КИБЕРСИГУРНОСТ И УПРАВЛЕНИЕ НА ДАННИ В СЪВРЕМЕННИЯ СПОРТ

Петър Йорданов

Национална спортна академия „Васил Левски“,

катедра „Тежка атлетика, бокс, фехтовка и спорт за всички“

ORCID

Petar Jordanov – https://orcid.org/0000-0003-3860-6019

РЕЗЮМЕ

Съвременният спорт разчита на информационни системи за управление на събития, онлайн тренировки и комуникация със спортисти, което води до нови предизвикателства пред киберсигурността и защитата на данните. Тези системи събират и обработват чувствителна информация за участници, организатори и зрители, налагайки необходимостта от стриктна защита на данните. Настоящият доклад разглежда основните киберрискове в спортния сектор, подходите за управление на данни и предлага методи за повишаване на сигурността. Чрез прилагането на подходи като анализ на заплахи, тестове за проникване и симулации на кибератаки се идентифицират уязвимости и се предоставят препоръки за ефективно управление на данните.

Целта на настоящото изследване е да анализира основните киберрискове, свързани с управлението на данни в спортния сектор, и да предложи подходящи методи за тяхното предотвратяване. Предметът на изследването обхваща процесите по управление на данни и киберсигурност в спортните информационни системи. Обект на изследването са дигиталните платформи, използвани от спортни организации и спортисти, както и произтичащите от тях уязвимости. За целите на изследването са приложени различни методи, включително анализ на заплахи, тестове за проникване и симулации на кибератаки.

Ключови думи: *киберсигурност, спорт, данни, защита, събития, киберзаплахи*

CYBERSECURITY AND DATA MANAGEMENT IN MODERN SPORTS

Petar Yordanov

National Sports Academy “Vassil Levski”,

Department of Heavy athletics, boxing, fencing and sport for all

ABSTRACT

Modern sports rely on information systems for event management, online training, and athlete communication, leading to new challenges in cybersecurity and data protection. These systems collect and process sensitive information about participants, organizers, and spectators, necessitating strict data protection. This report examines the main cyber risks in the sports

sector, data management approaches, and offers methods to enhance security. By applying approaches such as threat analysis, penetration testing, and cyber-attack simulations, vulnerabilities are identified, and recommendations are provided for effective data management.

The aim of this study is to analyze the primary cyber risks associated with data management in the sports sector and to propose appropriate prevention methods. The subject of the research encompasses data management processes and cybersecurity in sports information systems.

The object of the study includes the digital platforms used by sports organizations and athletes, as well as the vulnerabilities arising from their use. The applied methods include threat analysis, penetration testing, and cyberattack simulations.

Keywords: *cybersecurity, sports, data, protection, events, cyber threats*

ВЪВЕДЕНИЕ

С нарастващата дигитализация на спортния сектор киберсигурността се превръща във все по-критична област, особено що се отнася до защита на личните данни и предотвратяване на потенциални заплахи. Много от съвременните спортни организации използват разнообразни платформи и информационни системи за управление на събития, осъществяване на комуникация с атлети, събиране на данни за зрители и организиране на онлайн тренировки (Йорданов, 2023). Например, платформи като Strava и MyFitnessPal съхраняват огромно количество лична информация, като физическа активност, здравни данни и геолокации. Наличието на такъв тип чувствителни данни създава привлекателна цел за кибератаки, тъй като атакуващите могат да използват тези данни за различни престъпни дейности – от финансови измами до шантаж (Йорданов, 2022).

През последните години редица спортни организации са станали жертва на кибератаки, които показват колко уязвим може да бъде този сектор (Петров, 2023). През 2020 г. например една от водещите платформи за продажба на билети за спортни събития беше атакувана, което доведе до изтичане на лични данни на стотици хиляди потребители. Подобен инцидент подчертава значението на надеждната защита на данните и необходимостта от въвеждане на стриктни мерки за киберсигурност в спортния сектор.

Настоящият доклад има за цел да изследва основните предизвикателства пред киберсигурността и управлението на данни в спорта, както и да предложи стратегии и методи за защита, които да предотвратят инциденти и да осигурят целостта на личната информация. Чрез прилагането на съвременни подходи за защита и управление на данни спортните организации могат да минимизират рисковете и да гарантират сигурността на своите информационни системи.

