НАЦИОНАЛНА СПОРТНА АКАДЕМИЯ „ВАСИЛ ЛЕВСКИ“
ФАКУЛТЕТ „СПОРТ“

КАТЕДРА „ТЕЖКА АТЛЕТИКА, БОКС, ФЕХТОВКА И СПОРТ ЗА ВСИЧКИ“

АВТОРЕФЕРАТ

на дисертационен труд на тема:

„ПОВИШАВАНЕ НА КИБЕРЗАЩИТАТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ, ПОДДЪРЖАЩИ МАСОВИ СПОРТНИ МЕРОПРИЯТИЯ“

за придобиване на образователната и научна степен **„Доктор“**

Научен ръководител: проф. д-р Красимир Петков

Автор: Петър Йорданов

Официални рецензенти:

Проф. Валентин Стефанов Панайотов, ДН

Проф. Любомир Кирилов Тимчев, ДН

София, 2024

Дисертационният труд е обсъден и насочен за публична защита от разширен научен колегиум на катедра „Катедра Тежка атлетика, бокс, фехтовка и спорт за всички“ при НСА „Васил Левски“ на 30. 10. 2024 г.

Трудът е с обем от 177 стандартни страници, в т.ч. използвана литература, която включва 188 източника. Онагледен е с 4 таблици и 33 фигури.

Публичната защита ще се състои на 14. 01. 2025 г. от 15.30 часа в зала А3 на НСА „Васил Левски“.

УВОД

Спортните събития в днешния дигитализиран свят привличат огромна аудитория и носят значителни приходи, което ги прави чести цели на кибератаки. С нарастващата роля на информационните технологии в управлението на такива мероприятия, киберсигурността е от критично значение за успешното им провеждане. Настоящото изследване ще разгледа ключови аспекти като уязвимости на информационните системи, методи за кибератаки, мерки за защита и препоръки за повишаване на сигурността.

Структура на дисертацията:

Литературен обзор – Обобщение на основните понятия и съществуващите изследвания по темата за киберсигурността в спорта.

Цели, задачи и методика – Определяне на целите, обхвата и методите на изследването, включително анализ на добри практики, SWOT анализ и анкетни проучвания.

Анализ на резултатите – Представяне на данни от литературното проучване и анализ на добри практики и уязвимости.

Изводи и препоръки – Обобщаване на основните заключения и предлагане на конкретни препоръки за подобряване на киберсигурността.

Значение на темата:

С нарастващото използване на информационни системи в спорта, киберсигурността е от съществено значение за успеха на събитията и безопасността на участниците и зрителите. Тези мероприятия са привлекателни цели за кибератаки, изискващи иновативни стратегии за защита.

Основни предизвикателства:

Масовите спортни мероприятия, поради своята значимост и видимост, се нуждаят от високо ниво на защита. България може да постигне завидна киберзащита чрез съвместни усилия между държавата, академичната общност и бизнеса, за да осигури безопасността на системите и нормалното функциониране на събитията.

I.ГЛАВА ПЪРВА ЛИТЕРАТУРЕН ОБЗОР

1.1. Спортни събития и киберсигурност: Теоретични и терминологични аспекти

Спортните събития разчитат на информационни системи, което ги прави уязвими към кибератаки. Киберсигурността е от съществено значение за защита на данни и поддържане на безопасността и доверието. Важно е спортните организации да инвестират в защита и да работят с експерти за минимизиране на рисковете. (Как да защитим киберсигурността на спортните организации., 2024)

I.1.1. Понятието „киберзащита“ в контекста на спортните събития

Киберсигурността е ключова за защита на спортните събития от атаки, които могат да увредят данни и репутация. Нужни са сигурни мрежи, мониторинг и обучение, като мерките трябва да са интегрирани в общата стратегия за сигурност на събитието.

I.1.2. Същност на информационните системи поддържащи спортни мероприятия

Информационните системи подпомагат управлението на спортни събития чрез регистрация, билети, комуникация и поддръжка на данни. Те осигуряват точност и достъпност на информацията и трябва да са надеждни, защитени и адаптивни, с устойчивост на киберзаплахи и добра поддръжка. (Калайков, 2005)

I.1.3. Фактори, определящи кибербезопасността на информационните системи в спорта

Кибербезопасността в спорта изисква защита на данните, автентикация, мрежова сигурност, редовни актуализации, обучение на персонала и бекъп. Мониторингът и одитите гарантират адаптация към нови заплахи и поддържат надеждността на системите.

I.1.4. Съотношение между понятията „информационна сигурност“ и „сигурност на информацията“

„Сигурност на информацията“ защитава данни за поверителност, цялост и достъпност, докато „информационната сигурност“ обхваща защита на всички технологии и системи, поддържащи данните.

I.1.5 Съвременни рискове в информационната сигурност на спорта

Спортни събития като Олимпиадата, UEFA и Супербоул са цел на кибератаки като DDoS, фишинг и зловреден софтуер, които застрашават данни и нарушават събитията. Спортните организации трябва да инвестират в сигурност, обучение и нови технологии за ефективна защита и. (E-security.bg. (, 2024).

I.2. Дигитална сигурност в Република България

България приоритизира дигиталната сигурност чрез национални и международни партньорства, адаптиране към европейските стандарти и дейности на организации като БАК и CERT. Целта е да се осигури защита и устойчивост срещу киберзаплахи и да се затвърди позицията на страната в дигиталната сигурност.

I.2.1. Основни структури в областта на кибербезопасността в България

Кибербезопасността в България се регулира от Закона за кибербезопасност, GDPR и Закона за защита на личните данни. Държавната комисия по информационна сигурност и Съветът за кибербезопасност надзират киберсигурността, а Министерството на електронното управление развива проекти за дигитализация. България работи активно с НАТО и ENISA, като защитава критичната инфраструктура и подготвя специалисти по кибербезопасност. (Държавна агенция "Електронно управление", 2024)

I.2.2. Готовност и предотвратяване на киберзаплаха

България предприема мерки за киберсигурност, включително създаване на Национален център и инициативи за обучение. Необходими са по-добра координация и осведоменост за киберзаплахите. Основните мерки включват образование, политики, сътрудничество между институции, сигурностни технологии, редовни обновления, резервни копия и защита на мобилни устройства. Постоянното адаптиране е ключово за ефективна киберсигурност.

I.3. Стратегии за ИТ сигурност

ИТ стратегиите за сигурност включват оценка на риска, политики, обучение, технически мерки и реагиране на инциденти. Те осигуряват защита на данни и готовност срещу киберзаплахи, като трябва да бъдат адаптивни и актуализирани. (Интегрирането на киберсигурността в корпоративните политики е стратегически императив., 2024)

I.3.1. Национална стратегия за киберсигурност

България участва в инициативи на ЕС за киберсигурност и прилага Национална стратегия за киберсигурност, целяща защитата на инфраструктурата, бизнеса и гражданите. Основните ѝ елементи включват оценка на рискове, политики за киберсигурност, обучение, технически мерки, международно сътрудничество и реактивни планове при инциденти. Тази стратегия укрепва способността на страната за откриване, предотвратяване и реагиране на кибератаки.

I.3.3. Агенцията на Европейския съюз за киберсигурност (ENISA)

Агенцията на Европейския съюз за киберсигурност (ENISA) е орган на ЕС, който подпомага държавите-членки и Европейската комисия чрез предоставяне на експертни съвети, стандарти и добри практики за защита. Тя осигурява обучение, обмен на

информация и техническа помощ, като работи с частния сектор и академичните среди за повишаване на устойчивостта на ЕС към кибератаки. ENISA играе ключова роля в създаването на единен подход към киберсигурността в Европа и защитата на дигиталната среда. (Агенция на Европейския съюз за киберсигурност (ENISA). , 2024)

I.4. Нарастващото значение на киберсигурността в спорта

Киберсигурността е от решаващо значение в съвременния спортен свят, тъй като спортът все повече разчита на цифрови технологии в тренировки, анализи и състезания. Системите и данните на спортните организации са подложени на рискове от хакерски атаки, които могат да компрометират събития и лични данни на спортисти. Спортните организации трябва да инвестират в мерки за защита, като редовни оценки на риска, обучение на персонала и професионална киберзащита. Това е особено важно и за електронния спорт, където киберсигурността гарантира справедлива игра и защита на репутацията.

I.4.1. Кибер терористични актове, осъществени по време на спортни събития

Кибертерористичните актове представляват сериозна заплаха за спортните събития, тъй като могат да нарушат информационната сигурност и функционирането на цифровата инфраструктура, необходима за провеждането на тези събития. Атаките могат да бъдат извършени чрез хакерски атаки, саботаж на компютърни системи, разпространение на зловреден софтуер и социален инженеринг. Целите могат да включват системите за управление на събития, медийните платформи и комуникационните канали, което може да доведе до сериозни последствия за безопасността на участниците, зрителите и организаторите. (TechNews.bg., 2023)

По време на Олимпиадата в Париж през 2024 г. бяха регистрирани над 140 кибератаки, насочени към ключови информационни системи, използвани за управлението на събитието. Тези атаки включваха DDoS атаки, които временно прекъснаха достъпа до официалните уебсайтове на игрите и затрудниха достъпа до важна информация за зрителите и участниците. Освен това, зловреден софтуер беше използван за саботиране на системите за управление на резултати, което доведе до забавяне в публикуването на резултатите от състезанията и създаде сериозни проблеми за организаторите. Тези инциденти показаха колко уязвими могат да бъдат спортните събития към киберзаплахи и подчертаха необходимостта от засилена киберсигурност. (Петкова, 2024)

Според експерти, терористични организации могат да използват кибератаки за техните цели, включително атаки от типа отказ на услуга (DDoS), които могат да прекъснат важни услуги по време на спортни събития. (Какво е кибератака?)

