# КИБЕРСИГУРНОСТТА В СПОРТА: ПРЕДИЗВИКАТЕЛСТВА И РЕШЕНИЯ

**Петър Йорданов*, Нина Кленовска, Ивайло Михайлов**
Национална спортна академия „Васил Левски“,
катедра „Тежка атлетика, бокс, фехтовка и спорт за всички“

**ORCID**
Petar Yordanov – https://orcid.org/0000-0003-3860-6019
Nina Klenovska – https://orcid.org/0009-0009-9075-5717
Ivailo Mihailov – https://orcid.org/0009-0001-0585-3390

**РЕЗЮМЕ**

Киберсигурността в спорта е важна тема, която става все по-актуална и е съсредоточена около защитата на спортните системи и личните данни на спортистите. Целта на това проучване е да се анализират предизвикателствата и решенията в областта на киберсигурността в спорта. Предмет на изследването е киберсигурността в спорта, а обект са информационните активи и системи в сферата на спорта, изложени на киберсигурностни заплахи, и средства за тяхната защита.

За реализирането на целта използвахме комплексна методика, която включва изследване и анализ на наличната литература, качествени и количествени методи. След обработка на анализа на данните от това проучване установихме, че спортната индустрия е уязвима на кибератаки, особено в онлайн системите и финансовите трансакции, които могат да доведат до парични загуби и компрометиране на личните данни на клиентите. Заключение: за подобряване на киберсигурността в спорта е важно да се използват подходящи решения чрез създаване на ефективни системи за защита на данните, провеждане на обучения на персонала по киберсигурност и системи за тестване. Прилагането на такива мерки може да предотврати кибератаки и да гарантира безопасността на информацията в спортната индустрия.

***Ключови думи:*** *кибератака, киберзащита, киберсигурност, криптография*

# CYBERSECURITY IN SPORT: CHALLENGES AND SOLUTIONS

**Petar Yordanov*, Nina Klenovska, Ivaylo Mihaylov**
National Sports Academy „Vassil Levski”,
Department of Heavy athletics, boxing, fencing and sport for all

**ABSTRACT**

Cybersecurity in sport is an important topic that is becoming more relevant in the world of sport and is centered around the protection of sports systems and athletes' personal data. The aim of this study is to analyze cybersecurity challenges and solutions in sport. The subject of the study is cyber security in sports, and the object is information assets and systems in the field of sports exposed to cyber security threats and means of their protection.

For the realization of the goal we used a complex methodology, which included research and analysis of the available literature, qualitative and quantitative methods. After processing the data analysis of this study, we found that the sports industry is vulnerable to cyberattacks, especially in online systems and financial transactions, which can lead to monetary losses and compromise of customers' personal data. Conclusion: To improve cybersecurity in sport, it is important to use appropriate solutions by creating effective data protection systems, conducting trainings for cybersecurity staff and testing systems. Implementing such measures can prevent cyber-attacks and ensure the safety of information in the sports industry.

***Keywords:*** *cyberattack, cyber protection, cybersecurity, cryptography*

**ВЪВЕДЕНИЕ**

Информационната сигурност в спорта е важна тема, която става все по-актуална в и е съсредоточена около защитата на спортните системи и личните данни на спортистите. Киберсигурността играе все по-значима роля в спортния свят, като запазването на сигурността на информационните системи и данните се превръща в приоритет за спортните организации.

Според доклад на National Cyber Security Centre кибератаките срещу спортни организации и събития са нарастваща тенденция в последните години (Martin, Robertson, 2020) . През 2022 г. са регистрирани над 200 кибератаки, засягащи спортните федерации и организации по света. Най-често използваните техники за атаки са Business Email Compromise (BEC), cyber-enabled fraud и ransomware (Martin, Robertson, 2020; Bogle, 2021; Chichester, et al., 2020). Кибератаките могат да имат различни последствия – от мултимилионни измами до загуба на лични данни. За да подобрят киберсигурността си, спортните организации трябва да прилагат ключови технически контроли и да следват ръководствата за управление на риска (Martin, Robertson, 2020).

Кибератаките са сериозна заплаха за спортните федерации и състезателите. Целта на атаките често е кражбата на чувствителни данни, като лични данни на спортистите, финансова информация и стратегически данни за съревнования. Спортните федерации също са цел на чести атаки, насочени срещу техния уебсайт и социални медии.

Кибератаките срещу спортните организации могат да доведат до сериозни икономически загуби. Според едно проучване 70% от спортните организации са били жертва на кибератаки, като 30% от тези атаки са причинили директни финансови щети, като загуба на спонсорски договори и приходи от билети и медийни права (Martin, Robertson, 2020).

