., Cai Z., Guan X., Du Y., Maxion R. A. User Authentication Through Mouse Dynamics. IEEE Transactions on Information Forensics and Security. 2013. Vol. 8, no. 1. P. 16–30. DOI: 10.1109/TIFS.2012.2223677.

2. Breiman L. Random Forests. Machine Learning. 2001. Vol. 45. P. 5–32. DOI: 10.1023/A:1010933404324.

3. Pedregosa F. et al. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research. 2011. Vol. 12. P. 2825–2830.