Засилването на сигурността около големи спортни събития, като например Олимпийските игри, е от съществено значение, тъй като те често стават цел на киберкампании и други заплахи. (Киберсигурност на ЕС: Комисията предлага създаването на съвместно киберзвено за засилване на способността за реагиране в случай на мащабни инциденти по сигурността., 2021).

Тези атаки имат потенциала да доведат до сериозни последици, включително нарушаване на игралните правила, изтичане на лични данни на участниците и зрителите, прекъсване на медийното излъчване и засегнатост на инфраструктурата на събитията. Те могат да създадат хаос и несигурност, както и да дестабилизират обществото и националната сигурност.

Примери за кибератаки по време на спортни мероприятия:

Олимпийските игри в Пьонгчанг (2018): Кибератака с използване на зловреден софтуер Olympic Destroyer, който целеше да прекъсне началната церемония и да саботира информационните системи на събитието. (Савов, 2024)

Световно първенство по футбол в Русия (2018): Хакери нападнаха системите на FIFA и публикуваха лични данни на футболисти.

Токио 2020 (проведени през 2021): Значителни рискове от кибератаки, включително възможни опити за саботаж на системи за управление на събития, медийни платформи и комуникационни канали. (Повишена опасност от кибератаки на спортните събития. , 2023)

Тези примери показват, че спортните мероприятия са подложени на сериозни киберзаплахи и изискват постоянен надзор и внимание в областта на киберсигурността.

За да се предотвратят кибертерористичните актове по време на спортни събития, е от съществено значение да се изгради здрава и сигурна стратегия за киберсигурност. Тази стратегия трябва да включва сътрудничество между правителствените институции, спортните организации, частния сектор и международни партньори.

Надлежно обучени и компетентни експерти по киберсигурност трябва да бъдат задействани за наблюдение на информационната сигурност и бързо реагиране на евентуални кибернападения. Технологичните системи, използвани по време на събитията, следва да бъдат обект на редовни одити и обновления, за да се гарантира тяхната защита срещу нови и развиващи се киберзаплахи.

Допълнително, разработването на планове за кризисно управление в случай на кибертерористичен инцидент е от съществено значение. Тези планове трябва да включват детайлни стъпки за реакция, координация с компетентните органи и организации, както

и механизми за бързо възстановяване на засегнатата инфраструктура и информационни системи.

Общественото осведомяване за киберсигурността и съзнателността за рисковете на кибертерористичните заплахи също са от изключително значение. Зрителите, участниците и организаторите на спортни събития следва да бъдат информирани за методите и техниките, използвани от кибертерористите, както и за необходимостта от предприемане на предпазни мерки за защита на техните лични данни и информационна сигурност.

I.4.2 Сигурност на спортните уебсайтове и приложения

Сигурността на спортните уебсайтове и приложения е от съществено значение за защита на потребителските данни и предотвратяване на кибератаки. Спортните организации трябва да използват шифроване, двуфакторна автентикация и редовни тестове за сигурност, за да осигурят защита срещу хакерски атаки, фишинг и зловреден софтуер.

Инвестициите в киберсигурност и обучения са критични за намаляване на риска, особено при големи събития като Олимпийските игри. Съвременни технологии като изкуствен интелект подпомагат откриването на заплахи в реално време. Сътрудничеството между организатори, доставчици и правителствени институции също е ключово за успешна и сигурна среда на спортните събития.

II. ГЛАВА ВТОРА ЦЕЛ, ЗАДАЧИ, ОБЛАСТ, МЕТОДИКА И ОРГАНИЗАЦИЯ НА ИЗСЛЕДВАНЕТО

II.1. Цел на изследването

Целта на изследването е да установи уязвимостите в информационните системи на спортни мероприятия и да анализира съвременните кибератаки. Препоръчаните мерки включват криптиране, контрол на достъпа, мониторинг и обучение на персонала за превенция и реакция при инциденти.

II.2. Задачи на изследването:

За изпълнение на така формулираната цел поставяме следните задачи:

1. Да извършим преглед и анализ на исторически примери, свързани с кибертерористични актове, засягащи масови спортни мероприятия от различен ранг, и да проведем обстойно проучване на съществуващите методи и технологии за киберзащита, използвани в спортните мероприятия и други подобни области.
2. Да изготвим детайлен анализ на рисковете и уязвимостите, свързани с информационните системи, които поддържат спортни мероприятия.
3. Да установим основните източници на заплаха в национален и международен план, както и да прогнозираме тяхната мотивация, насоченост, методи и способи на действие.
4. Да анализираме киберсигурността на информационните системи, поддържащи масови спортни събития.
5. Да разкрием мястото и ролята на отделните институции и структури на спортната общественост, които имат функции и задачи за противодействие на кибертероризма по време на спортни мероприятия.
6. Да анализираме техническите и организационните мерки за предотвратяване и управление на кибератаки.
7. Да представим резултатите от изследванията в писмена форма, като опишем добрите практики и предложим насоки за подобряване на киберзащитата на информационните системи, поддържащи спортни мероприятия.
8. Да разработим план за обучение на персонала на спортните мероприятия по киберсигурност и инструкции за бърза реакция в случай на инциденти.
9. Да прегледаме резултатите от дисертационната работа и да предложим подобрения за киберзащитата на информационните системи на спортните мероприятия чрез прилагане на стандартни методи за сигурност, като мултифакторна автентикация,

ограничаване на правата на потребителите, криптиране на данни и други защитни мерки.

II.3. Обект и предмет на изследването

Обект на изследването е киберсигурността на информационните системи, поддържащи спортни мероприятия, включваща хардуер, софтуер, мрежова инфраструктура, интернет протоколи, процедури и човешкия фактор.

Предмет на изследването е оптимизирането на киберзащитата на информационни системи, поддържащи спортни мероприятия, с акцент върху идентифициране на рискове и разработване на ефективни мерки за защита.

II.4. Област на изследването

Киберсигурността се състои от три основни области – физическа, техническа и човешка. Целта на настоящия научен труд е да изследва и характеризира тези три елемента, за да се установят най-добрите практики за киберсигурност при провеждане на спортни мероприятия. Областта на изследването е киберзащитата на информационните системи, които поддържат спортни мероприятия. Това включва технологиите, използвани за осигуряване на комуникация и обработка на информация, като уебсайтове, онлайн платформи за залагания, медийни платформи за предаване на живо и други.

Изследването се фокусира върху идентифицирането на възможните киберзаплахи и атаки върху тези информационни системи, както и върху разработването на мерки за подобряване на тяхната киберзащита, с цел да се предложат подобрения и решения за повишаване на сигурността и надеждността на тези системи.

II.5. Методика на изследването

За да бъдем максимално точни в резултатите, представени в настоящата разработка, използвахме разнообразни методи за събиране на данни, които могат да се синтезират в следните групи: проучване на литературни източници; анализ на добри практики за киберсигурност; SWOT анализ; сканиране и анализиране за уязвимости на спортни сайтове; анкетно проучване; структурен контент-анализ; математико-статистически методи.

Литературното проучване обхваща научни източници, книги и доклади в областта на киберсигурността на спортните събития. Анализирани са добри практики като управление на достъпа, криптиране и редовно обновяване на софтуера. Чрез S.W.O.T. анализ са идентифицирани силни и слаби страни, възможности и заплахи за киберзащитата в спорта. Проведено е сканиране на спортни сайтове за уязвимости, оценка на рисковете и съответствие с регулациите. Анкетното проучване и експертната

оценка събират мнения за рисковете и защитните мерки. Математико-статистическите методи като регресионен и клъстерен анализ подпомагат оценката на риска и разработването на ефективни стратегии за киберзащита в спортния сектор.

II.6 Организация на изследването

1. **Формиране на екип**
2. **Период**: 01/01/2022 – 31/01/2022

Дейности: Сформиране на екип от професионалисти в областта на киберсигурността, спорта и информационните технологии. Определяне на ясни цели и задачи за ориентация на проучването.

1. **Литературен обзор**

Период: 01/02/2022 – 01/04/2023

Дейности: Събиране и анализ на съществуващата литература и основни понятия, свързани с киберсигурността в спорта. Извършен бе преглед на същността на киберзащитата, рисковете за информационните системи и приложимите стратегии.

2. **Цели, задачи, област, методика и организация на изследването**

Период: 01/04/2022 – 30/04/2023

Дейности: Формулиране на основните цели и задачи на изследването, избор на методология, включваща SWOT анализ, сканиране за уязвимости, анкетни проучвания и експертни оценки. Планиране на детайлен хронологичен план на дейностите.

3. **Разработка на анкетна карта и анкетно проучване**

Период: 01/06/2022 – 31/12/2023

Дейности: Изготвяне на анкетна карта и провеждане на анкетно проучване, систематизация и анализ на събраната информация.

