Левченко Л.А.
Студент 3 курса
«СПбГУТ им. проф. М.А. Бонч-Бруевича», Санкт-Петербург, Россия
Селиванова Т.Е.
Преподаватель
«СПбГУТ им. проф. М.А. Бонч-Бруевича», Санкт-Петербург, Россия

УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОМ КИБЕРСПОРТЕ: ПОДМЕНА ИГРОКОВ, ИНФРАСТРУКТУРНЫЕ АТАКИ И РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье систематизированы актуальные угрозы кибербезопасности в профессиональном киберспорте по состоянию на 2024–2026 годы. Рассмотрены инциденты подмены игроков с применением дистанционного управления через Discord (дело Tokyogurl/Cheerio, SEA Games 2025), аккаунт-шаринг и матч-фиксинг (дело Sensability, Dota 2), DDoS-атаки на игровую инфраструктуру (финал DreamLeague Season 25, 2025), кризис аймбот-ботов в Team Fortress 2 и смёрфинг на платформе FACEIT. Отдельно проанализированы угрозы, связанные с уязвимостью каналов связи (Discord, TeamSpeak), утечками персональных данных с киберспортивных платформ, а также с применением искусственного интеллекта в качестве нового вектора атак. Результаты систематизированы в матрице угроз и контрмер.

Ключевые слова: киберспорт, кибербезопасность, подмена игрока, аккаунт-шаринг, распределенный отказ от обслуживания, матч-фиксинг, античит, смёрфинг, утечка данных, искусственный интеллект.

Abstract. This article presents a systematic analysis of current cybersecurity threats in professional esports as of 2024–2026. Incidents examined include: remote player substitution via Discord Screen Share (the Tokyogurl/Cheerio case, SEA Games 2025), account sharing and match-fixing (the Sensability case, Dota 2), DDoS attacks on gaming infrastructure (DreamLeague Season 25 grand final, 2025), the aimbot crisis in Team Fortress 2, and smurfing on the FACEIT platform. Threats related to communication channel vulnerabilities (Discord, TeamSpeak), personal data breaches on esports platforms, and the emerging use of artificial intelligence as an attack vector are analyzed separately. Findings are consolidated into a threat-and-countermeasure matrix.

Keywords: esports, cybersecurity, player substitution, account sharing, distributed denial of service (DDoS), match-fixing, anti-cheat, smurfing, data breach, artificial intelligence (AI).

УДК 004.056.5

Введение. Профессиональный киберспорт к середине 2020-х годов превратился в индустрию с многомиллиардными оборотами: призовой фонд The International по Dota 2 превышал 40 млн долларов в 2021 году. Столь высокая концентрация финансовых интересов неизбежно привлекает злоумышленников. Особенность угроз в данной сфере состоит в том, что традиционные средства защиты информации (межсетевые экраны, антивирусные решения) оказываются недостаточными: требуются инструменты, функционирующие в реальном времени непосредственно с игровыми движками и платёжными платформами, а также согласованные действия организаторов соревнований, разработчиков и самих спортсменов.

Актуальность. Киберспорт стал одной из самых быстрорастущих цифровых экосистем, однако его безопасность серьёзно отстаёт от темпов коммерциализации. Участившиеся случаи подмены игроков, DDoS-атак на финалы турниров, кризис аймбот-ботов и использование искусственного интеллекта для обхода античитов создают прямые репутационные и финансовые риски. При этом многие угрозы (например, «гостинг» через Discord или фишинг сессионных токенов) не имеют системного описания в научной литературе, что делает их актуальным объектом исследования.

Цель статьи. Целью статьи является систематизация наиболее значимых угроз кибербезопасности в профессиональном киберспорте в период 2024–2026 годов и их группировка по основным векторам воздействия.

Задачи:

1. выделить ключевые векторы угроз (подмена игроков, DDoS, матч-фиксинг, боты, смёрфинг, утечки данных, ИИ-атаки);
2. проанализировать конкретные инциденты, произошедшие в 2025–2026 годах, с описанием механизмов реализации;
3. оценить роль искусственного интеллекта как нового класса атакующих и защитных средств;
4. представить результаты в виде наглядной матрицы угроз и контрмер.

