Секция «1.3 Государственное управление спортом 5.0: от олимпийских стандартов к интеллектуальной системе администрирования»

Цифровая инфраструктура и кибербезопасность в спорте: защита данных, верификация достижений и управление рисками

Научный руководитель – Апольский Евгений Александрович

Малервейн Анжелика Павловна

Студент (специалист)

Всероссийский государственный университет юстиции (РПА Минюста России), Москва, Россия

E-mail: anzhelikamalervein@yandex.ru

Спорт сегодня – это не только мышцы и пот, это огромный поток данных. Мы видим это повсюду: онлайн-трансляции, системы анализа данных, мобильные приложения для болельщиков, носимые устройства, отслеживающие каждый удар сердца спортсмена. Цифровизация проникает во все аспекты спортивной индустрии, делая ее более эффективной, увлекательной и доступной. Но вместе с возможностями приходят и риски.

Спорт в XXI веке переживает эпоху цифровой трансформации. Внедрение цифровых технологий охватывает все аспекты спортивной индустрии – от управления соревнованиями и тренировочного процесса до взаимодействия с болельщиками и монетизации контента. Эта цифровизация открывает новые возможности для развития спорта, но одновременно создает серьезные вызовы в области кибербезопасности и защиты данных.

Сбор и обработка персональных данных спортсменов и зрителей является неотъемлемой частью цифровой инфраструктуры спорта. Эти данные могут включать:

Спортсмены: Медицинская информация, данные о тренировках, геолокация, финансовая информация, личные данные.

Зрители: Имена, адреса электронной почты, номера телефонов, данные о покупках билетов, предпочтения в просмотре, геолокация.

Несанкционированный доступ к этим данным может привести к серьезным последствиям, включая:

• Утечку конфиденциальной информации: Нарушение приватности спортсменов и зрителей.

• Финансовые потери: Кража личных данных и использование их для мошеннических операций.

• Репутационный ущерб: Потеря доверия к спортивным организациям.

• Манипулирование результатами соревнований: Использование данных о спортсменах для нечестной игры.

Для защиты персональных данных необходимо:

- Соблюдение законодательства о защите данных: Внедрение принципов GDPR, CCPA и других соответствующих нормативных актов.

- Внедрение строгих мер безопасности: Использование шифрования, многофакторной аутентификации, систем обнаружения вторжений и других технологий защиты.

- Обучение персонала: Повышение осведомленности сотрудников о рисках кибербезопасности и методах защиты данных.

- Проведение регулярных аудитов безопасности: Выявление и устранение уязвимостей в системе.

- Разработка политики конфиденциальности: Четкое определение правил сбора, обработки и хранения персональных данных.

- Получение согласия на обработку данных: Обеспечение прозрачности и информированности пользователей о том, как используются их данные.

Представьте себе: утечка медицинской информации спортсмена, манипуляции с результатами соревнований, кража данных болельщиков... Звучит как сюжет для триллера, правда? Но это вполне реальные угрозы, с которыми сталкивается спортивный мир. И речь идет не просто о деньгах, речь идет о репутации, о честности соревнований, о доверии миллионов фанатов.

Статистика неутешительна. Количество кибератак на спортивные организации растет экспоненциально. Почему? Потому что мы – лакомая цель. У нас есть ценные данные, мы зависим от цифровых систем, и часто, к сожалению, недостаточно защищены.

Давайте поговорим о данных. Что мы собираем? Медицинские карты спортсменов, их тренировочные данные, финансовую информацию, личные контакты. А что насчет болельщиков? Имена, адреса, номера телефонов, предпочтения в просмотре... Это огромный массив информации, который требует надежной защиты. Представьте, что произойдет, если эти данные попадут в чужие руки. Это не просто нарушение приватности, это потенциальный удар по карьере спортсмена и по репутации всей организации.

Но есть и хорошие новости! Технологии приходят на помощь. Блокчейн – это не просто криптовалюта, это революционная технология, которая может изменить правила игры в спорте. Представьте себе: результаты соревнований, записанные в блокчейн, невозможно подделать. Цифровые паспорта спортсменов с верифицированной информацией. Прозрачная система управления билетами, исключающая спекуляции. Блокчейн– это гарантия честности и прозрачности.

Но блокчейн – это лишь один из инструментов. Для защиты цифровых платформ управления спортом нам нужен комплексный подход. Это как строительство крепости: нужны мощные стены (брандмауэры), надежные ворота (многофакторная аутентификация), бдительные стражи (системы обнаружения вторжений) и постоянный мониторинг.

Ключевым нормативным актом в большинстве юрисдикций является законодательство, основанное на принципах GDPR (General Data Protection Regulation) Европейского Союза. Это означает, что спортивные организации обязаны обеспечивать законность, справедливость и прозрачность обработки данных, собирать только необходимые данные для конкретных целей, обеспечивать точность и актуальность данных, а также обеспечивать их безопасность. Нарушение этих принципов может привести к значительным штрафам, установленным законодательством.

Угрозы кибербезопасности, такие как хакерские атаки, утечки данных, вирусы-вымогатели и фишинговые атаки, представляют собой прямую угрозу соблюдению законодательства о защите данных. Утечка персональных данных спортсменов или болельщиков может повлечь за собой ответственность в соответствии с законодательством о защите персональных данных, включая обязательство уведомления уполномоченных органов и пострадавших лиц, а также выплату компенсаций.