4. **Анализ на резултатите**

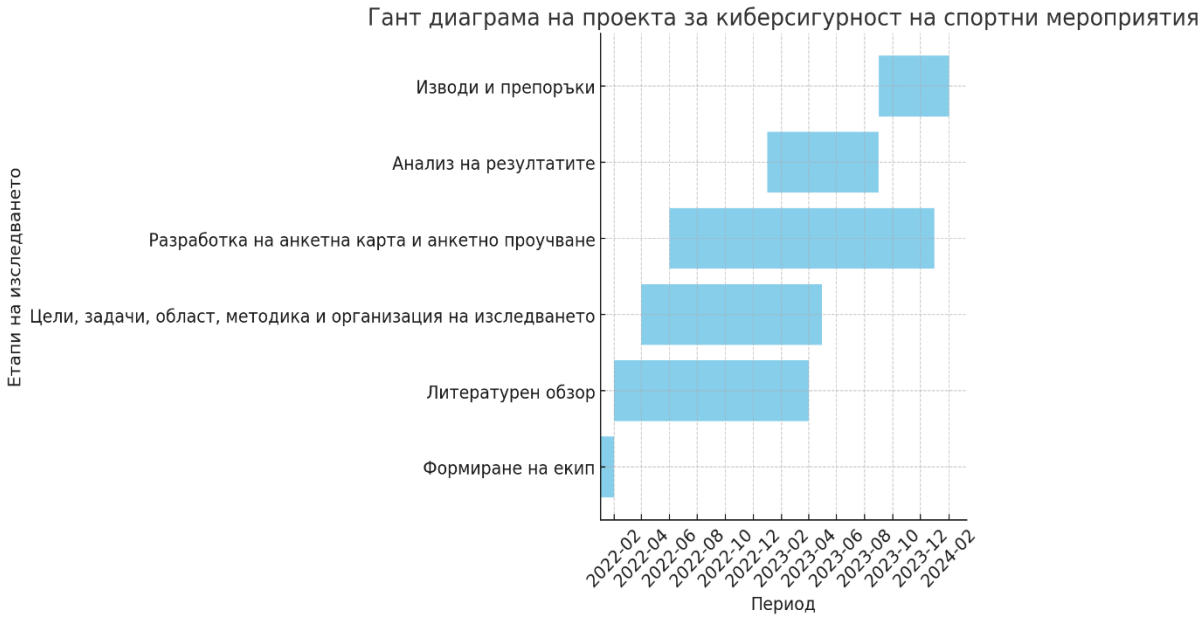
Период: 01/01/2023 – 31/08/2023

Дейности: Анализ на събраните данни от литературното проучване, добрите практики в киберсигурността, резултатите от SWOT анализа и сканирането за уязвимости, както и от анкетните проучвания.

5. **Изводи и препоръки**

Период: 01/09/2023 – 01/02/2024

Дейности: Обобщение на основните изводи от изследването и предоставяне на препоръки за подобряване на киберсигурността в спортните мероприятия, както и насоки за бъдещи изследвания. Изследването обхваща екип, литературен обзор, цели, методика, анкети, анализ и изводи за подобряване на киберсигурността в спорта.



Фигура 6. *Гант диаграма на проекта за киберсигурност на спортни мероприятия*

Фигурата визуализира продължителността и времевите периоди на различните етапи от проекта. Това улеснява разбирането за последователността и взаимната зависимост между етапите.

III. ГЛАВА ТРЕТА - АНАЛИЗ НА РЕЗУЛТАТИТЕ

III.1. Обобщение на целите и задачите на изследването

В изследването са приложени методи като сканиране на уязвимости, анкети и експертни оценки, за да се идентифицират рисковете за киберсигурността на спортни събития и да се предложат ефективни решения. Целта е да се анализира текущото състояние на киберсигурността на системи, поддържащи спортни мероприятия, и да се предложат мерки за подобряване на сигурността. Основните задачи включват литературен преглед, анализ на добри практики, S.W.O.T. анализ, сканиране на уязвимости, анкетно проучване, контент анализ и експертна оценка. Резултатите подчертават важността на редовните актуализации, многопластовата защита, криптирането и мониторинга на системите за сигурността на спортните мероприятия. Тези мерки са ключови за защита на личните данни на потребителите и предотвратяване на кибератаки.

III.2. Анализ на резултатите от проучването на литературните източници

Литературният преглед разкри ключови тенденции и предизвикателства в киберсигурността на спортните събития, като нарастващ брой кибератаки, значението на мултифакторна аутентикация, криптиране и нуждата от редовни одити. Проучването потвърди нарастващия интерес към сигурността на информационните системи, обслужващи спортни мероприятия, идентифицирайки заплахи като хакерски атаки и зловреден софтуер. Препоръките включват използването на криптографски технологии, редовни актуализации, изолирани мрежи и обучение на персонала. Използването на математико-статистически методи като регресионен и клъстерен анализ е доказано като полезен подход за оценка на риска и уязвимости. Обзорът предоставя ценна основа за подобрения в киберзащитата и бъдещи изследвания в тази област.

III.2.1.Обобщение на най-важните изводи и препоръки

Литературният преглед подчерта необходимостта от многостепенна защита, международни стандарти и редовно обучение за киберсигурност в спортните мероприятия. Препоръчва се внедряване на многостепенна защитна система, процедури при инциденти и повишаване на осведомеността на персонала. Анализът на риска акцентира върху защита на паролите и актуализация на софтуера. Тези мерки ще помогнат на организаторите на спортни събития да подобрят сигурността си срещу кибератаки.

III.3.Анализ на добри практики за киберсигурност

Проучихме добрите практики за киберсигурност, прилагани в спортни организации по света, за да идентифицираме ефективни стратегии за адаптиране към българските спортни мероприятия. Анализът показа, че е препоръчително да се използват стандарти като ISO/IEC 27001 и NIST Cybersecurity Framework, както и редовно обновяване на софтуера, силни пароли и сканиране за зарази. Важно е също обучението на персонала и изграждане на култура на киберсигурност. Основните акценти включват изграждане на сигурна мрежова инфраструктура, защита на лични данни и противодействие на кибератаки.

III.4. Анализ на резултатите от S.W.O.T анализ

S.W.O.T. анализът предостави подробен преглед на силните и слабите страни, възможностите и заплахите, свързани с киберсигурността в спорта. Силните страни включват обучени ИТ специалисти и модерни технологии, докато слабите са липсата на координация и ресурси. Възможностите включват международно сътрудничество и нови технологии, а заплахите – увеличаващите се кибератаки и нови видове зловреден софтуер. Въз основа на анализа бяха предложени препоръки за подобряване на киберзащитата, като създаване на киберзащитна политика, въвеждане на двуфакторна автентикация, обучения и инвестиции в съвременни технологии.

III.5. Анализ на резултатите от сканиране и анализиране на уязвимости на спортни сайтове

Анализът на уязвимостите на спортни сайтове разкри основни рискове като SQL инжекции, XSS атаки, липса на криптиране и слаби пароли. Тези проблеми подчертават нуждата от редовни актуализации и защита на данните, за да се предотвратят кибератаки. Сканирането с инструменти като Nmap и Nikto идентифицира отворени портове, липса на HTTP заглавки и други уязвимости, които представляват потенциални рискове. Резултатите показват необходимостта от въвеждане на по-силни пароли, SSL сертификати, редовно обновяване на софтуера и ограничаване на достъпа до критични директории. Тези мерки ще повишат сигурността на спортните платформи срещу зловредни атаки.

III.6. Анкетно проучване

Анкетното проучване установи, че основните предизвикателства пред киберсигурността в спортните системи са липсата на ресурси и недостатъчно обучение на персонала, като също се подчертава нуждата от по-добра координация и обмен на информация. Целта на анкетата беше да събере мнения и препоръки от потребители на спортните информационни системи, за да се подобри тяхната киберзащита. Изследването,

проведено сред студенти от Военна академия „Г. С. Раковски“ и Национална спортна академия „Васил Левски“, включваше 16 въпроса, обхващащи знания, умения и възприятия за рисковете. Резултатите бяха анализирани и използвани за формулиране на препоръки за повишаване на киберзащитата в спортните информационни системи.

III.7. Структурен-контент анализ

Анализът на документи разкри, че много спортни организации нямат ясни политики за киберсигурност и често пренебрегват най-добрите практики. Структурно-контент анализът идентифицира ключови теми като представяне на проблема, цели, методи и заключения на изследването, подчертавайки важността му за научната общност. Основните теми включват проблемите с киберсигурността, целите на изследването, използваните методи и заключенията. Този анализ е полезен инструмент за извличане на информация и структуриране на съдържанието в научни изследвания.

III.8. Експертна оценка

Анализът на експертната оценка потвърди, че предложените мерки за киберзащита са адекватни и приложими, като експертите препоръчаха допълнителни AI-базирани решения за откриване на аномалии. Консултациите разкриха ключови рискове и уязвимости, което позволи изготвянето на детайлна оценка на състоянието на киберзащитата на системите за спортни мероприятия. Комбинацията от експертна оценка с други методи като структурно-контент анализ и анкетно проучване осигури цялостен преглед на рисковете и слабостите, които трябва да бъдат адресирани. Експертната оценка подчертава значимостта на адекватната киберзащита, особено за спортни системи, податливи на кибератаки.

III.8.2.Обобщение на мненията на експертите относно предложените решения

Експертите единодушно подкрепиха необходимостта от повишена киберзащита за информационните системи, свързани със спортни мероприятия, като се съгласиха, че те са изложени на значителен риск от кибератаки. Сред препоръките, които подкрепиха, бяха внедряването на двуфакторна автентикация и редовни проверки на уязвимостите. Един експерт предложи мултифакторна автентикация с биометрични данни, която бе призната като ефективен метод за повишаване на сигурността.

III.8.3. Анализ на резултатите и формулиране на заключения за допълнителни действия

Експертната оценка показа уязвимости в системите за спортни събития, които могат да бъдат експлоатирани. Основните препоръки включват подобряване на осведомеността и обучението на персонала, внедряване на многофакторна автентикация и шифроване на

данни. Спортната организация трябва да продължи с редовни проверки и прилагане на предложените мерки. Фиг. 30 показва разпределението на предложените мерки.

III.9 Математико-статистически методи

Статистическият анализ на данните от анкетите и сканирането на уязвимости разкри ключови зависимости и помогна за класифициране на рисковете. Изследването показа, че по-високото ниво на обучение на персонала води до намаляване на уязвимостите, докато слабите пароли значително увеличават риска от атаки. Клъстерният анализ позволи сегментиране на системите на три нива на риск, което улеснява приоритизирането на защитните мерки.

Основни изводи:

1. Повишеното обучение намалява уязвимостите.
2. Слабите пароли увеличават риска, препоръчва се многофакторна автентикация.
3. Клъстерният анализ е полезен за сегментиране по риск.

Препоръки:

- Обучение на персонала за киберсигурност.
- Политики за силни пароли и редовна смяна.
- Внедряване на многофакторна автентикация.
- Редовни одити за уязвимости.