Научная новизна. В работе впервые систематизированы угрозы кибербезопасности киберспорта с учётом резонансных инцидентов 2025–2026 годов (дело Tokyogurl/Cheerio, DDoS на DreamLeague Season 25, пожизненные баны ESIC). Предложена авторская матрица угроз, объединяющая технические, организационные и правовые аспекты. Отдельно введено понятие ИИ-вектора: показано, как нейросетевые читы и LLM-фишинг формируют новое противостояние атакующих и защитных систем.

Профессиональный киберспорт к середине 2020-х годов превратился в индустрию с многомиллиардными оборотами: призовой фонд The International по Dota 2 превышал 40 млн долларов в 2021 году [23]. Столь высокая концентрация финансовых интересов неизбежно привлекает злоумышленников. Особенность угроз в данной сфере состоит в том, что традиционные средства защиты информации такие как: межсетевые экраны, антивирусные решения оказываются недостаточными: требуются инструменты, функционирующие в реальном времени непосредственно с игровыми движками и платёжными платформами, а также согласованные действия организаторов соревнований, разработчиков и самих спортсменов [1]. Настоящая статья систематизирует наиболее значимые угрозы 2024–2026 годов, сгруппировав их по основным векторам воздействия.

Первый и наиболее резонансный вектор угроз — подмена игроков и аккаунт-шаринг, непосредственно подрывающие целостность соревнований. Показательным примером служит дело тайской киберспортсменки Напхат «Tokyogurl» Варасин. 15 декабря 2025 года в ходе полуфинального матча женского турнира по Arena of Valor на 33-х Юго-Восточноазиатских играх в Бангкоке судьи зафиксировали подозрительное поведение участницы [9]. Расследование установило: Варасин использовала личный телефон, внешне идентичный официальному соревновательному устройству, для подключения к Discord. Через функцию трансляции экрана (Screen Share) она передавала изображение сообщнику за пределами арены, который дистанционно управлял её персонажем, — схема получила в материалах следствия наименование «ghosting» [10]. Операция «Ghostbuster» завершилась 4 февраля 2026 года задержанием обоих фигурантов; суд района Патхумван вынес приговор в виде трёх месяцев лишения свободы с учётом признания вины [10]. Тайская федерация киберспорта пожизненно отстранила Варасин от

соревнований. Данное дело обнажило фундаментальную уязвимость: процедуры идентификации участников во многих турнирах опираются исключительно на визуальный контроль, тогда как технических средств обнаружения дистанционного управления устройством не предусмотрено [22].

Принципиально иную, но схожую по сути угрозу представляет аккаунт-шаринг. Российский игрок Александр «Sensability» Филатов стал центральной фигурой расследования ESIC, завершившегося в апреле 2026 года пожизненным баном [7]. Комиссия установила 17 нарушений Кодекса поведения и 13 нарушений Антикоррупционного кодекса: участие в фиксации результатов, передача инсайдерской информации ставочным структурам, вымогательство и принуждение других игроков к мошеннической деятельности [7]. Одновременно аналогичный запрет получил норвежский игрок Томми «Taiga» Ле за систематическую передачу конфиденциальных внутренних данных команды третьим лицам [8]. Оба случая наглядно иллюстрируют, как аккаунт-шаринг создаёт точку входа для коррупции, непосредственно угрожая финансовой и репутационной безопасности всей соревновательной экосистемы.

Второй ключевой вектор — DDoS-атаки на игровую инфраструктуру. Они направлены на три основных цели: домашние подключения игроков в онлайн-матчах; выделенные серверы матчей; трансляционные серверы и серверы операторов турниров. Перегрузка достигается посредством ботнетов, генерирующих интенсивный UDP- или TCP SYN-flood [2]. По данным организации ESTV (2024), 63% профессиональных игроков хотя бы раз сталкивались с DDoS-атакой во время официального матча.

