ISSN 2224-087X. Електроніка та інформаційні технології. 2024. Випуск 26. С. 88–97
Electronics and information technologies. 2024. Issue 26 P. 88–97

UDC 004.932 DOI: https://doi.org/10.30970/eli.26.8

THE ANTICHEAT DEVELOPMENT IN THE COUNTER-STRIKE MAIN SERIES

Y. Kuzhii, Y. Furgala

Ivan Franko National University of Lviv,
50 Drahomanova St., 79005 Lviv, Ukraine

Yurii.Kuzhii@lnu.edu.ua, *Yuriy.Furhala@lnu.edu.ua*

This research investigates methods to identify and prevent cheating in online games, focusing on Counter-Strike (CS). It explores various cheating behaviors and their evolution alongside anti-cheat development. The limitations of current anti-cheat systems, exemplified by Valve Anti-Cheat and Faceit Anti-Cheat, are highlighted through real-world cases where cheating suspicions arose but no conclusive evidence was found. The paper proposes analyzing player mechanics, including keyboard patterns and movement, as a potential solution to detect radar hacks, smurfing, and unsportsmanlike behavior. By training a system on player behavioral patterns, the authors aim to create a fairer and more enjoyable online gaming experience for CS players.

Keywords: pattern recognition, cheating, anti-cheat, esport, smurfing, Counter - Strike, CS2

This paper examines various types of cheating and user behavior in order to identify approaches for identification and effective prevention of such phenomena. The analysis is carried out on the example of the popular game Counter-Strike, describes the types of cheating in esports over the years, the development of cheats and ways to combat them. The current problems of cheat identification and existing solutions are highlighted using the example of Valve Anti-Cheat and Faceit Anti-Cheat.

The relevance and sensitivity of this topic is illustrated by cases where players were suspected of cheating, but no one was able to provide evidence [1]. To date, players who have confessed to using cheats and have bans on various platforms (Faceit, ESEA, Challengermode) have not received an account ban on the Steam service from Valve. During the qualifying matches for the World Cup, the Challengermode platform administrators disqualified the team [2] for using cheats, but the anti-cheat from Valve did not identify cheating.

An overview of the approaches to combating Aimbot-type cheats is provided. The classification system for identifying smurfing is also considered using the example of the Dota2 game, its advantages and disadvantages. In general, the paper considers the development trend of anti-cheats that work on the client computer, their effectiveness, the method of collecting datasets of unfair games using the Overwatch service, and the effectiveness of detecting unfair players using a neural network from Valve.

Anti-Cheat and Cheating Techniques. Computers and video games are closely intertwined, with the development of one influencing the development of the other. Esports, or competitive video gaming, is a testament to this relationship. Esports has transformed over

time from amateur tournaments between friends into a major industry with millions of fans, professional players, teams, and sponsors.

The inaugural Space Invaders tournament transpired in 1982, offering a monetary prize of $10,000 to the victorious participant. This event is widely recognized as one of the earliest official esports competitions. The first formalized video game competition was conducted in 1972 at Stanford University (USA) for the game "Spacewar!". The 1980s witnessed the ascendancy of arcade games. In 1980, Atari sponsored a Space Invaders tournament that attracted over 10,000 participants [3]. In 1982, Twin Galaxies established the first professional gaming team and organized international competitions against national teams from Japan, Italy, and Great Britain. These competitions were covered by several prominent publications and television channels.

Diminished expenses, technological advancements, the proliferation of the internet, and the advent of personal computers served as catalysts for the growth of esports. Leagues such as ESL, CPL, and WCG were established. Major sponsors included Samsung Corporation and South Korean ministries. The overarching concept was to elevate esports to an equivalent of the Olympic Games. In 2005, approximately 800 players from 70 countries participated in the final event held in Singapore. Over a million individuals partook in the preliminary national qualifiers. Cheating presents a persistent challenge in any FPS (first-person shooter) game. As the Counter-Strike series held the top spot in popularity for an extended period [4], cheating became an inherent aspect of the game. A cheat is software or code employed to gain an unfair advantage in a computer game.