Тези мерки значително ще подобрят устойчивостта на системите срещу киберзаплахи и ще улеснят безопасното провеждане на масови спортни мероприятия.

IV ГЛАВА ЧЕТВЪРТА ИЗВОДИ И ПРЕПОРЪКИ

IV.1. Изводи

1. Нарастваща роля на киберсигурността в спорта: Развитието на технологиите значително увеличава нуждата от ефективна киберзащита в спортните мероприятия, поради новопоявили се рискове за сигурността на данните и инфраструктурата.
2. Чести типове киберзаплахи: В изследването е установено, че киберзаплахите към спортните събития са разнообразни и често водят до компрометиране на данни, нарушаване на системни функции или редки физически щети. Това подчертава необходимостта от специализирани мерки, насочени към тези специфични заплахи.
3. Необходимост от подходящи мерки за сигурност: Във връзка с поставените цели се откроява значимостта на подходи като криптиране, управление на достъпа и редовни обновления на системите, за да се намали риска от кибератаки.
4. Липсващи стандарти за киберсигурност в спортните организации: Литературното проучване и анализът на добрите практики показват липсата на унифицирани стандарти за киберзащита в спорта, което води до необходимост от разработване на специализирани политики и насоки за спортните организации.
5. Наличие на уязвимости в спортните системи: Сканирането на уязвимостите показва конкретни слабости, като междусайтов скриптинг и SQL инжекции, което изисква адекватни мерки за защита на информационните ресурси на спортните организации.
6. Липса на информираност сред персонала: Анкетното проучване подчертава нуждата от обучения и повишаване на осведомеността сред персонала и участниците в спортни събития относно основни киберзаплахи, което е съществено за укрепване на сигурността.
7. Роля на обучението: Изводът от проучването сочи, че редовното обучение и информиране на персонала за новите киберзаплахи и добрите практики е от ключово значение за поддържането на киберустойчивост на спортните системи.

IV.2. Препоръки

След приключването на настоящото изследване предлагаме следните ключови препоръки за подобряване на киберзащитата на информационните системи, обслужващи спортни мероприятия:

1. **Изграждане на силни пароли:** Използването на силни пароли е сред най-ефективните начини за защита на лични данни и информационни системи. Препоръчваме въвеждането на политика за създаване на сложни пароли, която да включва комбинации от символи, цифри и букви, както и редовна проверка на силата на паролите на потребителите. Също

така е необходимо внедряване на инструменти за управление на паролите, които да улеснят потребителите в създаването и поддържането на сигурни пароли.

2. **Внедряване на система за мониторинг:** Инсталирането на система за мониторинг на мрежовия трафик и анализ на логовете на сървърите е ключово за ранно откриване на неоторизирани опити за достъп до информационните системи. Подобни системи за мониторинг следят за аномалии в поведението на мрежата и сървърите, което позволява своевременно предприемане на мерки за защита. Използването на инструменти за анализ на логове и алармиране при съмнителна активност е от критично значение за намаляване на времето за реакция при инциденти.
3. **Изграждане на мрежова защита:** Защитата на мрежовите системи е от съществено значение за предотвратяване на хакерски атаки и проникване на зловреден софтуер. Препоръчваме използването на решения като защитни стени (Firewall) и системи за предотвратяване на прониквания (Intrusion Prevention Systems – IPS), които да блокират нежелания достъп до системата и да предотвратяват разпространението на зловредни програми. Внедряването на мрежова сегментация осигурява допълнителен слой защита, като ограничава разпространението на атаки в различни части на мрежовата инфраструктура.
4. **Обучение на персонала:** Обучението на персонала е ключов елемент в процеса на подобряване на киберзащитата. Всеки служител трябва да бъде информиран за своите отговорности по отношение на киберсигурността и да бъде обучен как да разпознава потенциални заплахи, като фишинг атаки, социално инженерство и съмнителни линкове. Редовните обучения и семинари са препоръчителни, за да се актуализират знанията на персонала относно новите заплахи и добрите практики за защита.
5. **Редовно обновяване на софтуера:** Актуализациите на софтуера са от критично значение за затваряне на уязвимости, които биха могли да бъдат използвани от злонамерени лица. Редовното обновяване на всички системни компоненти, включително операционните системи, приложенията и защитните решения, намалява риска от атаки, свързани с известни уязвимости. Внедряването на автоматизирани инструменти за управление на актуализациите ще осигури навременното инсталиране на критични поправки и защити.
6. **Разработване на план за действие при инцидент:** Разработването и прилагането на план за действие при киберинциденти е от съществено значение за бърза и ефективна реакция в случай на атака. Планът трябва да включва ясен процес за идентифициране на инцидентите, процедура за комуникация с всички засегнати страни и възстановяване на

системите след инцидента. Важно е този план да бъде редовно актуализиран и тестван чрез симулации, за да се гарантира неговата максимална ефективност при реални атаки.

В заключение, за да се подобри киберзащитата на информационните системи, които поддържат спортни мероприятия, е необходимо да се прилагат няколко ключови мерки, които гарантират сигурността на данните и защитата на системите от потенциални заплахи. Сред тези мерки са:

- **Защита на паролите и поверителността на данните:** Препоръчва се използването на сложни пароли, криптиране на данните и двуфакторна автентикация, за да се осигури максимална защита на чувствителната информация.
- **Редовно обновяване на софтуера и системните компоненти:** Актуализациите на софтуера са жизненоважни за отстраняване на уязвимостите и подобряване на защитата на системите.
- **Изграждане на стратегии за откриване и противодействие на кибератаките:** Използването на съвременни технологии, като машинно самообучение и изкуствен интелект за анализ на големи масиви от данни, може да подобри откриването на кибератаки и да ускори реакцията при инциденти.
- **Провеждане на редовни тестове на сигурността:** Проверките и тестовете за уязвимости (като penetration tests) осигуряват увереност, че системите са защитени и готови да посрещнат потенциални заплахи.

С прилагането на тези препоръки значително ще се подобри киберзащитата на информационните системи, които поддържат спортни мероприятия. Това ще осигури по-висока степен на сигурност за съхраняваните данни и ще защити личните данни на потребителите от неоторизиран достъп.

IV.3. Приноси на научната работа

Научната работа представлява важен принос за областта на киберзащитата на информационните системи, които поддържат спортни мероприятия. Работата предоставя необходимата теоретична база и анализира най-съвременните тенденции и методи в областта на киберзащитата.

Резултатите от изследването на уязвимостите в информационните системи, които се използват за поддръжка на спортни мероприятия, позволяват да се идентифицират конкретни рискове и да се предложат мерки за подобряване на киберзащитата на тези системи.

Препоръките за подобряване на киберзащитата на информационните системи, които поддържат спортни мероприятия, включват редица мерки, които могат да бъдат

внедрени в практиката, като например използване на силни пароли, редовна актуализация на софтуера, редовни тестове за уязвимости и други. Тези мерки могат да помогнат за по-ефективна защита на информационните системи и за намаляване на риска от кибератаки.

Резултатите и препоръките от тази научна работа могат да бъдат полезни за специалисти в областта на киберзащитата, за разработчици на информационни системи, които се използват за поддръжка на спортни мероприятия, както и за ръководствата на спортни организации, които имат нужда от повишаване на нивото на киберзащитата в своите системи.

Научната работа за подобряване на киберзащитата на информационните системи, които поддържат спортни мероприятия, има голям принос за киберсигурността в тази област. Първо, работата представя подробен анализ на уязвимостите на информационните системи, свързани с организирането на спортни мероприятия, както и на рисковете, свързани с тяхното експлоатиране от злонамерени атаки. Второ, работата представя редица препоръки за подобряване на киберзащитата на информационните системи, включително съвети за подобряване на паролите, защита на устройствата и мрежите, защита на данните и обучение на персонала. Тези препоръки могат да бъдат от полза за различни видове спортни мероприятия, включително големи спортни събития като олимпийски игри или световни първенства, както и за по-малки и локални събития. Трето, научната работа предлага използването на математико-статистически методи за анализ на данни и оценка на риска. Това може да помогне за по-ефективното откриване и предотвратяване на кибератаки.

Заключението на научната работа представя важни приноси в областта на киберзащитата на информационните системи, използвани за поддръжка на спортни мероприятия. Работата предоставя подробна теоретична база и анализира най-съвременните тенденции и методи в областта на киберзащитата. Резултатите от изследването на уязвимостите в информационните системи, свързани със спортните мероприятия, позволяват идентифициране на конкретни рискове и предлагат мерки за подобряване на киберзащитата на тези системи. Препоръките за подобряване на киберзащитата включват използване на силни пароли, редовна актуализация на софтуера, редовни тестове за уязвимости и други мерки, които могат да подобрят ефективността на защитата на информационните системи и да намалят риска от кибератаки. Резултатите и препоръките от тази научна работа могат да бъдат полезни за специалисти в областта на киберзащитата, разработчици на информационни системи, използвани за поддръжка на спортни мероприятия, както и за ръководствата на спортни организации, които се

нуждаят от повишаване на нивото на киберзащитата в своите системи. Научната работа представя и математико-статистически методи за анализ на данни и оценка на риска, които могат да помогнат за по-ефективното откриване и предотвратяване на кибератаки. В заключение, научната работа има голям принос за подобряването на киберзащитата на информационните системи, които поддържат спортни мероприятия, и може да бъде от полза за различни видове спортни събития, както и за спортни организации в тяхната усилена борба с киберзловещи заплахи.

Научната работа разглежда възможността за интеграция на изкуствен интелект и машинно обучение в процеса на анализ на уязвимости, като това може значително да ускори откриването на потенциални заплахи. Въведените препоръки са базирани на анализ на реални случаи на кибератаки върху спортни мероприятия, което прави предложените мерки изключително практически приложими. Освен това, научната работа включва и оценка на финансовите и организационни последствия от кибератаките върху спортни организации. Тези аспекти подчертават необходимостта от стратегическо планиране и инвестиции в киберсигурността на спортните събития.