Целта на настоящото изследване е да определи основните киберрискове, свързани с управлението на данни в спортния сектор, и да предложи мерки за тяхното минимизиране.

Предметът на изследването обхваща процесите по управление на данни и киберсигурност в спортните информационни системи.

Обект на изследването са информационните платформи, използвани от спортни организации, треньори и спортисти, както и уязвимостите, произтичащи от тяхната дигитализация.

МЕТОДИКА

За целите на изследването са приложени няколко метода за анализ на киберсигурността и управлението на данни, включително анализ на заплахи (Threat Modeling), тестове за проникване (Penetration Testing) и симулации на кибератаки (Cyberattack Simulations). Тези методи позволяват идентифициране на уязвимостите в информационните системи и оценка на нивото на сигурност на платформите, използвани в спортния сектор.

В доклада се използват следните методи за анализ на киберсигурността и управлението на данни в спорта:

1. Анализ на заплахи (Threat Modeling). Използването на моделиране на заплахите предоставя метод за систематично идентифициране на възможните киберрискове в спортния сектор. Това включва разглеждане на всички възможни заплахи – от зловреден софтуер до неоторизиран достъп и ***социално инженерство***. Чрез този метод спортните организации могат да предвидят потенциалните уязвимости и да предприемат мерки за тяхното минимизиране (Йорданов и кол., 2023).

2. Тестове за проникване (Penetration Testing). Тези тестове имат за цел да симулират реални кибератаки върху информационните системи на спортните организации, за да се оценят нивото на сигурност и съществуващите слабости. Например, тестването може да се фокусира върху достъпа до данни на потребителите, сигурността на платформите за онлайн продажба на билети или защитата на мрежовата инфраструктура в спортните центрове. Чрез тези тестове се откриват слабости, които могат да бъдат коригирани, преди да бъдат използвани от злонамерени лица.

3. Анализ на най-добри практики (Benchmarking). Чрез анализ на добри практики от други сектори, като финансовия и здравния, спортните организации могат да идентифицират иновативни и ефективни мерки за сигурност. Например, финансовите институ-

ции прилагат високо ниво на криптиране за чувствителни данни и многослойни механизми за автентикация, които могат да бъдат внедрени и в спортния сектор. Така спортните организации могат да се възползват от успешни подходи за защита, доказани в други индустрии.

4. Оценка на осведомеността за сигурността (Security Awareness Assessment). Чрез анкети и интервюта със спортисти и персонал спортните организации могат да получат по-добра представа за нивото на осведоменост за киберзаплахите. Тези проучвания могат да разкрият пропуски в знанията на служителите относно основни мерки за защита на данни, което налага необходимостта от обучение и повишаване на културата за киберсигурност.

5. Анализ на съответствие със законови и регулаторни изисквания (Compliance Analysis). Този метод включва проверка на съответствието с важни законови и регулаторни рамки, като например GDPR за защита на личните данни в ЕС (e-Security.bg, 2023). За спортните организации, които оперират на международно ниво, спазването на тези изисквания е от съществено значение, за да се избегнат глоби и санкции (K. & Partners, 2024).

6. Мониторинг и анализ на инциденти (Incident Monitoring and Analysis). Следенето и анализът на инциденти, свързани с киберсигурността, могат да разкрият повтарящи се проблеми и слабости в сигурността. В спорта е важно да се установят практики за навременна реакция и управление на инциденти, което ще позволи минимизиране на щетите при евентуална атака.

7. Симулации на кибератаки (Cyberattack Simulations). Провеждането на симулации на кибератаки помага на спортните организации да проверят своята реактивна способност и да оценят готовността на персонала при потенциални заплахи (Йорданов, 2023). Чрез редовни симулации могат да се открият слабости и да се подобрят процедурите за реакция при кризи. Използваните методи за изследване са представени в Таблица 1, където са посочени целта и приложението им в спортния сектор. Чрез тях се разпознават основни уязвимости и се повишава сигурността на информационните системи.