In 1999, college students Minh Le and Jess Cliffe created a modification for the game Half-Life. Half-Life was revolutionary due to its Gold Source game engine. New weapons, maps, and bug fixes were released every 3-5 months. Notably, a melee knife was added in BETA 3. The popularity of the modification grew significantly during the release of Beta 5 and Beta 6, and by early 2000, Counter-Strike had become the most popular online game according to CLQ (Champions League for Quake). As Counter-Strike neared the end of its beta testing phases, the player count tripled compared to the figures at the start of 2000 [5]. On April 12, 2000, Counter-Strike was acquired by Valve Corporation. Even during this early period, methods of cheating, known as cheats, were also being developed alongside the game. Cheats are third-party software or modifications that give players an unfair advantage in online games, violating the established rules of the game. The first cheats were console commands within the game. Only the server administrator could grant access to use these commands - noclip, God mode, and other commands. One of the first cheats was called Trainer [6]. This program provided certain advantages - unlimited ammunition, unlimited character health points, no weapon reloading, and more.

In 2001, cheats well-known to most users appeared - WallHack and Aimbot. WallHack is a special cheat program that gives an advantage over other users. The advantage is that a WallHack player can see other players through walls. Aimbot is popular software that is commonly used in first-person and third-person shooters. Aimbot's function is to make aiming easier in the game. Once Aimbot is installed, it will lock your cursor onto your enemies, so you can shoot with perfect accuracy. Modern Aimbot can be configured to make aiming look like a real user's actions.

Cheats were available on various forums that users could easily download. This led to user complaints that game developer Valve had to address. In April 2002, Valve released the first anti-cheat VAC1. In-game bans were temporary (from one to five years). The first version was not perfect. With each new version, the anti-cheat improved, the number of bans increased,

and users were added to a public list of banned players. Already at that time, many users received false positives in the game.

At that time, VAC checked the user's computer's RAM for manipulations with the game's memory. A WallHack block was also created - a constant check to see if the user can see the opponent's players through an obstacle (wall). If not, then the opponent's game model was not displayed.

In 2004, a new version of the game CS Source was released for the first time, which used a game engine called Source. Most of the users who played the previous version did not switch to the new version. Therefore, cheats were more actively developed for the 1.6 game version.

In 2005, Valve's response was to release a new version of the anti-cheat VAC2 [7]. Unfortunately, this did not affect the hackers, who always kept their solutions up to date. At this time, a new cheat appeared that provided users with information about the location of opponents using audio. It was called LanHack.

It's worth mentioning here that the Ukrainian team Natus Vincere was formed in 2009. They competed in version 1.6. Over the course of a year, the team won four major tournaments in a row, which is still a record today [8].

After that, in 2012, a new version of the game CS GO was released. It can be said that this game was very different from the previous version. New cheats appeared just 2 days after the release of the version.

In 2013, Valve released a new service called Overwatch, which allows players to review matches and report whether they believe a particular player is using a cheat. The final decision is the result of the opinions of 10 reviewers [9]. All matches played in the competitive ranked game mode are saved in demo format, and they used them to develop an AI model [10] to detect player behavior based on the frequency of changes in the player's viewing angles. Demo recordings that the model flagged as fraudulent were sent to the Overwatch system and used as feedback for the model.

Even some esports athletes were banned by the anti-cheat. The most famous is probably Hovik "KQLY" Tovmasyan [11], who received a VAC ban - a ban from Valve [7]. Another Swedish player, Joel "Emilio" Mak, was banned during a match against the Hellraisers team [12]. But many other professional players have been suspected of cheating, although their guilt has not been proven. In 2020, a leak became known. The code for the 2017 version of the game was fully available to all abusers [13]. Work [14] analyzed the largest Game Hacking forums (MPGH) [15] and UnknownCheats (UC) [16], where information about various cheats is posted. The structure of these communities, the types of cheats and the tools with which they are developed, the users and the games for which the cheats are written are described.