Наиболее показательным инцидентом 2025 года стала атака в финале DreamLeague Season 25 — турнира Dota 2 с призовым фондом 1 млн долларов.

2 марта 2025 года, при счёте 2:1 в пользу Team Spirit в серии до трёх побед, на 18-й минуте четвёртой игры игроки Collapse и Larl внезапно отключились от сервера [11]. По заявлению Collapse, атака реализовывалась путём массовой рассылки приглашений через Steam — до 100 запросов в секунду, что вызывало краш игрового клиента [21]. Попытки продолжить матч на альтернативных аккаунтах оказались безуспешными: атакующий оперативно переключался на новые данные входа. После двухчасовой паузы организатор ESL перенёс оставшуюся часть серии на 4 марта; Team Spirit победила 3:2 [12]. Инцидент выявил структурную уязвимость прикладного уровня: механизм Steam, допускавший неограниченное число уведомлений на аккаунт, использовался как вектор denial-of-service-атаки [21].

Матч-фиксинг образует отдельный, особо опасный класс угроз, нередко сопряжённый с компрометацией учётных записей. Для реализации договорных матчей злоумышленники перехватывают сессионные токены про-игроков: фишинговое письмо или поддельный сайт авторизации через Steam OpenID открывает доступ как к ценному игровому инвентарю, так и к возможности участия от имени игрока в сфальсифицированных встречах [4]. В 2024 году 14 аккаунтов игроков второго дивизиона Dota 2 были скомпрометированы через поддельный сайт регистрации на турнир и использованы для накрутки рейтинга с целью последующей продажи аккаунтов [6]. За 2023 год ESIC вынесла 37 дисквалификаций за матч-фиксинг, включая четыре команды из топ-50 [6]. Совокупный ущерб от подобных схем выражается не только в финансовых потерях участников ставочного рынка, но и в системной девальвации доверия к соревновательным результатам.

Боты в матчмейкинге и смёрфинг формируют устойчивую угрозу целостности рейтинговых систем. Кризис аймбот-ботов в Team Fortress 2 (TF2) — один из наиболее показательных примеров системной уязвимости при недостаточном

внимании разработчика к безопасности. Начиная с конца 2019 года автоматизированные аккаунты массово вторгались в матчи TF2 в роли снайпера, мгновенно уничтожая всех игроков хедшотами и манипулируя системой голосования за исключение через динамическую смену имён [15]. В 2022 году сообщество организовало кампанию #SaveTF2: свыше 200 тысяч игроков подписали петицию [15]. К 2024 году ситуация повторно обострилась. Операторы ботов прибегали к деанонимизации (doxxing), SWAT-атакам и угрозам физического насилия в адрес авторов инструментов по отслеживанию читеров [20]. Это является свидетельством формирования организованного криминального сегмента, эксплуатирующего уязвимости игровых экосистем.

Смёрфинг — создание вторичных аккаунтов опытными игроками для участия в матчах против менее квалифицированных соперников — нарушает принцип честной конкуренции. Для обхода HWID-банов нарушители применяют программные спуферы аппаратных идентификаторов, подделывающие серийные номера материнской платы, идентификаторы дисков и MAC-адреса сетевых карт на уровне ядра ОС [13], что обусловливает непрекращающуюся гонку вооружений между разработчиками античитов и авторами инструментов обхода [14].

Угрозы через каналы связи составляют отдельный вектор, часто недооцениваемый организаторами. В профессиональном киберспорте переговоры несут стратегическую ценность: тактические планы, драфтовые предпочтения и внутренние уязвимости команды. TeamSpeak, при отсутствии шифрования трафика, потенциально уязвим для перехвата: злоумышленник, реализовавший атаку «человек посередине» (MitM) на LAN-сети турнира или перехвативший незащищённое Wi-Fi-соединение, может получать переговоры команды в реальном времени [2]. Discord, как показало дело Tokyogurl, способен применяться непосредственно как вектор для реализации

мошеннических схем: функция Screen Share позволила организовать дистанционное управление персонажем [9]. Несанкционированный доступ к командному серверу Discord раскрывает стратегические документы, пре-драфт обсуждения и персональные данные участников.

