

УДК 004.9

Обзор способов борьбы с несанкционированными модификациями в онлайн-играх

Изранов Кирилл Сергеевич

izranovks@gmail.com

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

Рассмотрены способы борьбы с несанкционированными модификациями (также называемыми «читами») в онлайн-играх. Читы являются огромной проблемой современных онлайн-игр. Разработчикам часто приходится прибегать к разнообразным способам борьбы с ними. Цель работы — рассмотрение различных способов решения данной проблемы, проведение анализа результатов борьбы и выявления методов, подходящих в той или иной ситуации.

Ключевые слова: онлайн-игры, несанкционированные модификации

Онлайн-игры стали неотъемлемой частью современной цифровой культуры, привлекая миллионы пользователей по всему миру. С развитием технологий и увеличением популярности многопользовательских игр появилась серьезная проблема, с которой сталкиваются разработчики и игроки — читерство. Читы позволяют нечестным игрокам получать несправедливое преимущество, разрушая баланс игры, ухудшая игровой опыт и негативно влияя на всю экосистему игр. В результате разработчики вынуждены применять различные меры для борьбы с этой проблемой [1].

Полномочный сервер. Одним из наиболее надежных способов предотвращения читерства является просчет всей логики игры на сервере. В этом подходе весь игровой процесс выполняется на сервере, а клиентские приложения игроков получают только информацию, необходимую для визуализации происходящего на экране. Такой способ позволяет минимизировать возможность вмешательства игрока в игровой процесс через клиентские читы, поскольку пользователи не имеют доступа к игровой механике напрямую. Также это помогает скрыть информацию, которую игроки не должны видеть [2].

2. Шифрование трафика. Еще одним важным методом является шифрование трафика между клиентом и сервером. Суть метода заключается в защите данных, передаваемых между игроком и сервером, с использованием современных криптографических алгоритмов. Это предотвращает атаки типа «человек посередине» (MITM) и попытки вмешательства в сетевой трафик игры с целью его изменения или подмены [3].

3. Автоматизированные системы анализа игрового процесса. Автоматизированные системы анализа игрового процесса представляют собой сложные программные инструменты, которые отслеживают поведение игроков в реальном времени для выявления аномалий, вызванных читерством. Такие системы используют алгоритмы машинного обучения и анализа данных для выявления действий, которые выходят за рамки нормального игрового про-

цесса (например, слишком быстрые реакции или невозможные движения или действия). В случае обнаружения подозрительной активности система автоматически предупреждает разработчиков или блокирует нарушителей.

Эти системы работают на базе большого массива данных, анализируя все аспекты игры, включая передвижение персонажей, частоту использования определенных действий, взаимодействие с окружающей средой и многое другое. Автоматизированные системы могут анализировать не только поведение игрока, но и взаимодействие игры с оборудованием пользователя, отслеживая возможные вмешательства стороннего ПО (например, сторонних программ для изменения игрового процесса) [4].

4. Ловушки для читеров. Ловушки для читеров — это особые механизмы, которые закладываются разработчиками в код игры с целью обнаружения нечестных игроков. Эти методы специально разработаны, чтобы выявлять попытки вмешательства в игровой процесс, манипуляции с данными или использование стороннего ПО. Ловушки могут принимать форму скрытых проверок, которые выполняются без ведома игрока, чтобы выявить признаки использования читов. К примеру, они могут проверять изменение параметров клиента, которые в нормальных условиях не должны изменяться.

Ловушки для читеров можно сравнить с системой капканов, которая срабатывает, когда нарушитель пытается изменить игровой процесс. Одним из примеров таких ловушек может быть проверка на изменения файлов игры — при вмешательстве в код или конфигурацию игра отправляет сигнал на сервер, оповещая о нарушении. В случае с многопользовательскими играми, такие ловушки могут даже временно предоставлять читеру преимущество только для того, чтобы затем полностью его изолировать или заблокировать [5].

Эксперимент. Для проведения эксперимента был разработан 3D-шутер от третьего лица на Unity, сетевое взаимодействие в котором осуществлено с помощью SDK Colyseus. В ходе эксперимента использовались следующие несанкционированные манипуляции: изменение просчета урона (изменение логики игрового процесса посредством реверс-инжиниринга с помощью dnSpy), телепортация (перехват и модификация сетевых пакетов с помощью WireShark), aim-bot (библиотека Python OpenCV для распознавания изображений), изменение параметров оружия (изменение файлов конфигурации игры), а также автокликер (макрос, созданный с помощью AutoHotkey). Полномочный сервер (изменение логики передачи состояний комнаты в Colyseus) эффективно предотвратил изменение просчета урона и телепортацию, исключив возможность вмешательства в логику игры на клиентской стороне. Шифрование трафика с помощью безопасного подключения помогло защититься от попыток телепортации и манипуляций с параметрами через сетевые атаки, защитив от подмены данных. Автоматизированные системы анализа (создание скрипта, отслеживающего среднюю скорость мыши и количество нажатий кнопки мыши в секунду) успешно выявляли подозрительные действия, такие как использование aim-bot и автокликеров, обнаруживая аномальные паттерны поведения. Ловушки для читеров (проверка целостности

данных в файлах) позволили обнаружить подмену файлов игры и изменения параметров, предупреждая вмешательство в игровой процесс через модификации клиента.

Эти методы в комплексе обеспечили защиту от различных типов читов, поддерживая честность игрового процесса.

На основе результатов эксперимента можно сделать вывод, что отсутствуют универсальные решения, позволяющие идентифицировать читеров и предотвращать изменения игрового процесса. В каждом конкретном случае для обеспечения надежной борьбы с читерами в онлайн-играх необходимо использовать методы в комплексе, выбирая их исходя из многих факторов, например, вычислительной мощности сервера, темпа игры, количества пользователей в одном матче и других.

Литература

- [1] *Читерство в мультиплеерных играх и борьба с ним*. URL: <https://sky.pro/wiki/gamedev/chiterstvo-v-multipleerh-igrah-i-borba-s-nim/> (дата обращения 17.10.2024).
- [2] *Архитектура сервера онлайн-игры на примере Skyforge*. URL: <https://habr.com/ru/companies/vk/articles/220359/> (дата обращения 05.10.2024).
- [3] *Как разработать сетевой протокол мобильной MMO-RPG*. URL: <https://habr.com/ru/articles/451512/> (дата обращения 10.10.2024).
- [4] *Человек мухлюющий — читы в гейм-индустрии. Часть 2: Античиты, их проблемы и возможности*. URL: <https://habr.com/ru/companies/serverspace/articles/832858/> (дата обращения 15.10.2024).
- [5] *Борьба с читерами в онлайн-играх: 22 «нужно» и «нельзя»*. URL: <https://habr.com/ru/articles/320602/> (дата обращения 01.10.2024).

Overview of methods for combating cheating in online - games

Izranov K.S. izranovks@gmail.com

BMSTU (KB), Kaluga, Russia

Methods for combating cheating in online games are reviewed. Cheating is a huge problem in modern online games. Developers often have to resort to various methods to combat it. The aim of this report is to examine different ways of addressing this issue, analyze the results of anti-cheating measures, and identify methods that are suitable for different situations.

Keywords: online games, cheats