There were hvh (hacker vs hacker) communities on various forums [17]. There, players who like to play unfairly teamed up to play on a common server.

In 2023, a new version of the game CS2 was released, which uses the Source2 game engine [18]. Fig. 1 and 2 show the dynamics of changes in search queries for the CS GO and CS2 versions. Source 2 is a 3D game engine currently under development by Valve as the successor to Source. Source 2 is written in C++ using the following key technologies:

- Vulkan - a modern API used for 3D graphics rendering. Vulkan provides high performance and flexibility, making it ideal for game engines.
- Havok Physics - a physics engine used to simulate actions based on physical laws in games. Havok Physics can simulate a wide range of physical phenomena, such as collisions, deformation, and fluid behavior.

- Steamworks - an API used to integrate games with the Steam platform. Steamworks provides access to features such as online multiplayer, achievements, cloud saves, and community.

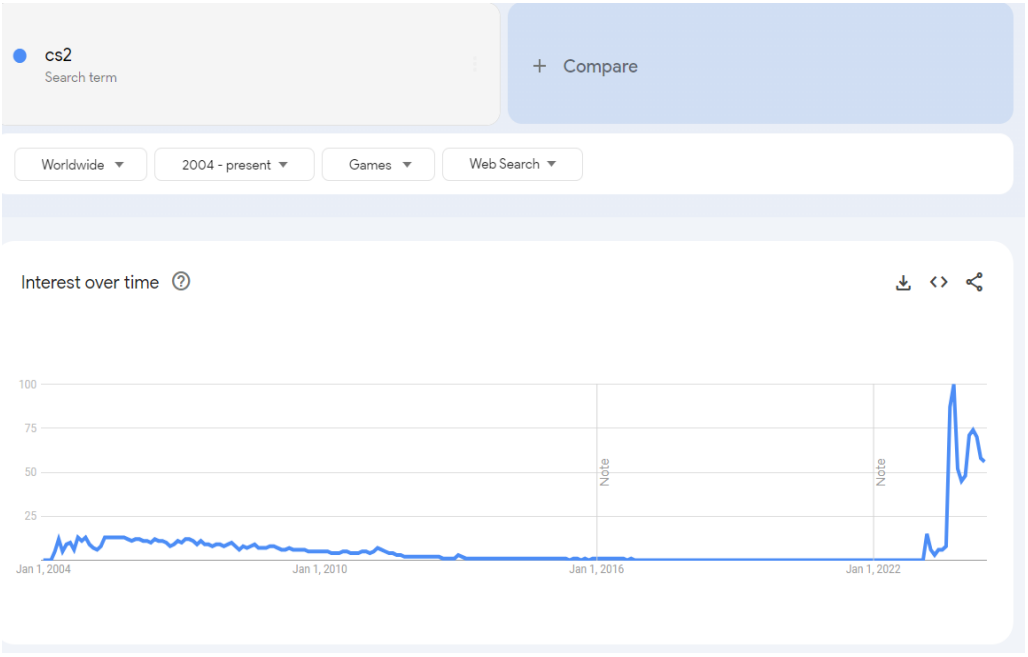

Fig. 1: Illustrating the Rise in Popularity of the Search Term "cs2" from the 2005