За обработка на събраните данни в настоящото изследване са използвани следните математико-статистически методи:

Корелационен анализ. Прилаган е за установяване на връзките между различни променливи, свързани с нивото на сигурност и осведомеността за киберрискове. Този метод позволява да се изследват зависимостите между фактори като осведоменост на персонала и прилагане на защитни мерки.

Регресионен анализ. Използван е за прогнозиране на вероятността от кибератаки, базирайки се на различни фактори, като защитни мерки и идентифицирани уязвимости в спортните информационни системи. Чрез регресионния анализ са установени факторите, които най-силно влияят върху вероятността за пробив в сигурността.

Анализ на честотите. Приложен е за идентифициране на повтарящи се модели и най-често срещаните уязвимости в информационните системи на спортни организации. Този анализ позволява да се разкрият тенденциите в уязвимостите и да се насочат препоръките за подобрения.

Комбинацията от тези методи предоставя надеждни количествени данни, които подкрепят анализа на киберсигурността и предлаганите препоръки. Чрез тях се разпознават основни уязвимости и се повишава сигурността на информационните системи.

Таблица 1. *Методи за изследване на киберсигурността в спорта*

Метод	Цел/Фокус	Приложение в спорта
Анализ на заплахи	Идентифициране на потенциални рискове	Оценка на рискове за данните на спортистите
Тестове за проникване	Откриване на уязвимости	Проверка на сигурността на платформите и инфраструктурата
Анализ на най-добри практики	Сравнение с други сектори	Внедряване на успешни стратегии за сигурност от финансовия сектор
Оценка на осведомеността	Измерване на знания за киберзаплахи	Определяне на нивото на информираност за киберрискове и нуждата от обучения
Анализ на съответствие	Спазване на законови изисквания	Съответствие с GDPR и други регулаторни рамки
Мониторинг и анализ на инциденти	Идентифициране и анализ на повтарящи се проблеми	Оценка на реакцията на организациите при инциденти и установяване на слабости
Симулации на кибератаки	Тестване на реактивна способност при кибератаки	Оценка на готовността за отговор при потенциални заплахи

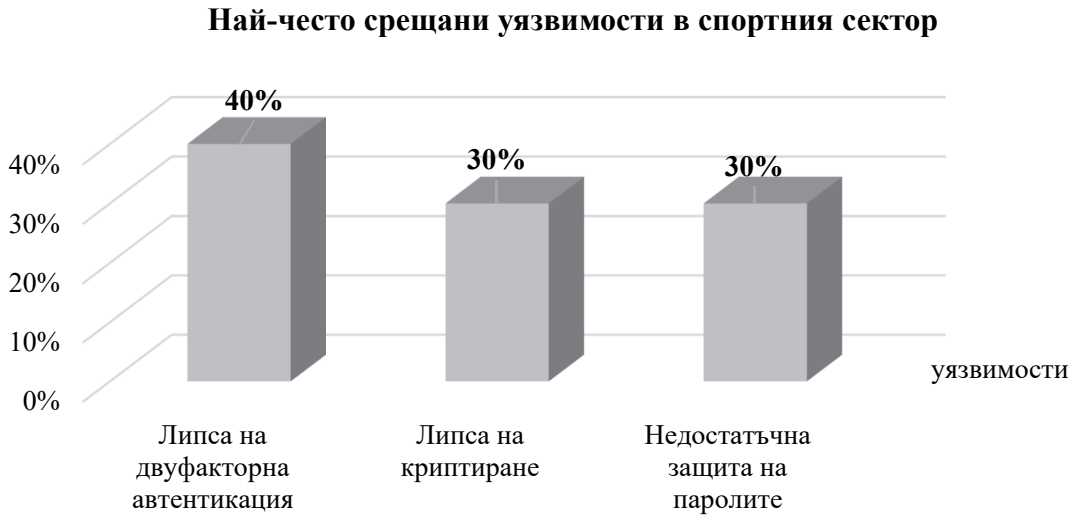
РЕЗУЛТАТИ

Данните в настоящото изследване бяха събрани чрез комбиниран подход, включващ анкетно проучване сред спортисти и треньори, както и тестове за проникване в използваните информационни системи. Анкетата включваше въпроси, свързани с нивото на осведоменост по отношение на киберрисковете, използването на защитни механизми като двуфакторна автентикация, както и практики за сигурност като разпознаване на фишинг атаки и избора на сигурни пароли. Резултатите от анкетата допълват анализа на данните от тестовете за проникване, които целят да идентифицират основни уязвимости в информационните системи на спортните организации.