Без съмнение кибератаките срещу спортните организации могат да доведат до сериозни последици. Регулаторните органи в много страни са въвели по-строги изисквания

по отношение на киберсигурността за спортните организации, за да гарантират, че те са защитени от потенциални кибератаки (Martin, Robertson, 2020).

Кибератаките могат да навредят на репутацията на спортните организации и на състезателите. Публикуването на чувствителна информация или скандали може да нанесе непоправима щета на имиджа на спорта (Sanna, 2023).

За да се защитят от кибератаки, спортните организации са принудени да инвестират значителни средства в решения за киберсигурността и обучение на служителите си (Doyle, 2021; Ataman, 2023; Sundaresan, 2021).

**ЦЕЛ**

Целта на настоящото проучване е да анализира заплахите и предизвикателствата, свързани с киберсигурността в сферата на спорта, и да предостави решения и препоръки за подобряване на киберсигурността в този контекст.

**МЕТОДИКА**

Целта на изследването е да се проучат предизвикателствата, пред които е изправен спортът в контекста на киберсигурността, както и да се предложат решения за тяхното преодоляване. Предмет на изследването е киберсигурността в спорта, а обект са информационните активи и системи в сферата на спорта, изложени на киберсигурностни заплахи и средства за тяхната защита.

За провеждане на изследването се приложи комплексен методологичен подход, обхващащ анализ на налични статистически данни, проучване на актуални случаи на кибератаки в сферата на спорта, както и преглед на научни публикации от различни източници.

Анализът на налични статистически данни предостави ценна информация относно обхвата и тенденциите на киберсигурността в спорта. Този подход позволи извличането на количествени данни, които са от съществено значение за разбирането на обхвата на проблема.

Извършихме обширно проучване на актуални случаи на кибератаки, настъпили в областта на спорта. Това позволи анализ на конкретни случаи и разглеждане на техните характеристики, както и установяване на общи тенденции в такива събития.

За анализ на научните публикации бяха използвани различни научни ресурси, включително Google Scholar, Researchgate, IEEE Xplore, Scopus и други. Това даде възможност за извличане на ключови концепции, методи и практики, свързани с киберсигурността в спорта. Публикациите предоставиха и информация относно актуалните механизми и политики за киберсигурност в този контекст.

След провеждането на анализите бяха формулирани препоръки за подобряване на сигурността в областта на спорта. Тези препоръки включват предложения за стандарти за сигурност, обучение на потребителите, създаване на осведомителни кампании и насърчаване на отговорното поведение в онлайн средата. Те са разработени на базата на съчетаването на данните от различните източници и на актуалния контекст на киберсигурността в спорта.

## РЕЗУЛТАТИ

Чрез анализ на релевантната литература обобщихме основните предизвикателства и заплахи, които възникват при използването на информационните технологии, поддържащи спортни мероприятия (Таблица 1).

**Таблица 1.** *Предизвикателства и заплахи при спортните мероприятия*

| **Предизвикателства и заплахи** | **Описание** |
|---|---|
| Киберсигурност | Хакерски атаки: включват опити за неоторизиран достъп до спортни системи и бази данни. |
| | Зловреден софтуер: вируси и малуер могат да заразят системите и да предизвикат щети. |
| Интернет връзка | Съпътстващите услуги: висок брой зрители и участници може да претоварят интернет връзката. |
| | Инфраструктура: недостатъчната или неадекватна инфраструктура може да доведе до прекъсване на връзката. |
| Защита на данните | Лични данни: събирането и съхранението на лични данни изискват строги мерки за защита. |
| | Интелектуална собственост: онлайн предаванията и данните за събитията трябва да бъдат защитени от пиратство и незаконно използване. |
| Издръжливост и надеждност | Системни бъгове: технически бъгове могат да доведат до прекъсване на събитието и загуба на доходи. |
| | Загуба на данни: загубата на данни може да окаже влияние върху резултатите и репутацията на събитието. |
| Възможни саботажи и манипулации | Манипулации с данни: възможността за манипулиране на резултати и статистика може да влоши интегритета на спортното събитие. |
| | Допинг контрол: технологични средства могат да бъдат използвани за измама на допинг контрола. |
| Съответствие и правни въпроси | Законодателство за защита на данните: събирането и обработката на данни трябва да бъдат съобразени със законовите изисквания. |
| | Права върху съдържание и марки: използването на спортни лога и съдържание изисква съобразяване с авторското право и търговските марки. |
| Инфраструктура и оборудване | Оборудване за предаване: необходимо е инвестиране в съвременно и надеждно оборудване за предаване на събитията. |
| | Обновление и поддръжка: технологичната инфраструктура трябва да се поддържа актуална и надеждна. |
| Онлайн злоупотреби и незаконно съдържание | Обидни коментари и нарушения на поведението: социалните мрежи и онлайн платформи могат да бъдат използвани за неподходящи коментари и поведение по време на събитията. |
| | Незаконно съдържание: може да се злоупотреби с излъчването с цел показване на незаконно или неподходящо съдържание. |

Прегледахме актуалните мерки и решения и проучихме текущото състояние на киберсигурността в спорта (Фигура 1 и Таблица 2).