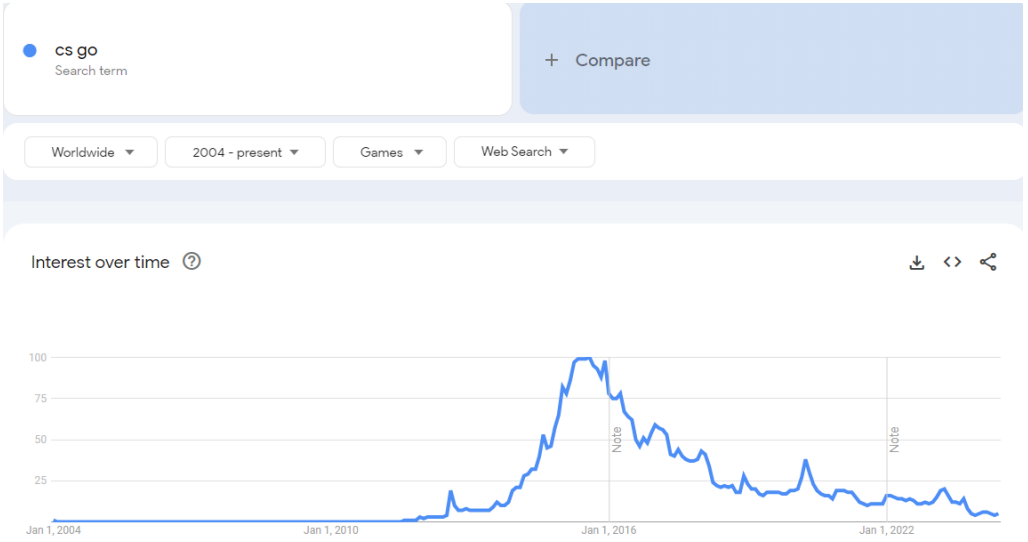

Fig. 2: Depicting the Downtrend in Popularity of the Search Term “cs go”

C++ Standard Library: used for tasks such as memory handling, containers, and algorithms. The C++ Standard Library provides the basic functionality needed for game engine development.

Source 2 also uses a number of other technologies, such as OpenGL, OpenAL, SQLite, and Lua.

CS2 users constantly raised the problem of cheaters in matchmaking. Since the previous version was completely replaced with a new game, millions of users immediately started playing the new game. At the start of the game's release, most of the ranked users were cheaters. At the moment, there is a fairly large selection of cheats for Cs2 on well-known forums [19]. They later received VAC bans. With the release of the VAC NET update, some professional players received false positive bans, which Valve later overturned.

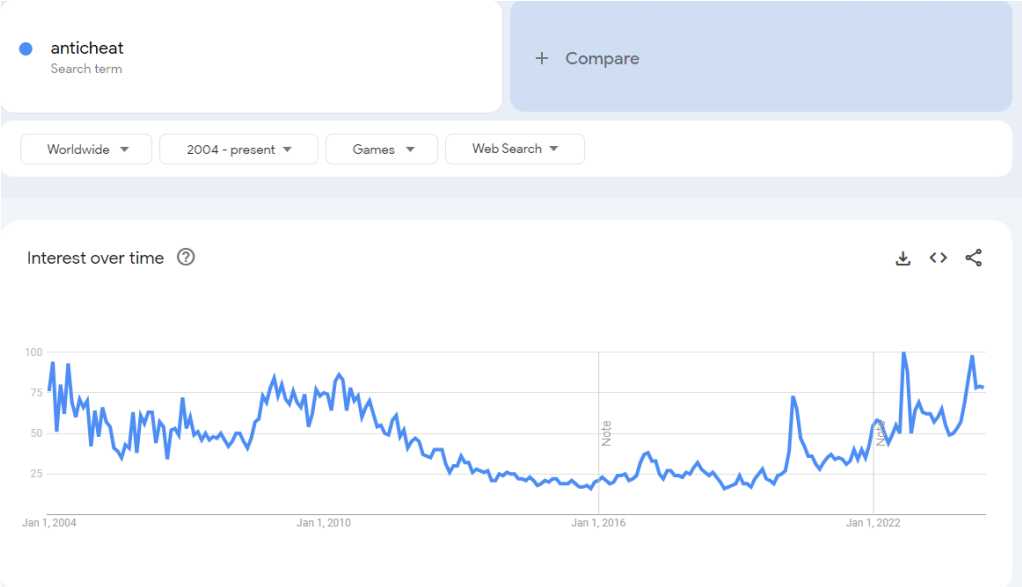

Fig. 3. Illustrating the Popularity Trend of the Search Term "anticheat"