Утечки персональных данных с киберспортивных платформ представляют не менее серьёзную угрозу. Платформы FACEIT, ESEA, Nevagg, Fast Cup хранят логины, адреса электронной почты, Steam/Riot ID, IP-адреса входов, платёжные реквизиты, а нередко — номера телефонов и документы верификации. Наиболее значимым документально подтверждённым инцидентом стала утечка данных ESEA в 2016 году, затронувшая более 1,5 миллиона аккаунтов; база данных впоследствии появилась в открытом доступе [3]. В последующие годы ряд региональных платформ также фиксировал случаи несанкционированного доступа. Риски для игроков многообразны: скомпрометированные учётные данные открывают доступ к связанным аккаунтам Steam с дорогостоящим инвентарём; утечка IP-адресов создаёт возможности для целевых DDoS-атак; реальные имена, связанные с игровыми псевдонимами, повышают риски деанонимизации и преследования [5].

Искусственный интеллект формирует принципиально новый класс угроз. Отправной точкой для осмысления его роли стал матч на The International 2017: бот OpenAI победил профессионала Данила «Dendi» Ишутина в формате 1v1 менее чем за 10 минут, демонстрируя нечеловеческую точность микроконтроля [17]. Развитием стал проект OpenAI Five, к 2019 году достигший уровня, позволявшего побеждать чемпионов мира в полноценных матчах 5v5 [16]. Сегодня именно нечеловеческая точность и предсказуемость движений служат маркерами читов в античит-системах. Однако параллельно ИИ применяется для совершенствования мошеннического ПО: читы нового

поколения используют нейросетевые модели для имитации «человеческих» паттернов прицеливания с намеренно внесёнными неточностями, что существенно затрудняет их обнаружение статистическими методами [18]. LLM-модели автоматизируют создание персонализированных фишинговых писем на основе публично доступных данных об игроке. Эти тенденции формируют противостояние двух ИИ-систем — атакующей и защищающейся, которое определит облик кибербезопасности в киберспорте на ближайшее десятилетие [16].

Таблица 1 – Матрица угроз кибербезопасности в профессиональном киберспорте (2024–2026)

Вектор угрозы	**Механизм реализации**	**Приоритет**
Подмена игрока (ghosting)	Дистанционное управление через Discord Screen Share; аккаунт-шаринг	Критический
DDoS на домашний IP игрока	UDP/TCP flood через ботнет; флуд Steam-запросами (до 100/с)	Критический
DDoS на серверы матча	Перегрузка инфраструктуры оператора	Высокий
Аймбот / гипервизорные читы	Чтение памяти ядра; DLL-инъекция; ИИ-имитация паттернов	Высокий
Матч-фиксинг	Подкуп, принуждение, аккаунт-шаринг, компрометация аккаунта	Высокий
Боты в матчмейкинге	Массовые аймбот-аккаунты; HWID-спуферы	Средний
Утечка стратегий (Discord, TeamSpeak)	MitM-перехват; несанкционированный доступ к серверу	Средний
Утечка персональных данных	SQL-инъекция; компрометация БД платформы	Средний
ИИ-фишинг и ИИ-читы	LLM-генерация фишинга; нейросетевые паттерны обхода	Средний

Таким образом, совокупность рассмотренных угроз охватывает как технические, так и организационно-правовые аспекты безопасности киберспортивной отрасли. Угрозы подмены игроков вышли за рамки типичного читерства: дело Tokyogurl продемонстрировало, что

злоумышленники эксплуатируют легитимные инструменты коммуникации в противоправных целях, а правовые механизмы ряда юрисдикций уже распространяются на подобные деяния [10]. DDoS-атаки сохраняют критическую актуальность, поскольку векторы реализуются на прикладном уровне, а не только сетевом [12]. Экосистемные проблемы — кризис ботов в TF2, смёрфинг — требуют активного участия разработчиков: пассивная позиция ведёт к репутационному и коммерческому ущербу [20]. Наконец, ИИ одновременно усиливает как атакующие, так и защитные возможности сторон, формируя принципиально новую динамику угроз, требующую постоянного переосмысления существующих подходов к безопасности [16].