Научната работа подчертава важността на сътрудничеството между спортни организации, ИТ специалисти и органи за сигурност за цялостна киберзащита, като математико-статистическите методи подпомагат идентифицирането на тенденции и прогнозирането на заплахи, водещи до намаляване на риска от кибератаки и повишаване на сигурността в спортните мероприятия.

СПИСЪК
на публикациите по темата на дисертационния труд

1. Петър Йорданов, „Изследване на рисковете за киберсигурността във въоръжените сили на България“, Годишна студентска научна сесия „Факултет „Командно-щабен” Военна академия „Г. С. Раковски“, Съвременни аспекти на сигурността – предизвикателства, подходи, решения, 27 септември 2022 г., Военна академия „Георги Стойков Раковски“, издател, 2022 г., София стр. 357-366, ISSN: 2738-7526
1. Петър Йорданов*, Нина Кленовска, Ивайло Михайлов „Киберсигурността в спорта предизвикателства и решения“. – 2023. ГОДИШНИК БРОЙ 2 / 2023.
2. Сашо Йорданов, Петър Йорданов, Ивайло Здравков – „MODERN PRACTICE AND ETHODS FOR INTEGRATION THROUGH GOLF“, DOI: 10.37393/ICASS2022/12.

Библиография

Киберсигурност на ЕС: Комисията предлага създаването на съвместно киберзвено за засилване на способността за реагиране в случай на мащабни инциденти по сигурността. (Юни 23 2021 г.). Извлечено от Европейска комисия.: Взето от https://ec.europa.eu/commission/presscorner/a

Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. (н.д.). Изтеглено на 10 6 2024 г. от mdpi.com: https://www.mdpi.com/1424-8220/23/15/6666

E-security.bg. (,). О. (1 август 2024 г.). *"Олимпийските игри: Как да защитим киберсигурността на спортните организации"*. Извлечено от e-security.bg: https://e-security.bg/articles/olimpijskite-igri-kak-da-zasthitim-kibersigurnostta-na-sportnite-organizaczii/

TechNews.bg. (7 август 2023 г.). Извлечено от Повишена опасност от кибератаки на спортните събития. : Взето от https://technews.bg/article-153594.html

Агенция на Европейския съюз за киберсигурност (ENISA). . (2024). Извлечено от Европейски съюз.: Взето от https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_bg

АНАЛИТИЧЕН ДОКЛАД по резултатите от проведеното проучване на нивото на дигитализация в спорта. (2023). *„Дигитална демокрация в действие“, финансирана от Оперативна програма „Добро управление“ 2014-2020 г.*, (стр. bcci.bg). Изтеглено на 10 6 2024 г. от https://www.bcci.bg/bulgarian/projects/Doklad_Digitalizacia_v_sporta.pdf

Важността на дигитализацията в спортния и общинския спортен сектор. (17 10 2023 г.). Изтеглено на 10 6 2024 г. от Календар: https://sportenkalendar.bg/blog/vaznostta-na-digitalizaciata-v-sportnia-i-obsinskia-sporten-sektor-186

Държавна агенция "Електронно управление". (2024). Извлечено от Мрежова и информационна сигурност. : Взето от https://e-gov.bg/wps/portal/agency/home/NIS

Интегрирането на киберсигурността в корпоративните политики е стратегически императив. (1 юни 2024 г.). Извлечено от e-security.bg.: Взето от https://e-security.bg/articles/integriraneto-na-kibersigurnostta-v-korporativnite-politiki-e-strategicheski-imperativ/

Как да защитим киберсигурността на спортните организации. (1 август 2024 г.). Извлечено от e-security.bg: Взето от https://e-

security.bg/articles/olimpijskite-igri-kak-da-zasthitim-kibersigurnostta-na-sportnite-organizaczii/

Какво е кибератака? (н.д.). *Microsoft*, стр. https://www.microsoft.com/bg-bg/security/business/security-101/what-is-a-cyberattack.

Калайков, Й. (2005). *Теория и технология на управлението в спорта*. София: Национална спортна академия "Васил Левски". .

Олимпийските игри: Експерти тестват киберзащитата на ключови системи и съоръжения. (5 4 2024 г.). Изтеглено на 10 6 2024 г. от euronewsbulgaria.com.

Петкова, Ц. (13 август 2024 г.). Франция съобщи за над 140 кибератаки, свързани с Олимпийските игри. стр. Взето от https://nova.bg/news/view/2024/08/13/466630/.

Повишена опасност от кибератаки на спортните събития. . (7 август 2023 г.). Извлечено от TechNews.bg.: Взето от https://technews.bg/article-153594.html

Савов, И. (30 юли 2024 г.). Новото „нормално“ блести на олимпийските игри в Париж - „безпрецедентно“ ниво на киберзаплахи и кибератаки. . стр. Взето от https://faktor.bg/bg/articles/mneniya-lacheni-tsarvuli-novoto-normalno-blesti-na-olimpiyskite-igri-v-parizh-bezp.

NATIONAL SPORTS ACADEMY "VASIL LEVSKI"
FACULTY OF SPORTS

DEPARTMENT OF WEIGHTLIFTING, BOXING, FENCING AND SPORTS FOR ALL

ABSTRACT

of a dissertation on the topic:

"INCREASING THE CYBER PROTECTION OF INFORMATION SYSTEMS SUPPORTING MASS SPORTS EVENTS"

for the acquisition of the educational and scientific degree **"Doctor"**

Supervisor: Prof. Dr. Krasimir Petkov

Author: Petar Yordanov

Official reviewers:

Prof. Valentin Stefanov Panayotov, DN

Prof. Lyubomir Kirilov Timchev, DN

Sofia, 2024

The dissertation was discussed and sent for public defense by an extended scientific collegium of the Department of Weightlifting, Boxing, Fencing and Sports for All at the National Sports Academy "Vasil Levski" on 30. 10. 2024

The work has a volume of 177 standard pages, including used literature, which includes 188 sources. It is illustrated with 4 tables and 33 figures.

The public defense will take place on 14. 01. 2025 at 15.30 in Hall A3 of NSA "Vasil Levski".

INTRODUCTION

Sporting events in today's digitized world attract a huge audience and bring in significant revenue, making them frequent targets of cyberattacks. With the growing role of information technology in the management of such events, cybersecurity is critical to their successful implementation. This study will look at key aspects such as vulnerabilities of information systems, cyberattack methods, security measures and recommendations for enhancing security.

Dissertation structure:

Literature review – A summary of the basic concepts and existing research on the topic of cybersecurity in sport.

Objectives, objectives and methodology – Defining the objectives, scope and methods of the survey, including good practice analysis, SWOT analysis and survey studies.

Analysis of results – Presentation of data from the literature study and analysis of good practices and vulnerabilities.

Conclusions and recommendations – Summarizing the main conclusions and offering specific recommendations for improving cybersecurity.

Significance of the topic:

With the increasing use of information systems in sports, cybersecurity is essential for the success of events and the safety of participants and spectators. These events are attractive targets for cyberattacks, requiring innovative defense strategies.

Main challenges:

Mass sports events, due to their importance and visibility, need a high level of protection. Bulgaria can achieve enviable cyber protection through joint efforts between the state, academia and business to ensure the safety of systems and the normal functioning of events.

I.CHAPTER ONE LITERATURE REVIEW

1.1. Sporting events and cybersecurity: Theoretical and terminological aspects

Sporting events rely on information systems, making them vulnerable to cyberattacks. Cybersecurity is essential for protecting data and maintaining safety and trust. It is important for sports organizations to invest in protection and work with experts to minimize risks. (Как да защитим киберсигурността на спортните организации., 2024)

I.1.1. The concept of 'cyber defence' in the context of sporting events

Cybersecurity is key to protecting sporting events from attacks that can damage data and reputation. Secure networks, monitoring and training are needed, and the measures must be integrated into the overall event security strategy.

I.1.2. Essence of the information systems supporting sports events

Information systems support the management of sporting events through registration, ticketing, communication and data maintenance. They ensure accuracy and accessibility of information and must be reliable, secure and adaptable, with resilience to cyber threats and good support. (Калайков, 2005)

I.1.3. Factors determining the cybersecurity of information systems in sport

Cybersecurity in sports requires data protection, authentication, network security, regular updates, staff training, and backups. Monitoring and audits ensure adaptation to new threats and maintain the reliability of systems.

I.1.4. Correlation between the concepts of "information security" and "information security"

'Information security' protects data for confidentiality, integrity and availability, while 'information security' encompasses the protection of all technologies and systems supporting the data.

I.1.5 Contemporary Risks in Sport Information Security

Sporting events such as the Olympics, UEFA and the Super Bowl are targeted by cyberattacks such as DDoS, phishing and malware that threaten data and disrupt events. Sports organizations need to invest in security, training and new technologies for effective protection and ...(E-security.bg. (, 2024)

I.2. Digital Security in the Republic of Bulgaria

Bulgaria prioritizes digital security through national and international partnerships, adaptation to European standards and activities of organizations such as BAC and CERT. The goal is to ensure protection and resilience against cyber threats and to strengthen the country's position in digital security.

I.2.1. Main structures in the field of cybersecurity in Bulgaria

Cybersecurity in Bulgaria is regulated by the Cybersecurity Act, the GDPR and the Personal Data Protection Act. The State Commission on Information Security and the Cybersecurity Council supervise cybersecurity, and the Ministry of e-Government develops digitalization projects. Bulgaria is actively working with NATO and ENISA, protecting critical infrastructure and training cybersecurity specialists. (Държавна агенция "Електронно управление", 2024)

I.2.2. Cyber threat preparedness and prevention

Bulgaria is taking cybersecurity measures, including the establishment of a National Center and training initiatives. Better coordination and awareness of cyber threats are needed. Key measures include education, policies, institution-to-institutional collaboration, security technologies, regular updates, backups, and mobile device protection. Constant adaptation is key to effective cybersecurity.