The overall state of the problem has reached a level where situational responses to cheating have become clearly insufficient, and there is a need to develop and implement systemic approaches to its solution. Since 2020, the number of search queries related to this issue has begun to grow rapidly. This is due to the period when, due to COVID 19, the number of online users in various game genres increased. In the article [20], great attention is paid to such cheats as Aimbot. The Aimdetector program was created, which identified cheaters, taking into account the discrepancy between the behavioral characteristics of players of different game levels. A low-level player with an aim cheat will usually not have such high mechanical characteristics (character control in the game), will make many mistakes - choosing a position, managing ammunition, etc.

In the work [21], an open-source anti-cheat [22] and an anti-cheat from Valve were tested to detect Aimbot cheats, whose behavior is similar to that of real players. The researchers came to the conclusion that the higher the level of the player, the more difficult it is to understand whether he is using auxiliary programs for the game. It was found that some players can shoot

while the game model is moving. Such behavioral patterns are not characteristic of mid-level and high-level players. Therefore, in further research, it is worth paying attention to the study of how well the player controls the model and whether he uses the keyboard correctly in comparison with professional players. Although this work did not provide quantitative indicators of the player's level (game level on the Faceit platform). The accounts of players who used cheats were not classified by the service [9] as suspicious.

Smurfing is a term used in computer games to describe experienced players who intentionally create new accounts to play with less experienced players. This problem also exists in CS2 on the Faceit platform. A player who is a smurf and helps to raise the rating of other players, receiving a financial reward, is called a booster. In [23], the problem of boosters in esports is considered, quantitative indicators are described, for example, the relative indicator of boosters. The main reason is the financial component. South Korea is fighting this phenomenon at the legislative level. Image recognition will help identify smurfs and boosters.

Smurfing can be identified by analyzing the statistical indicators of players over 20 matches [24]. In this work, the PCA method was used to determine the characteristics that help to form a complete image of the smurf. In the work [25], the author investigated the impact of smurfs on ordinary players. Of course, he came to the conclusion that this is a negative experience. Game manufacturers should do more to protect. Although these users who are smurfs do not consider their behavior to be dishonest, but perceive such an experience as an opportunity to play against a strong player.

With the growth of the popularity of esports, fixed-result matches, the so-called 322, have become a problem. Match-fixing is when players or teams intentionally lose a match by agreement or for money. The term "322" has an interesting history. Team ROX.KiS player Alexei Solo Berezin placed a bet on his loss in the amount of $100 USD at odds of 3.22, thus the winning amount was $322.

In the work [26], various aspects and types of unsportsmanlike behavior are considered. The author came to the conclusion that the boundaries of sports behavior are vaguely defined and difficult to interpret unequivocally. And any online game is a favorable environment for unsportsmanlike behavior and cheating. Sometimes it can increase the interest and attention of viewers to the game.

In 2011, the Faceit platform was created in London. It has a different rating system and anti-cheat compared to Valve. Most ranked players play their regular and tournament matches there. Faceit Anti-Cheat will be described below. It must be installed for each user. A list of reasons [27] for which you can be banned from the game for a different period of time is published on the Faceit platform. These reasons are related to the use of cheats, violation of platform rules, or behavior directly in the game. Most bans are issued after complaints are considered by the support service and may not always be objective.

Even at offline tournaments, cases of playing with cheats are known [28]. However, today the main problem in esports is the radar hack and fixed-result matches. For ordinary users, the problem is smurfing and various types of unsportsmanlike behavior in the game.

Radar hack is a type of cheat used in CS2 to give players an unfair advantage. This cheat allows you to see the positions of all players on the opposing team on the radar, even if they are behind walls or in other places where they cannot be seen normally.