Библиографический список:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. — М.: Машиностроение, 2020. — 508 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение. — М.: ДМК Пресс, 2022. — 434 с.
3. Нестеров С.А. Информационная безопасность и защита информации. — СПб.: Лань, 2022. — 324 с.
4. Ковалёв Д.В., Сизов А.Н. Облачные системы контроля доступа: архитектура и угрозы безопасности // Вопросы кибербезопасности. — 2023. — № 2 (54). — С. 71–82.
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 14.07.2022).
6. ESIC. Annual Report 2023: Incidents and Sanctions in Professional Esports. — London: ESIC, 2024.
7. ESIC Sanction Outcome: Lifetime Ban on Alexandr «Sensability» Filatov. — Режим доступа: https://esic.gg/sanction-outcomes/ (дата обращения: 05.05.2026).

8. ESIC Sanction Outcome: Lifetime Ban on Tommy «Taiga» Le. — Режим доступа: https://esic.gg/sanction-outcomes/ (дата обращения: 05.05.2026).
9. Dexerto. Thai esports player and her boyfriend arrested for cheating after he played instead. — Режим доступа: https://www.dexerto.com/esports/ (дата обращения: 05.05.2026).
10. VnExpress International. Thai esports players Tokyogurl, Cheerio get 3 months detention for cheating at SEA Games. — Режим доступа: https://e.vnexpress.net/ (дата обращения: 05.05.2026).
11. GosuGamers. Team Spirit overcome DDoS attacks and Tundra Esports to win DreamLeague Season 25. — Режим доступа: https://www.gosugamers.net/dota2/news/74435 (дата обращения: 05.05.2026).
12. Esports.gg. DreamLeague S25 grand final postponed mid-series as DDoS attacks strike Dota 2 team. — Режим доступа: https://esports.gg/news/dota-2/ (дата обращения: 05.05.2026).
13. FACEIT Support. Anti-Cheat Smurf Detection FAQ. — Режим доступа: https://support.faceit.com/hc/en-us/articles/16873826012060 (дата обращения: 05.05.2026).
14. FACEIT Support. New Streamlined Smurf Reporting Process. — Режим доступа: https://support.faceit.com/hc/en-us/articles/17006838525852 (дата обращения: 05.05.2026).
15. Windows Central. Over 200,000 Team Fortress 2 players sign #FixTF2 petition. — Режим доступа: https://www.windowscentral.com/gaming/ (дата обращения: 05.05.2026).
16. Wikipedia. OpenAI Five. — Режим доступа: https://en.wikipedia.org/wiki/OpenAI_Five (дата обращения: 05.05.2026).

17. Habr. Бот OpenAI победил трёх топовых профессионалов в Dota 2. — Режим доступа: https://habr.com/ru/articles/405939/ (дата обращения: 05.05.2026).
18. Shazoo. Победа ботов OpenAI над профессионалами в Dota 2. — Режим доступа: https://shazoo.ru/2026/05/03/183342/ (дата обращения: 05.05.2026).
19. SmurfScanner. Faceit & Valve Smurf Ban Policy 2026. — Режим доступа: https://smurfscanner.com/blog/smurf-ban-policy-2026 (дата обращения: 05.05.2026).
20. VideoGamer. Slander, extortion and doxxing — beneath the surface of TF2's bot crisis. — Режим доступа: https://www.videogamer.com/features/ (дата обращения: 05.05.2026).
21. dota2.ru. Что случилось с Team Spirit в гранд-финале DreamLeague Season 25. — Режим доступа: https://dota2.ru/articles/50672 (дата обращения: 05.05.2026).
22. vkplay.ru. Парень играл за девушку на турнирах — пару арестовали по уголовному делу. — Режим доступа: https://vkplay.ru/media/news/ (дата обращения: 05.05.2026).
23. esports.ru. История призовых The International с 2011 по 2025 год. — Режим доступа: https://esports.ru/articles/prizovie-international-dota/ (дата обращения: 05.05.2026).