I.3. IT security strategies

IT security strategies include risk assessment, policies, training, technical measures, and incident response. They provide data protection and preparedness against cyber threats, and must be adaptable and updated. (Интегрирането на киберсигурността в корпоративните политики е стратегически императив., 2024)

I.3.1. National Cybersecurity Strategy

Bulgaria participates in EU cybersecurity initiatives and implements a National Cybersecurity Strategy aimed at protecting infrastructure, businesses and citizens. Its main elements include risk assessment, cybersecurity policies, training, technical measures, international cooperation and incident response plans. This strategy strengthens the country's ability to detect, prevent, and respond to cyberattacks.

I.3.3. European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) is an EU body that assists Member States and the European Commission by providing expert advice, standards and good security practices. It provides training, information exchange and technical assistance, working with the private sector and academia to increase the EU's resilience to cyber-attacks. ENISA plays a key role in creating a unified approach to cybersecurity in Europe and protecting the digital environment. (Агенция на Европейския съюз за киберсигурност (ENISA). , 2024)

I.4. The growing importance of cybersecurity in sport

Cybersecurity is crucial in today's sports world, as sports increasingly rely on digital technologies in training, analytics, and competitions. The systems and data of sports organizations are subject to the risks of hacker attacks, which can compromise events and personal data of athletes. Sports organisations need to invest in protection measures, such as

regular risk assessments, staff training and professional cyber protection. This is especially important for esports, where cybersecurity ensures fair play and reputation protection.

I.4.1. Cyber terrorist acts committed during sporting events

Cyber-terrorist acts pose a serious threat to sporting events, as they can disrupt information security and the functioning of the digital infrastructure necessary for the conduct of these events. Attacks can be carried out through hacker attacks, sabotage of computer systems, malware distribution, and social engineering. Objectives may include event management systems, media platforms and communication channels, which can lead to serious consequences for the safety of participants, spectators and organisers. (TechNews.bg., 2023)

During the Paris 2024 Olympics, more than 140 cyberattacks were recorded, targeting key information systems used to manage the event. These attacks included DDoS attacks that temporarily cut off access to the games' official websites and made it difficult for viewers and participants to access important information. In addition, malware was used to sabotage the results management systems, which led to a delay in the publication of the results of the competitions and created serious problems for the organizers. These incidents showed how vulnerable sporting events can be to cyber threats and highlighted the need for enhanced cybersecurity. (Петкова, 2024)

According to experts, terrorist organizations can use cyberattacks for their own purposes, including denial-of-service (DDoS) attacks that can disrupt important services during sporting events. (Какво е кибератака?)

Strengthening security around major sporting events, such as the Olympic Games, is essential, as they often become the target of cyber campaigns and other threats.. (Киберсигурност на ЕС: Комисията предлага създаването на съвместно киберзвено за засилване на способността за реагиране в случай на мащабни инциденти по сигурността., 2021)

These attacks have the potential to lead to serious consequences, including violation of gaming rules, leakage of personal data of participants and spectators, interruption of media broadcasting, and damage to the infrastructure of events. They can create chaos and insecurity, as well as destabilize society and national security.

Examples of cyberattacks during sporting events:

Olympic Games in Pyeongchang (2018): A cyberattack using the Olympic Destroyer malware, which aimed to interrupt the kick-off ceremony and sabotage the event's information systems. (Савов, 2024)

FIFA World Cup in Russia (2018): Hackers attacked FIFA systems and published personal data of football players.

Tokyo 2020 (held in 2021): Significant risks of cyber-attacks, including possible attempts to sabotage event management systems, media platforms and communication channels. (Повишена опасност от кибератаки на спортните събития. , 2023)

These examples show that sporting events are subject to serious cyber threats and require ongoing cybersecurity oversight and attention.

To prevent cyber terrorist acts during sporting events, it is essential to build a robust and secure cybersecurity strategy. This strategy must include cooperation between government institutions, sports organisations, the private sector and international partners.

Duly trained and competent cybersecurity experts must be deployed to monitor information security and respond quickly to possible cyber attacks. The technological systems used during the events should be subject to regular audits and updates to ensure their protection against new and evolving cyber threats.

Additionally, developing crisis management plans in the event of a cyber-terrorist incident is essential. These plans should include detailed response steps, coordination with the competent authorities and organisations, as well as mechanisms for the rapid recovery of the affected infrastructure and information systems.

Public awareness of cybersecurity and awareness of the risks of cyber-terrorist threats are also of utmost importance. Spectators, participants and organisers of sporting events should be informed about the methods and techniques used by cyberterrorists, as well as the need to take precautions to protect their personal data and information security.

I.4.2 Security of sports websites and applications

The security of sports websites and apps is essential for protecting user data and preventing cyberattacks. Sports organizations should use encryption, two-factor authentication, and regular security tests to provide protection against hacker attacks, phishing, and malware.

Investments in cybersecurity and training are critical to reducing risk, especially at major events such as the Olympic Games. Modern technologies such as artificial intelligence help detect threats in real time. Cooperation between organisers, suppliers and government institutions is also key to a successful and secure environment for sporting events.

II. CHAPTER TWO PURPOSE, TASKS, FIELD, METHODOLOGY AND ORGANIZATION OF THE STUDY

II.1. Purpose of the study

The aim of the study is to identify vulnerabilities in the information systems of sports events and to analyze modern cyberattacks. Recommended measures include encryption, access control, monitoring, and training of staff to prevent and respond to incidents.

II.2. Objectives of the study:

To fulfill the goal formulated in this way, we set the following tasks:

10. To review and analyze historical examples related to cyber-terrorist acts affecting mass sports events of various ranks, and to conduct a thorough study of the existing methods and technologies for cyber protection used in sports events and other similar areas.
11. To prepare a detailed analysis of the risks and vulnerabilities associated with the information systems that support sports events.
12. To identify the main sources of threat nationally and internationally, as well as to predict their motivation, direction, methods and methods of action.
13. To analyze the cybersecurity of the information systems supporting mass sporting events.
14. To reveal the place and role of the individual institutions and structures of the sports community that have functions and tasks to counter cyberterrorism during sports events.
15. Analyze technical and organizational measures to prevent and manage cyberattacks.
16. To present the results of the research in writing, describing good practices and offering guidelines for improving the cyber protection of information systems supporting sports events.

17. To develop a plan for training the staff of sports events on cybersecurity and instructions for rapid response in case of incidents.
18. To review the results of the dissertation and propose improvements for the cyber protection of the information systems of sports events by applying standard security methods, such as multi-factor authentication, restriction of user rights, data encryption and other security measures.

II.3. Object and subject of the study

The object of the study is the cybersecurity of information systems supporting sports events, including hardware, software, network infrastructure, Internet protocols, procedures and the human factor.

Subject of the study is the optimization of cyber protection of information systems supporting sports events, with an emphasis on identifying risks and developing effective protection measures.

II.4. Field of study

Cybersecurity consists of three main areas – physical, technical, and human. The purpose of this scientific work is to investigate and characterize these three elements in order to establish the best practices for cybersecurity in the conduct of sports events. The field of study is the cyber protection of information systems that support sports events. This includes the technologies used to ensure communication and information processing, such as websites, online betting platforms, live streaming media platforms, and more.

The study focuses on identifying possible cyber threats and attacks on these information systems, as well as developing measures to improve their cyber defense, in order to propose improvements and solutions to increase the security and reliability of these systems.

II.5. Methodology of the study

In order to be as accurate as possible in the results presented in this paper, we used a variety of methods for data collection, which can be synthesized in the following groups: study of literature sources; analysis of good cybersecurity practices; SWOT analysis; scanning and analyzing for vulnerabilities on sports sites; questionnaire; structural content analysis; mathematical and statistical methods.

The literature study covers scientific sources, books and reports in the field of cybersecurity of sports events. Good practices such as access management, encryption and regular software updates are analyzed. Through S.W.O.T. analysis, strengths, weaknesses, opportunities and threats to cyber protection in sports have been identified. Sports sites were scanned for vulnerabilities, risk assessment and compliance with regulations. The survey and

expert assessment collect opinions on the risks and protective measures. Mathematical and statistical methods such as regression and cluster analysis support risk assessment and the development of effective cyber defense strategies in the sports sector.

II.6 Organisation of the study

3. **Team Formation**
4. **Period**: 01/01/2022 – 31/01/2022

Activities: Forming a team of professionals in the field of cybersecurity, sports and information technology. Defining clear goals and objectives for the orientation of the study.

6. **Literature review**

Period: 01/02/2022 – 01/04/2023

Activities: Collection and analysis of existing literature and basic concepts related to cybersecurity in sport. An overview of the nature of cyber defense, risks to information systems and applicable strategies was carried out.

7. **Goals, objectives, field, methodology and organization of the study**

Period: 01/04/2022 – 30/04/2023

Activities: Formulation of the main goals and objectives of the study, selection of a methodology including SWOT analysis, vulnerability scanning, survey studies and expert assessments. Planning of a detailed chronological plan of activities.

8. **Development of a questionnaire and survey**

Period: 01/06/2022 – 31/12/2023

Activities: Preparation of a questionnaire and conducting a questionnaire survey, systematization and analysis of the collected information.

9. **Analysis of the results**

Period: 01/01/2023 – 31/08/2023

Activities: Analysis of the collected data from the literature study, good practices in cybersecurity, the results of SWOT analysis and vulnerability scanning, as well as from survey studies.

10. **Conclusions and recommendations**

Period: 01/09/2023 – 01/02/2024

Activities: Summary of the main conclusions of the study and providing recommendations for improving cybersecurity in sports events, as well as guidelines for future research. The study covers a team, literature review, objectives, methodology, surveys, analysis and conclusions for improving cybersecurity in sport.