DMA (Direct Memory Access) is a technology that allows computer peripherals (such as video cards) to access system memory directly without involving the CPU. This can significantly improve computer performance for some tasks. DMA can be used for radar hacking in the following way: The cheat uses DMA to access system memory. The cheat

searches memory for player position data and sends it to another device. Therefore, the system anti-cheat is not able to identify the behavior of the player-system due to memory manipulations through DMA.

With the growth of esports and bookmakers' bets on games, the problem of cheating has become particularly relevant. Most tournaments are held in online mode. This makes it difficult to check the honesty of the players. The prizes of the most popular tournaments are measured in millions of dollars.

The most popular solutions today are VACnet and Faceit Anti-Cheat.

FACEIT Anti-Cheat is a system for ensuring honesty and security in the gaming environment. The system consists of three main components:

- *Client* - runs during the game for protected games, such as CS2, and collects data about gameplay and player behavior.
- *Kernel driver* - loads during system startup and provides low-level protection against unauthorized access to game processes.

- Server-side SDK - used for secure data exchange between the client and the server, as well as for data analysis and fraud detection.

The Faceit Anti-Cheat system is designed with security and data privacy in mind**.** It complies with GDPR and other data protection regulations.

To combat smurfing, the Faceit platform uses MFA and KYC [29]. Historically, the platform has changed its approach to dealing with smurfs [30] and users with multiple accounts. These methods can be quite effective for new accounts, but smurfs often use inactive accounts of existing users. It is also possible to create a request to the support service, indicate another player's account and wait for the application to be considered. This process is quite imperfect. By using programs that change the component IDs, it is easy to mislead the support service and this player will continue his activity.

Conclusions. Cheating as a type of player and team behavior has been a significant problem in online Counter-Strike games since the game's release. The most popular platforms that provide identification of this today are VACnet and Faceit Anti-Cheat. Faceit Anti-Cheat is a more effective solution according to the assessment. Faceit uses an anti-cheat that is effective against most types of cheat programs, except for radar. However, this anti-cheat is not able to identify unsportsmanlike behavior and smurfing, which are also significant problems in CS2.

At the same time, to identify the use of prohibited means, it is important to consider the mechanics of the players' motor activity, since the Counter - Strike games are mechanically complex [31,32]. That is, it is worth paying attention not only to the aim, but also to the patterns of keyboard work when controlling the game character, the use of grenades, understanding the geometry and physics of the game, the spatial orientation of the player [21].

Identification of patterns that are formed on the basis of the behavioral characteristics of players can help to solve these problems**.** In particular, the cheating detection system can be trained on the basis of a system of behavioral signs, in order to identify players who use the radar cheat and detect smurfs or unsportsmanlike behavior.

The use of pattern identification can make online games fairer and more enjoyable for users. This will increase their popularity.

REFERENCES

[1] *Harry Richards*. ESIC suspends Ukrainian quartet for two years over match-fixing charges: [Electronic resource]. - 2023. - [Cited 2024, 1 Apr.]. – Available from: https://www.hltv.org/news/37629/esic-suspends-ukrainian-quartet-for-two-years-over-match-fixing-charges.

[2] *Andre Guaraldo*. Unprecedented CS2 cheating crisis strikes European RMR. - 2024. - [Cited 2024, 3 Apr.]. - Available from: https://www.strafe.com/news/read/unprecedented-cs2-cheating-crisis-strikes-european-rmr/.

[3] *Julian Heinz, Anton Ströh*. (2017). The eSports Market and eSports Sponsoring. DOI: https://doi.org/10.1080/24704067.2020.1846906.

[4] Steam Charts by SteamDB: [Electronic Resource]. - [Cited 2024, 1 Mar.]. - Available from: https://steamdb.info/charts/?tagid=1663.

[5] Counter-Strike Beta: [Electronic Resource]. - [Cited 2024, 7 Mar.]. - Available from: https://counterstrike.fandom.com/wiki/Counter-Strike_Beta#Preparing_for_the_first_release.