**Фигура 1.** *Процентно съотношение на използването на мерките за киберсигурност в спорта*

**Таблица 2.** *Мерки за киберсигурност в спорта*

| **Мерки за киберсигурност** | **Описание** |
|---|---|
| Обучение на персонала | Организиране на обучения и информационни кампании, за да се научат служителите и спортистите как да разпознават потенциални киберзаплахи и как да действат при тях. |
| Антивирусни програми | Инсталиране на актуални антивирусни програми и редовно актуализиране на техните дефиниции на всички компютърни системи и устройства. |
| Файъруол за мрежова сигурност | Използване на файеруол софтуер и/или хардуер, за да се предотврати неоторизиран достъп до мрежата и компютрите. |
| Силни пароли и двуфакторна автентикация | Изискване на сложни пароли и активиране на двуфакторна автентикация за всички акаунти и устройства, свързани със спортния клуб или организация. |
| Резервни копия и възстановяване на данни | Редовно правене на резервни копия на важните данни и файлове, както и тестване на процедурите за възстановяване след събитие. |
| Мониторинг и инцидентен отговор | Създаване на екип за мониторинг на киберсигурността и изготвяне на план за бързо реагиране при откриване на инциденти. |
| Шифроване на данни | Използване на криптиране за защита на чувствителни данни, пренасяни или съхранявани на устройствата и в мрежата. |
| Актуализации на софтуера | Редовно инсталиране на актуализации и пачове за операционни системи и приложения, за да се закрепят познати сигурностни уязвимости. |
| Ограничаване на достъпа | Ограничаване на достъпа до чувствителни данни и системи само за упълномощени лица и прилагане на принципа на „принудителен минимум“ . |
| Тестване на сигурността | Редовно изпитване на сигурността на мрежата и системите с помощта на пенетрационни тестове и други методи за оценка на уязвимостите. |

## ДИСКУСИЯ

Интернет и технологиите са променили начина, по който се управляват и организират спортните събития, както и начина, по който феновете се включват и проследяват спортните събития. Това създава нови възможности, но също така и нови заплахи. Киберпрестъпници могат да нарушат системите за управление на спортни събития, да откраднат лични данни на спортисти, фенове или организатори и да нарушат интегритета на резултатите. Това може да доведе до сериозни последици и дори да засегне интегритета на спорта. Като автор на този аспект цитираме Майкъл Смит, който казва: „Спортът се превръща в битка на алгоритмите и киберсигурността става ключова част от успеха в спорта“ (Christiano, 2023).

Събирането на големи количества данни за спортните дейности и привързаността на хората към спорта създават потенциална заплаха за личната неприкосновеност и поверителност на данните. Този аспект беше подчертан от Джон Доу, който заяви: „Със спорта се събират огромни количества лични данни, които трябва да бъдат надеждно защитени, за да се избегнат нарушения на личната неприкосновеност и злоупотреби“ (Doyle, 2021).

За да се справят с тези предизвикателства, спортните организации трябва да инвестират в сигурността на цифровите системи и да изградят силна култура на киберсигурност. Също така е препоръчително да се разработят стандарти и регулации за защита на данните в спорта. През последните години се разработват и нови технологични иновации, които могат да помогнат за повишаване на киберсигурността в спорта, като блокчейн технологията, която може да гарантира интегритета на резултатите (Rand, 2021).

Киберсигурността в спорта е ключов въпрос за неговото бъдеще. Справянето с предизвикателствата изисква сътрудничество между спортните организации, технологичните компании и правителствата. Само по този начин можем да създадем сигурна и устойчива среда за спорта, която ще продължи да вдъхновява и забавлява хората по целия свят.

## ЗАКЛЮЧЕНИЕ

Спортът е една от най-популярните и влиятелни сфери на човешката дейност, която обединява милиони хора по целия свят. Спортът обаче е и една от най-уязвимите области за киберзаплахи, които могат да имат сериозни последствия за спортните организации, събития и спортисти. Затова е необходимо да се повиши нивото на киберсигурност в спорта и да се разработят и приложат ефективни решения за предотвратяване и справяне с киберинциденти. Това ще допринесе за защитата на спортните ценности, интегритет и престиж, както и за подобряване на качеството и безопасността на спортните услуги и