Проучването на сигурността в спортния сектор показа, че редица информационни системи и приложения, използвани за управление на спортни събития, имат значителни уязвимости, които могат да се използват от злонамерени лица. Чрез проведените тестове за проникване бяха открити няколко основни слабости:

- Липса на криптиране на чувствителни данни, като лични данни на спортисти и резултати от тренировки.
- Недостатъчна защита на паролите и липса на двуфакторна автентикация в повечето платформи.
- Неправилна настройка на мрежовата инфраструктура, която позволява лесен достъп до базите данни.

Анкетите сред спортисти и треньори показаха, че по-голямата част от участниците не разполагат с базови познания за киберсигурността. Мнозина не са запознати с рисковете от фишинг атаки и не знаят как да защитят данните си. Освен това, някои спортни организации не прилагат стандартни протоколи за защита на данни, което увеличава риска от изтичане на информация. Тези резултати показват спешната нужда от обучение и повишаване на културата за сигурност в спорта. Чрез проведените тестове за проникване бяха идентифицирани основни слабости в сигурността, включително липса на криптиране, липса на двуфакторна автентикация и неправилна настройка на мрежовата инфраструктура (Фигура 1).



Фигура 1. *Най-често срещани уязвимости в спортния сектор*

ДИСКУСИЯ

Разгледаните резултати подчертават, че спортният сектор е по-уязвим в сравнение с институции като финансовата или здравния сектор, където сигурността на данните е приоритет. Въпреки наличието на съвременни технологии за защита, спортните организации често изостават поради ограничените ресурси и липсата на достатъчна информираност относно възможните рискове.

Един от основните проблеми е социалното инженерство, което лесно засяга служители без опит в киберсигурността. Затова е важно да се прилагат обучения за разпознаване на фишинг атаки и други методи на ***социално инженерство*** (Георгиев, 2024).

Освен това, спортните организации могат да се възползват от опита на финансовите институции, като прилагат многослойни мерки за защита, включително криптиране, двуфакторна автентикация и редовен мониторинг на мрежовия трафик. На база резултатите, социалното инженерство, техническите уязвимости и човешките грешки представляват основни рискове за киберсигурността в спортния сектор (Фигура 2). Тези рискове са илюстрирани в разпределението, представено на фигурата.

Фигура 2. *Разпределение на риска в спортния сектор*

ЗАКЛЮЧЕНИЕ

Настоящият доклад акцентира върху нарастващата необходимост от засилено внимание към аспектите на киберсигурността и управлението на данни в спортния сектор. С нарастващата дигитализация на спорта защитата на личните данни на спортисти и организатори придобива все по-голямо значение предвид увеличаващите се рискове, свързани с киберзаплахи. В съответствие с препоръките на Ангелова (2024), балансираният

подход към киберсигурността е от решаващо значение, като същевременно се обръща внимание на бързата дигитална трансформация и свързаните с нея предизвикателства за защита на данните. Посредством тези мерки организациите могат да повишат нивото си на подготвеност спрямо киберзаплахи и да осигурят цялостна защита на своите информационни системи.

Увеличаващата се употреба на дигитални платформи и технологични решения в спорта изисква изграждането на цялостна стратегия за киберзащита, съчетаваща технически и организационни подходи. Това включва утвърдени политики за сигурност, протоколи за реакция при инциденти и съвременни механизми за защита на личните данни. Прилагането на тези мерки е съществено не само за минимизиране на кибератаките, но и за укрепване на доверието на всички заинтересовани страни, включително спортисти, организатори и публика.

В допълнение, спортният сектор следва да насърчава сътрудничеството с представители на други институции, като финансовата и здравния сектор, където практиките за киберсигурност вече са добре развити (Насоки за киберсигурност…, 2024). Междусекторната колаборация би могла да способства за пренасяне и адаптиране на ефективни практики за сигурност, което от своя страна би допринесло за създаването на по-устойчиви и сигурни информационни екосистеми в спорта.