[6] 9trainers: [Electronic Resource]. - [Cited 2024, 7 Mar.]. - Available from: https://9trainers.com/counter-strike-1-6-multiplayer-trainer-free-download/.

[7] Steam support: [Electronic Resource]. - [Cited 2024, 7 Mar.]. - Available from: https://help.steampowered.com/en/faqs/view/571A-97DA-70E9-FF74

[8] NaVi history: [Electronic Resource]. - [Cited 2024, 21 Mar.]. - Available from: https://navi.gg/ua/company/history.

[9] Overwatch: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://blog.counter-strike.net/index.php/overwatch/.

[10] Using Deep Learning to Combat Cheating in CS:GO: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://www.youtube.com/watch?v=GC6JXAO8sT4.

[11] *Evan Lathi*. CS:GO competitive scene in hacking scandal, 3 players banned: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://www.pcgamer.com/csgo-competitive-scene-embroiled-in-hacking-scandal-as-three-players-are-banned/

[12] Emilio: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://liquipedia.net/counterstrike/Emilio

[13] *Cecilia D'Anastasio*. Valve Confirms the Leak of Counter-Strike: Global Offensive Code: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://www.wired.com/story/counter-strike-global-offensive-team-fortress-2-code-leak/.

[14] *Panicos Karkallis, Jorge Blasco, Guillermo Suarez-Tangil & Sergio Pastrana*. (2021) Detecting video-game injectors exchanged in game cheating communities. DOI: https://doi.org/10.1007/978-3-030-88418-5_15.

[15] MPGH: [Electronic Resource]. - [Cited 2024, 16 Mar.]. - Available from: https://www.mpgh.net/.

[16] Unknowcheats: [Electronic Resource]. - [Cited 2024, 11 Feb.]. - Available from: https://www.unknowncheats.me/forum/index.php.

[17] Hackvshack:[Electronic Resource]. - [Cited 2024, 1 Apr.]. - Available from: https://hackvshack.net/.

[18] Source2 engine: [Electronic Resource]. - [Cited 2024, 6 Mar.]. - Available from: https://developer.valvesoftware.com/wiki/Source_2.

[19] Unknowcheats Counter-Strike: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://www.unknowncheats.me/forum/counter-strike-2-a/?s=a36b7c8e78939e4d2dd42d25b5095042.
[20] *D Liu, X Gao, M Zhang, H Wang, A Stavrou.* (2017). Detecting Passive Cheats in Online Games via Performance-Skillfulness Inconsistency. DOI: 10.1109/DSN.2017.20
[21] *Tim Witschel. Christian Wressnegger*. (2020). Aim Low, Shoot High: Evading Aimbot Detectors by Mimicking User Behavior. DOI: https://doi.org/10.1145/3380786.3391397
[22] *E. Edson.* Cow Anti-Cheat. https://github.com/eedson/Cow-Anti-Cheat, 2018. Accessed Feb. 2020
[23] *Eoin Conroy, Magdalena Kowal, Adam J. Toth, Mark J. Campbell*. (2021). Boosting: Rank and skill deception in esports. DOI: https://doi.org/10.1016/j.entcom.2020.100393
[24] *Ying-Jih Ding; Wun-She Yap; Kok-Chin Khor*. (2023). Profiling and Identifying Smurfs or Boosters on Dota 2 Using K-Means and IQR. DOI: 10.1109/TG.2023.3317053
[25] *Brian McCauley*. (2023). An Auto-netnographic Approach to Understanding Alternate Gaming Accounts: How Smurfing Impacts the Prosumer Experience in Counter-Strike:Global Offensive. DOI: https://doi.org/10.1123/jege.2023-0024
[26] *Sidney V. Irwin & Anjum Naweed*. (2020). BM'ing, Throwing, Bug Exploiting, and Other Forms of (Un)Sportsmanlike Behavior in CS:GO Esports. DOI: https://doi.org/10.1177/1555412018804952
[27] FACEIT Banning Policy: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://support.faceit.com/hc/en-us/articles/208282375-FACEIT-Banning-Policy
[28] Forsaken issued five-year ban by ESIC: [Electronic Resource]. - [Cited 2024, 1 May]. - Available from: https://www.hltv.org/news/25176/forsaken-issued-five-year-ban-by-esic.
[29] Introducing the FACEIT ID Verification system, an unmatched layer of security to create a more trusted community: [Electronic Resource]. - [Cited 2024, 15 Apr.]. - Available from: https://blog.faceit.com/introducing-the-faceit-id-verification-system-an-unmatched-layer-of-security-to-create-a-more-c3232fdba781.
[30] Cheating and Multi-accounting are at all-time lows since 2012 on FACEIT — Here's what we did: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://blog.faceit.com/cheating-and-multi-accounting-are-at-all-time-lows-since-2012-on-faceit-heres-what-we-did-920ec5f779ff.
[31] *Tim Witschel. Christian Wressnegger*. (2020).Aim Low, Shoot High: Evading Aimbot Detectors by Mimicking User Behavior. DOI: https://doi.org/10.1145/3380786.3391397
[32] A Guide to Mechanics in Counter-Strike: [Electronic Resource]. - [Cited 2024, 23 Mar.]. - Available from: https://dignitas.gg/articles/a-guide-to-mechanics-in-counter-strike.

