УДК-004.93

ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ ГРАВЦІВ ЗАСОБАМИ КОМП'ЮТЕРНОГО ЗОРУ

Фіронов Д.Ю.
e-mail: denys.fironov@nure.ua
Науковий керівник – канд. техн. наук, ст. викл. Кобилін І.О.
Харківський національний університет радіоелектроніки, каф. ІНФ
м. Харків, Україна

This study examines the application of computer vision methods for detecting anomalous player behaviour in first-person shooter games. Traditional signature-based anti-cheat systems demonstrate limited effectiveness against modern cheat software capable of bypassing file-level detection. The proposed approach employs real-time object detection algorithms, particularly YOLO, to identify game entities and analyse cursor movement patterns. Deviations from statistically typical human motor behaviour serve as indicators of automated assistance software. The method offers a non-invasive alternative to kernel-level anti-cheat solutions while maintaining detection capability for both aimbot and wallhack-type violations.

Нечесна гра в онлайн-іграх – не нова проблема. Але в кіберспорті, де гравці змагаються за реальні призи і рейтинг, це вже серйозно впливає на всю екосистему гри. Найпоширеніші порушення – aimbot і wallhack. Перший сам наводить приціл на голову ворога, другий показує гравців крізь стіни. Обидва руйнують чесну гру.

Класичні античіти працюють просто: шукають підозрілі файли або процеси на комп'ютері гравця. Довгий час це працювало непогано. Але зараз розробники чітів навчилися їх обходити – використовують обфускацію коду, динамічне завантаження, запуск з драйверного рівня. Тому старі методи вже не справляються так, як раніше. Потрібні нові підходи.

Один із них – використання комп'ютерного зору. Ідея в тому, щоб аналізувати саму картинку гри в реальному часі, як це робив би людина-спостерігач. Для виявлення персонажів та їхніх голів на екрані добре підходить архітектура YOLO – вона швидка і достатньо точна для роботи під час матчу [1]. Точність локалізації об'єктів оцінюється за метрикою:

$$IoU = \frac{|\ A\ \cap B\ |}{|\ A \cup B\ |}$$

де A – передбачений bounding box;

B – еталонний.

Система постійно фіксує, де знаходяться цілі, і паралельно стежить за траєкторією руху прицілу, обчислюючи його швидкість:

$$v = \frac{\sqrt{(\Delta x)^2+(\Delta y)^2}}{\Delta t},$$

де $\Delta x, \Delta y$ — зміщення прицілу між кадрами;

Δt — часовий інтервал.

Людина рухає мишкою не ідеально – є природній тремор, затримка реакції, невеликі відхилення від прямої лінії. Так влаштована моторика. Aimbot працює інакше: він наводиться різко, математично точно, без зайвих рухів. Система аналізує швидкість, прискорення та кутові відхилення прицілу – і якщо ці параметри систематично виходять за межі людської норми, це сигнал про порушення. Дослідження підтверджують, що такі патерни добре відрізняються від природніх рухів [2].

Таблиця 1 – Обчислення швидкості руху прицілу за формулою:

$$v = \frac{\sqrt{(\Delta x)^2 + (\Delta y)^2}}{\Delta t}$$

Кадр	$\Delta x(px)$	$\Delta y(px)$	Δt(мс)	v (px /мс)	Тип руху
1→2	12	8	16	0,87	Людина
2→3	15	11	16	1,14	Людина
3→4	9	6	16	0,68	Людина
4→5	187	143	16	14,7	Aimbot
5→6	193	139	16	15,1	Aimbot

Як видно з наведених даних, швидкість руху прицілу aimbot-програми перевищує людський показник у 13–17 разів. Такі значення виходять за межі фізіологічно можливих характеристик моторики людини, що дозволяє однозначно класифікувати подібну поведінку як автоматизовану.

Окремо варто згадати wallhack. Його теж можна виявити через поведінку гравця: якщо людина постійно повертає приціл саме туди, де за стіною стоїть ворог – це статистично неможливо без стороннього інструменту.

Система порівнює напрямок погляду гравця з реальними позиціями противників на карті і шукає підозрілі збіги.

Ще один важливий плюс такого підходу – він не чіпає комп'ютер гравця взагалі. Ніякого доступу до файлів, процесів чи оперативної пам'яті. Система просто аналізує відеопотік [3]. Це знімає питання конфіденційності, яке часто виникає до сучасних kernel-level античітів на кшталт Vanguard або Easy Anti-Cheat.

Звісно, є складнощі. Деякі нові чіти вже намагаються імітувати природній рух миші – додають штучний тремор, змінюють швидкість. Крім того, система потребує великих датасетів реальної поведінки гравців для навчання класифікатора. Але напрямок робочий. І скоріш за все саме поєднання комп'ютерного зору з поведінковим аналізом стане основою античіт-систем наступного покоління.

Список використаних джерел:

1. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection. CVPR, 2016. P. 779–788. URL: https://arxiv.org/abs/1506.02640

2. Galli L., Burger T. Detection of cheating in first-person shooter games using computer vision and machine learning. International Journal of Computer Games Technology, 2022. Article ID 551234. URL: https://doi.org/10.1155/2022/551234

3. Kim J., Hong J. AI-based Anti-Cheat System: A Non-Invasive Approach via Visual Behavior Analysis. Journal of Cybersecurity and Privacy, 2023. No. 3 (2), P. 215–230. URL: https://doi.org/10.3390/jcp3020011