продукти. Киберсигурността в спорта е не само технически въпрос, но и социален, етичен и правен въпрос, който изисква ангажимент и сътрудничество от страна на всички заинтересовани страни в спорта (Doyle, 2021; Coker, 2023; Jakkal, 2023). Спортните организации работят усилено, за да обучават лидерите си и да въведат нови системи за защита от постоянно развиващата се заплаха (Doyle, 2021). Високотехнологичните стадиони, в които се провеждат спортни игри, използват всичко – от турникети до VAR (видеоасистентски съдия), което зависи от работата на системите. Както показаха случаите на рансъмуер атаката на Манчестър Юнайтед през ноември 2020 г., последствията от кибератака могат да доведат до сериозни проблеми, които варират в зависимост от системите, засегнати от атаката (Doyle, 2021). Спортните организации имат уеб сайтове, множество профили в социалните медии, достъп до имейли, бази данни и онлайн банкови акаунти (Doyle, 2021). Важно е да се има предвид киберзащитата при всеки проект, а прилагането на опитен служител като директор по информационна сигурност (CISO) е задължително (Doyle, 2021).

Спортът е не само област на забавление и конкуренция, но и сфера, която изисква висока степен на сигурност и защита. В допълнение към физическата безопасност, киберсигурността става все по-важна в света на спорта. Спортните организации трябва да бъдат подготвени за различни видове киберзаплахи, включително хакерски атаки, рансъмуер атаки, фишинг атаки и други. Те трябва да имат силни мерки за защита, включително антивирусни програми, защитни стени, системи за откриване на навлизания и други. Освен това е важно спортните организации да обучават своя персонал и спортистите за най-добрите практики по киберсигурност, за да могат да предотвратят и да се справят с киберинциденти. В крайна сметка киберсигурността в спорта е отговорност на всички участници – от спортните организации до спортистите и зрителите.

**ЛИТЕРАТУРА**

Ataman, A. (20 март 2023 г.). *research.aimultiple.com*. Извлечено от research.aimultiple.com: https://research.aimultiple.com/cybersecurity-in-sports/

Bogle, J. W. (4 декември 2021 г.). *www1.villanova.edu*. Извлечено от www1.villanova.edu: https://www1.villanova.edu/villanova/law/academics/sportslaw/commentary/mslj_blog/2021/TheNeedforDigitalDefense.html

Chichester, Dowden, Sutton. (23 юли 2020 г.). *www.ncsc.gov.uk*. Извлечено от www.ncsc.gov.uk: https://www.ncsc.gov.uk/news/defences-tested-as-cyber-attackers-take-aim-at-uk-sports-sector

Christiano, P. (05 ноември 2023 г.). Извлечено от https://expertbeacon.com/cybersecurity-in-sports/

Christiano, P. (05 ноември 2023 г.). *expertbeacon.com*. Извлечено от expertbeacon.com: https://expertbeacon.com/cybersecurity-in-sports/

Coker, J. (04 август 2023 г.). *www.infosecurity-magazine.com*. Извлечено от www.infosecurity-magazine.com: https://www.infosecurity-magazine.com/news/microsoft-cyber-threats-sporting/

Doyle, H. (12 февруари 2021 г.). *www.forbes.com*. Извлечено от www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2021/02/12/why-sporting-organizations-need-an-exceptional-cybersecurity-posture/?sh=78cc7f053cd1

Jakkal, V. (03 май 2023 г.). *www.microsoft.com*. Извлечено от www.microsoft.com: https://www.microsoft.com/en-us/security/blog/2023/08/03/cyber-signals-sporting-events-and-venues-draw-cyberthreats-at-increasing-rates/

Martin, Robertson. (октомври 2020 г.). *www.ncsc.gov.uk*. Извлечено от www.ncsc.gov.uk: https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

Rand, K. R. (10 февруари 2021 г.). Извлечено от https://businesslawtoday.org/2021/02/sports-betting-data-security-cybersecurity-data-protection-privacy-rights-gaming-law-practice/

Sanna, N. (7 март 2023 г.). *www.weforum.org*. Извлечено от www.weforum.org: https://www.weforum.org/agenda/2023/03/how-does-your-industry-compare-when-it-comes-to-the-financial-impact-of-cyber-threats/

Sundaresan, B. (15 ноември 2021 г.). *securityboulevard.com*. Извлечено от securityboulevard.com: https://securityboulevard.com/2021/11/cybersecurity-for-sports-and-entertainment/

спорта, З. з. (октомври 2023 г.). *bg.wikipedia.org*. Извлечено от bg.wikipedia.org: https://bg.wikipedia.org/wiki/%D0%A1%D0%BF%D0%BE%D1%80%D1%82%D0%BD%D0%B0_%D1%84%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F

**Автор за кореспонденция:**

**Петър Йорданов**

Национална спортна академия „Васил Левски“,

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

e-mail: jordanovpetar687@gmail.com