РОЗВИТОК АНТИЧИТІВ У ВЕРСІЯХ ГРИ COUNTER-STRIKE

Ю. Кужій, Ю. Фургала

Львівський національний університет імені Івана Франка,
вул. Драгоманова 50, 79005 Львів, Україна
Yurii.Kuzhii@lnu.edu.ua, Yuriy.Furhala@lnu.edu.ua

На сьогоднішній день кіберспорт набув широкої популярності. Основною проблемою є нечесна поведінка користувачів – читерство. Читери постійно розробляють нові методи обходу античит систем, що робить їх неефективними з часом. Чити для останньої версії гри з'явились за кілька днів після релізу бета версії. Існуючі системи не завжди можуть

відрізнити чесну гру від читерства, що може призвести до помилкових блокувань або відсутності покарання для нечесних користувачів.

У роботі досліджено методи виявлення та запобігання читерству в онлайн-іграх, зокрема в різних версіях Counter-Strike. Проаналізовано різні види читерської поведінки, та їхню еволюцію паралельно з розвитком систем захисту від читів. Приведено приклади використання читів по типу “радар-хак” під час онлайн турнірів. А саме перехід від клієнтських античитів до систем, які використовують глибинне машинне навчання. Описано еволюцію ігрових рушіїв гри. Велику увагу приділено дослідженням поведінки користувачів, які використовують кілька облікових записів (смурфів) для підняття ігрового рейтингу та способів боротьби з ними. Розглянуто існуючі методи ідентифікації смурфів на прикладі кіберспортивної дисципліни Dota2. Досліджуються обмеження сучасних античит-систем, таких як Valve Anti-Cheat та Faceit Anti-Cheat. Наведено приклади гравців, які признались у використанні різних засобів, але не були заблоковані античитом від Valve. Встановлено, що приріст активності нечесних користувачів відбувся після переходу турнірів в онлайн режим у зв’язку з пандемією COVID-19.

Оскільки класичні підходи не є достатньо ефективними, в роботі запропоновано аналізувати ігрову механіку гравців, включаючи клавіатурні паттерни та інші ознаки для формування образу гравця. Використання розпізнавання образів допоможе виявити такі види нечесної гри.

*Ключові слова***:** розпізнавання образів, читерство, античит, кіберспорт, smurfing, Counter-Strike, CS2

The article was received by the editorial office on 16.06.2024.
Accepted for publication on 26.06.2024.