ЛИТЕРАТУРА

Ангелова, Е. (2024). Предизвикателства пред киберсигурността в условията на дигитална трансформация. *Икономически алтернативи*, 123–132. //Angelova, E. (2024). Predizvikatelstva pred kiber sigurnostta v usloviyata na digitalna transformatsiya. *Ikonomicheski alternativ*i, 123–132.

Георгиев, А. (15 ноември 2024 г.). *Насоки за защита на данните в спортните клубове*. Извлечено от: https://www.cybersecurity.bg/sport-data-protection // Georgiev, A. (2024). *Nasoki za zashtita na dannite v sportnite klubove.* Izvlecheno ot https://www.cybersecurity.bg/sport-data-protection

Йорданов, П. (2022). Нарастващото значение на киберсигурността в спорта. *Годишник на Национална спортна академия „Васил Левски“. Том 2*. НСА ПРЕС, София, 35–44. // Yordanov, P. (2022). Narastvashtoto znachenie na kiber sigurnostta v sporta. *Godishnik na Nacionalna sportna akademiya* „Vassil Levski“, *Tom 2.* NSA PRES, Sofia, 35–44.

Йорданов, П., Колева, Н. (2023). Онлайн тренировки и киберсигурност: потенциални заплахи и превенция. *Стратегии на образователната и научната политика*, 73–80. //

Yordanov, P., Koleva, N. (2023). Onlayn trenirovki i kiber sigurnost: Potentsialni zaplahi i preventsiya. *Strategii na obrazovatelnata i nauchnata politika*, 73–80.

Йорданов, П., Кленовска, Н., Михайлов, И. (2023). Киберсигурността в спорта: предизвикателства и решения. *Годишник на Национална спортна академия. Том 2.* НСА ПРЕС, София, 142–149. // Yordanov, P., Klenovska, N., Mihaylov, I. (2023). Kibersigurnostta v sporta: predizvikatelstva i reshenia. *Godishnik na Natsionalna sportna akademia. Tom 2.* NSA PRES, Sofia, 142–149.

Йорданов, П., Колева, Н. (2023). Киберсигурност в спорта: предизвикателства и решения. *e-Security.bg*, // Yordanov, P., Koleva, N. (2023). Kibersigurnost v sporta: Predizvikatelstva i resheniya. *e-Security.bg*. Извлечено от https://annual.nsa.bg/wp-content/uploads/2024/10/Kiber-sigurnostta-v-sporta-predizvikatelstva-i-resheniya.pdf

Насоки за киберсигурност в спортния сектор. (2024). Извлечено от Съвет на ЕС: https://www.consilium.europa.eu/bg/documents-publications/ // *Nasoki za kiber sigurnost v sportniya sektor.* (2024). Izvlecheno ot https://www.consilium.europa.eu/bg/documents-publications/

Олимпийските игри: Как да защитим киберсигурността на спортните организации. (2024). Извлечено от e-security.bg/articles/olimpijskite-igri-kak-da-zasthitim-

kibersigurnostta-na-sportnite-organizaczii// Olimpijskite igri: Kak da zashtitim kiber sigurnostta na sportnite organizatsii. (2024).//e-security.bg/articles/olimpijskite-igri-kak-da-zasthitim- kibersigurnostta-na-sportnite-organizaczii/

Петров, И. (2023). *Киберсигурност в спорта: стратегии и практики.* Техника. // Petrov, I. (2023). *Kiber sigurnost v sporta: Strategii i praktiki*. Tehnika.

K. & Partners (2024). *Медии, развлечения и спорт*. Извлечено от https://www.kambourov.biz/bg/capabilities/industry/media-entertainment-sports // Partners, K., & Kambourov, B. (2024). Medii, razvlecheniya i sport. Izvlecheno ot https://www.kambourov.biz/bg/capabilities/industry/media-entertainment-sports

Адрес за кореспонденция:

Петър Йорданов

Национална спортна академия „Васил Левски“,

катедра „Тежка атлетика, бокс, фехтовка и спорт за всички“

E-mail: jordanovpetar687@gmail.com