С юридической точки зрения, спортивные организации должны:

Разработать и внедрить политику конфиденциальности: Политика должна четко определять, какие данные собираются, как они используются, кому они передаются и как обеспечивается их безопасность.

Получить согласие на обработку данных: В случаях, предусмотренных законодательством, необходимо получить явное и информированное согласие субъектов данных на обработку их персональной информации.

Обеспечить безопасность данных: Внедрение технических и организационных мер для защиты данных от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Это включает в себя использование шифрования, межсетевых экранов,

антивирусного программного обеспечения и систем обнаружения вторжений.

Заключить договоры с обработчиками данных: Если спортивная организация передает обработку данных третьим лицам (например, поставщикам облачных услуг), необходимо заключить с ними договоры, обеспечивающие соблюдение требований законодательства о защите данных.

Разработать план реагирования на инциденты безопасности: План должен определять порядок действий в случае утечки данных или другого инцидента безопасности, включая уведомление уполномоченных органов и пострадавших лиц.

Проводить регулярные аудиты безопасности: Аудиты позволяют выявить уязвимости в системе безопасности ипринять меры по их устранению.

Кроме того, спортивные организации должны учитывать специфические правовые аспекты, связанные с обработкой медицинских данных спортсменов, которые подлежат особому режиму защиты. Также важно учитывать требования законодательства об интеллектуальной собственности при защите прав на трансляции и результаты соревнований.

И самое главное – сотрудничать! Обмениваться опытом, делиться информацией об угрозах, привлекать экспертов по кибербезопасности. Кибербезопасность – это не задача одного человека или одной организации, это общая ответственность.

Защита от киберугроз – это не просто установка антивируса. Это комплексный подход, который включает в себя:

Технические меры: Брандмауэры, системы обнаружения вторжений, шифрование данных, многофакторная аутентификация.

Организационные меры: Разработка политики безопасности, обучение персонала, проведение аудитов безопасности.

Правовые меры: Соблюдение законов о защите данных, страхование киберрисков.

Спорт всегда был передовым в использовании технологий. Вспомните первые трансляции по радио, потом по телевидению. Но сейчас мы переживаем настоящую цифровую революцию. Посмотрите на эти цифры: миллиарды долларов инвестиций в спортивные технологии, миллионы пользователей мобильных приложений, петабайты данных, генерируемые каждый день.

Что это значит на практике? Носимые устройства отслеживают физическое состояние спортсменов, позволяя оптимизировать тренировки и предотвращать травмы. Виртуальная и дополненная реальность переносят болельщиков на трибуны, даже если они находятся за тысячи километров. Аналитика данных помогает командам разрабатывать тактику и выявлять слабые места соперников. Электронные билеты упрощают доступ к соревнованиям и предотвращают подделку. Все это делает спорт более захватывающим, эффективным и доступным.

Но за всем этим стоит огромный объем данных. Данные о здоровье, тренировках, финансах, личной жизни спортсменов. Данные о предпочтениях, покупках и местоположении болельщиков. Этот "цифровой след" – ценный актив, но и огромная ответственность.

Утечка данных о здоровье спортсменов, взлом систем продажи билетов, манипуляции с результатами соревнований. Эти инциденты наносят огромный ущерб репутации и финансовым интересам спортивных организаций. Цена ошибки может быть очень высокой. Финансовые потери, репутационный ущерб, юридические последствия, потеря доверия болельщиков. И самое главное – подрыв честности соревнований.

Спорт в цифре – это захватывающее будущее. Но это будущее требует от нас ответственности и бдительности. Защищая данные, обеспечивая прозрачность и борясь с киберугрозами, мы защищаем честность соревнований, доверие болельщиков и саму суть спорта. Давайте вместе построим безопасный и надежный спортивный мир! Спасибо за внимание!

В заключение, обеспечение кибербезопасности и защита данных в спорте – это не только техническая, но и юридическая необходимость. Соблюдение законодательства о защите персональных данных, разработка и внедрение соответствующих политик и процедур, а также регулярный мониторинг и аудит безопасности являются лючевымиэлементами эффективной защиты информации и предотвращения юридической ответственности. Несоблюдение этих требований может привести к серьезным последствиям для спортивных организаций, включая финансовые штрафы, потерю репутации и судебные разбирательства.

Источники и литература

1) Кирьянова Людмила Александровна, Морозова Лада Владимировна, and Кузнецов Павел Константинович. "Информационная безопасность в сфере физической культуры и спорта" Ученые записки университета им. П. Ф. Лесгафта, no. 9 (163), 2018, pp. 144-148.
2) Гранкина Я.А., Баймедетов С.Д.. "КИБЕРБЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ: АКТУАЛЬНЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ" Вестник науки, vol. 1, no. 11 (80), 2024, pp. 864-870.
3) Рыбаков Д.А. РАЗВИТИЕ И ПРИМЕНЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ // Вестник науки №7 (64) том 5. С. 267 - 272. 2023 г.
4) Исупова, Т. Н. Формирование компетенций в области информационной безопасности при изучении дисциплины «Информационные технологии и информационная безопасность» студентами вуза / Т. Н. Исупова, М. С. Перевозчикова // Вестник гуманитарного образования. – 2017. – № 3. – С. 41-43
5) Сухомлин, В. А. Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, А. А. Русанов // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 695-710.