

РАЗРАБОТКА ИНТЕГРИРОВАННОЙ АНТИЧИТ-СИСТЕМЫ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ МНОГОПОЛЬЗОВАТЕЛЬСКИХ ИГР

Зинатов Р.Г. (ИТМО)

Научный руководитель – кандидат технических наук, доцент

Харитонов А.Ю. (ИТМО)

Введение. Читерство в многопользовательских онлайн-играх остается одной из ключевых угроз для игровой индустрии, подрывая справедливость соревновательного процесса, снижая лояльность игроков и нанося ущерб репутации разработчиков. Традиционные методы обнаружения нечестных игроков, такие как сигнатурный анализ или ручная модерация, демонстрируют ограниченную эффективность из-за динамичной эволюции чит-программ и роста объемов данных. В условиях стремительного развития киберспорта и увеличения числа игроков (по прогнозам, мировой рынок видеоигр достигнет \$257 млрд к 2030 году) необходимость внедрения интеллектуальных систем обнаружения аномалий становится критической [1]. Современные исследования в области искусственного интеллекта и машинного обучения открывают новые возможности для создания адаптивных античит-решений, способных анализировать поведение игроков в реальном времени и минимизировать ложные срабатывания.

Основная часть. В борьбе с читерством в онлайн играх ИИ предлагает новые перспективы, значительно превосходя традиционные методы детектирования мошенничества по ряду параметров. Предлагаемая архитектура античит-системы на базе ИИ включает три взаимосвязанных модуля:

1. *Сбор и обработка данных* — автоматизированная система записи игровых сессий, фиксирующая действия игроков, параметры игрового мира и контекстные события [2], [3]. Данные структурируются в форматы, пригодные для анализа временных последовательностей и пространственных паттернов.
2. *Анализ аномалий* — ядро системы, основанное на алгоритмах машинного обучения, которые выявляют отклонения от нормального поведения. Используются гибридные подходы, сочетающие анализ временных рядов [4] (например, траектории движения) и статических параметров (статистика убийств, точность стрельбы).
3. *Обучение и адаптация* — модуль непрерывного обновления моделей, позволяющий системе реагировать на новые виды читерства. Интеграция обратной связи от игроков и модераторов повышает точность классификации.

Ключевой потенциал системы заключается в её масштабируемости и универсальности. Архитектура поддерживает интеграцию в различные игровые движки и платформы, а модульный дизайн позволяет гибко настраивать параметры анализа под специфику жанров — от шутеров до стратегий. Преимуществами решения являются:

1. Снижение нагрузки на серверы за счет распределенной обработки данных.
2. Минимизация человеческого фактора благодаря автоматизации процессов обнаружения и валидации.
3. Совместимость с существующими античит-инструментами, что упрощает внедрение в текущую инфраструктуру.

Выводы. Разработка интеллектуальных античит-систем на базе ИИ имеет стратегическое значение для устойчивого роста игровой индустрии. Такие решения не только повышают качество игрового опыта, но и способствуют формированию доверия между разработчиками и сообществом. Перспективными направлениями для внедрения являются киберспортивные платформы, массовые многопользовательские проекты.

Список использованных источников:

1. Филиппов, А. В. Тенденции развития игровой индустрии в России / А. В. Филиппов // Тенденции развития науки и образования. – 2022. – № 85-1. – С. 72-74. – DOI 10.18411/trnio-05-2022-19. – EDN DRXSDG.
2. Alayed H., Frangoudes F., Neuman C. Behavioral-based cheating detection in online games using machine learning // IEEE Conference on Computational Intelligence in Games. — 2013.
3. L. Galli, D. Loiacono, L. Cardamone, и P. L. Lanzi, «A cheating detection framework for Unreal Tournament III: A machine learning approach», в *2011 IEEE Conference on Computational Intelligence and Games (CIG'11)*, Seoul, Korea (South): IEEE, авг. 2011, сс. 266–272. doi: [10.1109/CIG.2011.6032016](https://doi.org/10.1109/CIG.2011.6032016).
4. J. P. Pinto, A. Pimenta, и P. Novais, «Deep learning and multivariate time series for cheat detection in video games», *Mach Learn*, т. 110, вып. 11, сс. 3037–3057, дек. 2021, doi: 10.1007/s10994-021-06055-x.