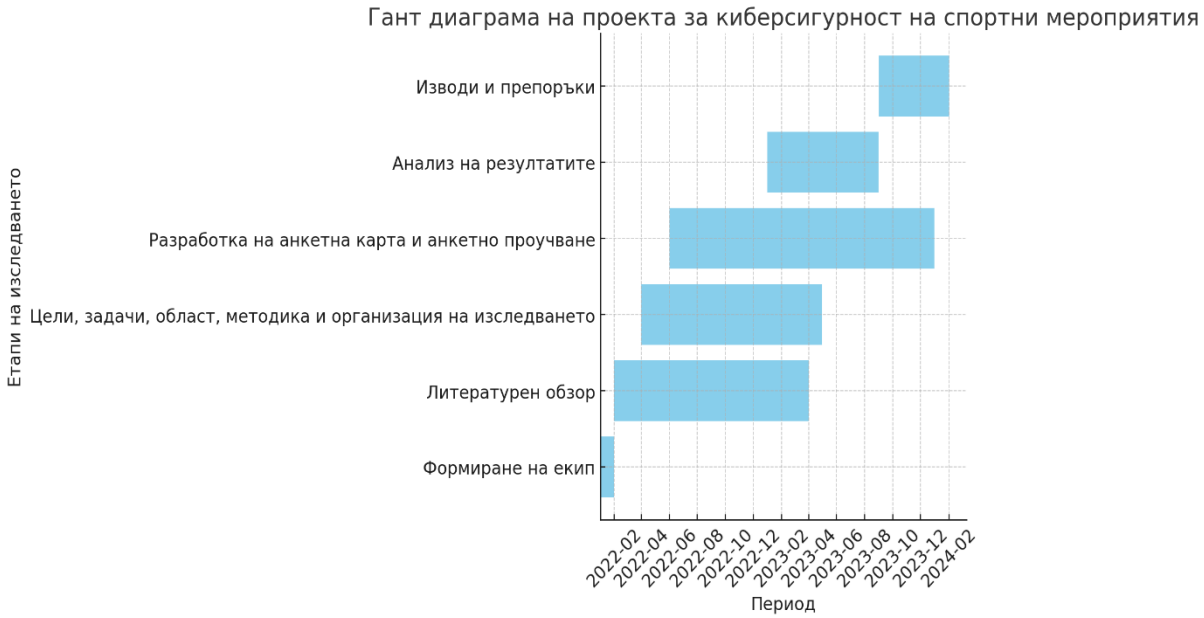


Figure 6. *Gantt Chart of the Sports Event Cybersecurity Project*

The figure visualizes the duration and time periods of the different stages of the project. This makes it easier to understand the sequence and interdependence between the stages.

III. CHAPTER THREE - ANALYSIS OF RESULTS

III.1. Summary of the goals and objectives of the study

The study applied methods such as vulnerability scanning, surveys and expert assessments to identify cybersecurity risks at sporting events and offer effective solutions. The aim is to analyze the current state of cybersecurity of systems supporting sports events and to propose measures to improve security. Key tasks include literature review, good practice analysis, S.W.O.T. analysis, vulnerability scanning, survey research, content analysis, and peer review. The results highlight the importance of regular updates, multi-layered protection, encryption and monitoring of the security systems of sports events. These measures are key to protecting users' personal data and preventing cyberattacks.

III.2. Analysis of the results of the study of literature sources

The literature review revealed key trends and challenges in the cybersecurity of sporting events, such as the increasing number of cyberattacks, the importance of multi-factor authentication, encryption, and the need for regular audits. The survey confirmed the growing interest in the security of information systems serving sports events, identifying threats such as hacker attacks and malware. Recommendations include the use of cryptographic technologies, regular updates, isolated networks, and staff training. The use of mathematical and statistical methods such as regression and cluster analysis has been proven to be a useful approach for assessing risk and vulnerabilities. The Monitor provides a valuable basis for improvements in cyber defence and future research in this area.

III.2.1.Summary of the most important findings and recommendations

The literature review highlighted the need for multi-level protection, international standards and regular cybersecurity training in sporting events. It is recommended to implement a multi-level protection system, incident procedures and staff awareness-raising. Risk analysis focuses on password protection and software updates. These measures will help organisers of sporting events improve their security against cyberattacks.

III.3.Analysis of good cybersecurity practices

We studied the best cybersecurity practices applied in sports organizations around the world to identify effective strategies for adapting to Bulgarian sports events. The analysis showed that it is advisable to use standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, as well as regular software updates, strong passwords and infection scanning. It is also important to train staff and build a culture of cybersecurity. The main highlights include building a secure network infrastructure, protecting personal data and countering cyberattacks.

III.4. Analysis of the results of the S.W.O.T analysis

The S.W.O.T. analysis provided a detailed overview of the strengths, weaknesses, opportunities and threats related to cybersecurity in sports. The strengths include trained IT professionals and modern technology, while the weaknesses are the lack of coordination and resources. Opportunities include international cooperation and new technologies, and threats include increasing cyberattacks and new types of malware. Based on the analysis, recommendations for improving cyber protection were proposed, such as creating a cyber defense policy, introducing two-factor authentication, training and investing in modern technologies.

III.5. Analysis of the results of scanning and analysis of vulnerabilities of sports sites

Analysis of sports site vulnerabilities revealed major risks such as SQL injections, XSS attacks, lack of encryption, and weak passwords. These issues highlight the need for regular updates and data protection to prevent cyberattacks. Scanning with tools like Nmap and Nikto identifies open ports, lack of HTTP headers, and other vulnerabilities that pose potential risks. The results indicate the need to introduce stronger passwords, SSL certificates, regularly update software and restrict access to critical directories. These measures will increase the security of sports platforms against malicious attacks.

III.6. Survey

The survey found that the main challenges to cybersecurity in sports systems are the lack of resources and insufficient training of staff, also highlighting the need for better coordination and exchange of information. The purpose of the survey was to collect opinions and recommendations from users of sports information systems in order to improve their cyber protection. The study, conducted among students from the G. S. Rakovski Military Academy and the Vasil Levski National Sports Academy, included 16 questions covering knowledge, skills and perceptions of risks. The results were analyzed and used to formulate recommendations for increasing cyber protection in sports information systems.

III.7. Structural-content analysis

The analysis of documents revealed that many sports organizations do not have clear cybersecurity policies and often ignore best practices. Structural-content analysis identifies key topics such as the presentation of the problem, goals, methods and conclusions of the research, emphasizing its importance to the scientific community. Key topics include cybersecurity issues, research objectives, methods used, and conclusions. This analysis is a useful tool for extracting information and structuring content in scientific research.

III.8. Expert assessment

The analysis of the expert assessment confirmed that the proposed cyber protection measures are adequate and applicable, with experts recommending additional AI-based solutions for

anomaly detection. The consultations revealed key risks and vulnerabilities, which allowed for a detailed assessment of the state of cyber protection of the systems for sports events. The combination of expert assessment with other methods such as structural-content analysis and survey research provided a comprehensive overview of the risks and weaknesses that need to be addressed. The expert assessment highlights the importance of adequate cyber protection, especially for sports systems susceptible to cyberattacks.

III.8.2.Summary of experts' views on proposed solutions

The experts unanimously supported the need for increased cyber protection for information systems related to sporting events, agreeing that they are at significant risk of cyberattacks. Among the recommendations they supported were the implementation of two-factor authentication and regular vulnerability checks. One expert proposed multi-factor authentication with biometric data, which was recognized as an effective method of increasing security.

III.8.3. Analysis of results and conclusions for further action

The expert assessment showed vulnerabilities in the systems for sporting events that could be exploited. Key recommendations include improving staff awareness and training, implementing multi-factor authentication, and data encryption. The sports organization must continue with regular inspections and implementation of the proposed measures. Fig. 30 shows the distribution of the proposed measures.

III.9 Mathematical and statistical methods

Statistical analysis of survey data and vulnerability scans revealed key dependencies and helped classify risks. The study showed that a higher level of staff training leads to a reduction in vulnerabilities, while weak passwords significantly increase the risk of attacks. Cluster analysis allowed for the segmentation of systems into three risk levels, which facilitates the prioritization of protective measures.

Key takeaways:

4. Increased training reduces vulnerabilities.
5. Weak passwords increase the risk, multi-factor authentication is recommended.
6. Cluster analysis is useful for segmentation by risk.

Recommendations:

- Cybersecurity staff training.
- Strong password policies and regular changeovers.
- Implementation of multi-factor authentication.
- Regular vulnerability audits.

These measures will significantly improve the resilience of systems against cyber threats and facilitate the safe conduct of mass sporting events.

CHAPTER IV CONCLUSIONS AND RECOMMENDATIONS

IV.1. Conclusions

8. Growing role of cybersecurity in sports: The development of technology significantly increases the need for effective cyber protection in sports events, due to emerging risks to data and infrastructure security.
9. Common types of cyber threats: The study found that cyber threats to sporting events are diverse and often result in data compromise, disruption of system functions, or rare physical damage. This underlines the need for specialised measures to address these specific threats.
10. Need for appropriate security measures: In relation to the objectives set, the importance of approaches such as encryption, access management and regular system updates to reduce the risk of cyberattacks stands out.
11. Missing cybersecurity standards in sports organizations: The literature research and the analysis of good practices show the lack of unified standards for cyber protection in sports, which leads to the need to develop specialized policies and guidelines for sports organizations.
12. Presence of vulnerabilities in sports systems: Vulnerability scans show specific weaknesses, such as cross-site scripting and SQL injections, which requires adequate measures to protect the information resources of sports organizations.

13. Lack of awareness among staff: The survey highlights the need for training and awareness-raising among staff and participants in sporting events on major cyber threats, which is essential for strengthening security.
14. Role of training: The conclusion of the study shows that regular training and information of staff about new cyber threats and good practices is key to maintaining the cyber resilience of sports systems.

IV.2. Recommendations

Following the completion of this study, we propose the following key recommendations for improving the cyber protection of information systems serving sports events:

7. **Building strong passwords:** Using strong passwords is one of the most effective ways to protect personal data and information systems. We recommend the introduction of a policy for creating complex passwords, which includes combinations of symbols, numbers and letters, as well as regular checking of the strength of users' passwords. to make it easier for users to create and maintain secure passwords.
8. **Implementation of a monitoring system:** The installation of a network traffic monitoring system and analysis of server logs is key to the early detection of unauthorized attempts to access information systems. Such monitoring systems monitor for anomalies in the behavior of the network and servers, which allows timely security measures to be taken. reduction of incident response time.
9. **Building network protection:** Protecting network systems is essential to prevent hacker attacks and malware intrusion. We recommend using solutions such as firewalls and Intrusion Prevention Systems (IPS) to block unwanted access to the system and prevent the spread of malware. by limiting the spread of attacks to different parts of the network infrastructure.
10. **Staff training:** Staff training is a key element in the process of improving cyber defense. Each employee should be informed about their cybersecurity responsibilities and be trained on how to recognize potential threats, such as phishing attacks, social engineering, and suspicious links.
11. **Regular software updates:** Software updates are critical to close vulnerabilities that could be exploited by malicious actors. Regular updates to all system components, including operating systems, applications, and security solutions, reduce the risk of attacks related to known vulnerabilities. Protect.
12. **Developing an incident action plan:** Developing and implementing a cyber incident action plan is essential for a quick and effective response in the event of an attack. The plan should include a clear process for identifying incidents, a procedure for communicating with all

affected parties, and restoring systems after the incident. to ensure its maximum effectiveness in real attacks.

In conclusion, in order to improve the cyber protection of the information systems that support sports events, it is necessary to implement several key measures that ensure data security and the protection of systems from potential threats. Among these measures are:

- **Password Protection and Data Privacy:** The use of complex passwords, data encryption, and two-factor authentication is recommended to ensure maximum protection of sensitive information.
- **Regular software and system component updates:** Software updates are vital for fixing vulnerabilities and improving system security.
- **Building strategies to detect and counter cyberattacks:** Using modern technologies, such as machine learning and artificial intelligence to analyze big data, can improve cyberattack detection and speed up incident response.
- **Conduct regular security tests:** Background checks and vulnerability tests (such as penetration tests) provide assurance that systems are secure and ready to meet potential threats.

The implementation of these recommendations will significantly improve the cyber protection of information systems that support sports events. This will provide a higher degree of security for the stored data and protect users' personal data from unauthorized access.

IV.3. Contributions to scientific work

The scientific work represents an important contribution to the field of cyber protection of information systems that support sports events. The work provides the necessary theoretical basis and analyzes the most up-to-date trends and methods in the field of cyber defense.

The results of the study of vulnerabilities in the information systems used to support sports events allow to identify specific risks and propose measures to improve the cyber protection of these systems.

Recommendations for improving the cyber protection of information systems that support sports events include a number of measures that can be implemented in practice, such as the use of strong passwords, regular software updates, regular vulnerability tests, and more. These measures can help to protect information systems more effectively and reduce the risk of cyberattacks.

The results and recommendations of this scientific work can be useful for specialists in the field of cyber defense, for developers of information systems that are used to support sports events, as well as for the management of sports organizations that need to increase the level of cyber protection in their systems.

Scientific work to improve the cyber protection of information systems that support sports events has made a great contribution to cybersecurity in this area. First, the paper presents a detailed analysis of the vulnerabilities of information systems related to the organization of sports events, as well as the risks associated with their exploitation by malicious attacks. Second, the work presents a number of recommendations for improving the cybersecurity of information systems, including tips for improving passwords, protecting devices and networks, protecting data, and training staff. These recommendations can be beneficial for different types of sporting events, including major sporting events such as the Olympic Games or World Cups, as well as smaller and local events. Thirdly, the scientific work suggests the use of mathematical and statistical methods for data analysis and risk assessment. This can help to detect and prevent cyberattacks more effectively.

The conclusion of the scientific work presents important contributions in the field of cyber protection of information systems used to support sports events. The work provides a detailed theoretical basis and analyzes the most up-to-date trends and methods in the field of cyber defense. The results of the study of vulnerabilities in information systems related to sports events allow the identification of specific risks and propose measures to improve the cyber protection of these systems. Recommendations for improving cybersecurity include the use of strong passwords, regular software updates, regular vulnerability testing, and other measures that can improve the effectiveness of information systems security and reduce the risk of cyberattacks. The results and recommendations of this scientific work can be useful for specialists in the field of cyber defense, developers of information systems used to support sports events, as well as for the management of sports organizations that need to increase the level of cyber protection in their systems. The scientific work also presents mathematical and statistical methods for data analysis and risk assessment, which can help to more effectively detect and prevent cyberattacks. In conclusion, the scientific work has made a great contribution to improving the cyber protection of the information systems that support sports events, and can benefit various types of sports events, as well as sports organizations in their intensive fight against cyber malicious threats.

The scientific work considers the possibility of integrating artificial intelligence and machine learning into the vulnerability analysis process, which can significantly accelerate the detection of potential threats. The introduced recommendations are based on an analysis of real cases of cyberattacks on sports events, which makes the proposed measures extremely practically applicable. In addition, the scientific work also includes an assessment of the financial and organizational consequences of cyberattacks on sports organizations. These

aspects highlight the need for strategic planning and investment in the cybersecurity of sporting events.

The scientific work emphasizes the importance of cooperation between sports organizations, IT specialists and security authorities for comprehensive cyber protection, as mathematical and statistical methods help identify trends and predict threats leading to reducing the risk of cyberattacks and increasing security in sports events.

LIST
of publications on the topic of the dissertation

3. Petar Yordanov, "Study of Cybersecurity Risks in the Armed Forces of Bulgaria", Annual Student Scientific Session "Faculty of Command and Staff", Military Academy "G. S. Rakovski", Contemporary Aspects of Security – Challenges, Approaches, Solutions, September 27, 2022, Georgi Stoykov Rakovski Military Academy, publisher, 2022, Sofia, p. 357-366, ISSN: 2738-7526
2. Petar Yordanov*, Nina Klenovska, Ivaylo Mihaylov "Cybersecurity in Sport: Challenges and Solutions". – 2023. YEARBOOK ISSUE 2 / 2023.
4. Sasho Yordanov, Petar Yordanov, Ivaylo Zdravkov – "MODERN PRACTICE AND ETHODS FOR INTEGRATION THROUGH GOLF", DOI: 10.37393/ICASS2022/12.

Bibliography

EU cybersecurity: The Commission proposes to set up a joint cyber unit to strengthen the response capability in the event of large-scale security incidents. (June 23, 2021). Excerpted from European Commission.: Taken from https://ec.europa.eu/commission/presscorner/a

Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. (n.d.). Retrieved on 10 6 2024 from mdpi.com: https://www.mdpi.com/1424-8220/23/15/6666

E-security.bg. (,). O. (August 1, 2024). *"The Olympic Games: How to Protect the Cybersecurity of Sports Organizations".* Retrieved from e-security.bg: https://e-security.bg/articles/olimpijskite-igri-kak-da-zasthitim-kibersigurnostta-na-sportnite-organizaczii/

TechNews.bg. (7 August 2023). Retrieved from Increased danger of cyberattacks at sporting events. : Retrieved from https://technews.bg/article-153594.html

European Union Agency for Cybersecurity (ENISA). . (2024). Extracted from European Union.: Taken from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_bg

ANALYTICAL REPORT on the results of the study on the level of digitalization in sports. (2023). *"Digital Democracy in Action", funded by the Operational Programme "Good Governance" 2014-2020.*, (p. bcci.bg). Retrieved on 10 6 2024, from https://www.bcci.bg/bulgarian/projects/Doklad_Digitalizacia_v_sporta.pdf

The importance of digitalization in the sports and municipal sports sector. (17 10 2023 r.). Retrieved on 10 6 2024 from Calendar: https://sportenkalendar.bg/blog/vaznostta-na-digitalizaciata-v-sportnia-i-obsinskia-sporten-sektor-186

State e-Government Agency. (2024). Extracted from Network and Information Security. : Taken from https://e-gov.bg/wps/portal/agency/home/NIS

Integrating cybersecurity into corporate policies is a strategic imperative. (June 1, 2024). Retrieved from e-security.bg.: Taken from https://e-security.bg/articles/integriraneto-na-kibersigurnostta-v-korporativnite-politiki-e-strategicheski-imperativ/

How to protect the cybersecurity of sports organizations. (August 1, 2024). Retrieved from e-security.bg: Retrieved from https://e-security.bg/articles/olimpijskite-igri-kak-da-zasthitim-kibersigurnostta-na-sportnite-organizaczii/

What is a cyberattack? (n.d.). *Microsoft*, p. https://www.microsoft.com/bg-bg/security/business/security-101/what-is-a-cyberattack.

Kalaykov, J. (2005). *Theory and Technology of Management in Sport.* Sofia: National Sports Academy "Vasil Levski".

The Olympic Games: Experts test the cyber defenses of key systems and facilities. (5 4 2024 r.). Retrieved on 10 6 2024 from euronewsbulgaria.com.

Petkova, C. (13 August 2024). France has reported more than 140 cyberattacks related to the Olympic Games. P.. Taken from https://nova.bg/news/view/2024/08/13/466630/.

Increased danger of cyberattacks at sporting events. . (August 7, 2023). Excerpted from TechNews.bg.: Taken from https://technews.bg/article-153594.html

Savov, I. (July 30, 2024). The new "normal" shines at the Paris Olympics - an "unprecedented" level of cyber threats and cyberattacks. . P.. Taken from https://faktor.bg/bg/articles/mneniya-lacheni-tsarvuli-novoto-normalno-blesti-na-olimpiyskite-igri-v-parizh-bezp.