Кандидат: маг. Искрен Павлинов Янков

Придобиване на образователна и научна степен „Доктор“

Област на висше образование - 5. Технически науки,

Професионално направление - 5.3. Комуникационна и компютърна техника,

Специалност - „Комуникационни мрежи и системи“

Резюметата на рецензираните публикации, на български език и на един от чуждите езици, които традиционно се ползват в съответната научна област

Група Г.8. Научни публикации в нереферирани списания с научно рецензиране или в редактирани колективни томове

Г.8.1. Research of the Network Infrastructure for Maintenance of Big Databases – **Yankov I.** - International Scientific Session ICTACSE 2018 – Winter Virtual Conference, November 23-24, 2018, Istanbul, presentation with a report, certificate awarded.

Резюме:

Тази публикация изследва основните принципи на компресия на данни, включително разделението между методите с пълна загуба на информация (lossy) и без загуба на информация (lossless). Представени са техники като кодиране чрез дължина на поредица (Run-length Encoding) и кодиране по метода на Хъфман (Huffman Encoding) за lossless компресия, както и анализ на стандартите за компресия като MPEG за lossy компресия. Обсъждат се приложенията на компресията в съвременните комуникационни и мултимедийни технологии, като се акцентира върху значението на тези методи за ефективно използване на ресурси за съхранение и предаване на информация.

Abstract:

This publication explores the fundamental principles of data compression, emphasizing the distinction between lossless and lossy methods. Techniques such as Run-length Encoding and Huffman Encoding for lossless compression are presented, alongside an analysis of compression standards like MPEG for lossy compression. The applications of compression in modern communication and multimedia technologies are discussed, highlighting the importance of these methods for efficient resource utilization in data storage and transmission.

Г.8.2. Осигуряване на киберзащита и сигурност в компютърна система, свързана с глобалната мрежа,- **Янков.И**, Сборник доклади: XXX Международен симпозиум на САИ „Джон Атанасов“, 10-11 ноември 2022 г., гр. София, представяне на доклад: (с. 53-56). Симпозиума е включен в НАЦИД

Резюме:

Докладът разглежда съвременните аспекти на киберотбраната и киберсигурността с фокус върху осигуряване на защита в глобалната мрежа. Представени са иновативни подходи за анализ на заплахи и противодействие на кибератаки, както и разработването на интегриран модел за защита. Обсъдени са конкретни сценарии на атаки като DDoS и ransomware, като са предложени стратегии за превенция и възстановяване. Докладът подчертава необходимостта от координация между държавните институции и внедряването на хибридни решения, съчетаващи локални и облачни технологии, за устойчиво управление на информационната сигурност.

Abstract:

The report explores modern aspects of cyber defense and cybersecurity, focusing on ensuring protection in the global network. Innovative approaches for threat analysis and countering cyberattacks are presented, along with the development of an integrated protection model. Specific attack scenarios, such as DDoS and ransomware, are discussed, offering prevention and recovery strategies. The report highlights the necessity of coordination among state institutions and the implementation of hybrid solutions combining on-premises and cloud technologies for sustainable information security management.

Г.8.3. Осигуряване на сигурност на компютърните мрежи и механизми за тяхната защита, Янков.И, Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023”, 30 юни 2023, гр. Ловеч, представяне с доклад (с.115-119). Конференцията е включена в НАЦИД

Резюме:

Публикацията се фокусира върху съвременните предизвикателства в осигуряването на сигурността на компютърните мрежи, като разглежда ключовата роля на технологии като Cisco Meraki MX Security Center. Представя се детайлно етапите на реализация на кибератаки, като акцентира върху зловредни софтуери като рансъмуер, които представляват сериозна заплаха за критичната инфраструктура. Специално внимание се отделя на иновационните методи за защита, включително интегрирани механизми за наблюдение, анализ на трафика и блокиране на зловредни действия в реално време. Освен това се подчертава значението на облачните технологии за централизирано управление на сигурността и ефективно възстановяване на данни при инциденти. Публикацията завършва с практически насоки за внедряване на тези технологии в мрежовата архитектура на държавни институции и частни компании.

Abstract:

The publication focuses on modern challenges in ensuring computer network security, emphasizing the pivotal role of technologies such as Cisco Meraki MX Security Center. It provides a detailed examination of the stages of cyberattacks, highlighting malware like ransomware, which poses significant threats to critical infrastructure. Innovative defense methods are given special attention, including integrated mechanisms for monitoring, traffic analysis, and real-time blocking of malicious activities. Furthermore, the importance of cloud technologies for centralized security management and effective data recovery in case of incidents is emphasized. The publication concludes with practical guidelines for implementing these technologies in the network architecture of governmental institutions and private companies.

Г.8.4. Кибер война – унищожителни действия без оръжия. Съвременна методология на Кибер отбраната,- **Янков.И** Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023”, 30 юни 2023, гр. Ловеч, представяне с доклад (с.167-171). Конференцията е включена в НАЦИД

Резюме:
Публикацията предлага задълбочен анализ на кибервойната като нова форма на конфликт, при която дигиталните технологии играят решаваща роля както в атаката, така и в защитата. Разглеждат се основните характеристики на кибервойната, включително анонимността, глобалният мащаб и хибридният ѝ характер. Анализирани са различните видове кибератаки, като DDoS, кибершпионаж и разпространение на дезинформация, и тяхното въздействие върху критичната инфраструктура. Особено внимание се отделя на методите за защита, като се акцентира на ролята на технологиите и международното сътрудничество в създаването на ефективни стратегии за киберотбрана. Примери от международната практика и препоръки за прилагане на закони и стандарти в областта на информационната сигурност допълват анализа, подчертавайки необходимостта от комплексен подход към киберзащитата.

Abstract:
The publication offers an in-depth analysis of cyber warfare as a new form of conflict where digital technologies play a crucial role in both offense and defense. The main characteristics of cyber warfare are examined, including its anonymity, global scale, and hybrid nature. Various types of cyberattacks, such as DDoS, cyber espionage, and disinformation campaigns, and their impact on critical infrastructure are analyzed. Special emphasis is placed on defense methods, highlighting the role of technologies and international cooperation in creating effective cyber defense strategies. Examples from international practices and recommendations for implementing laws and standards in information security complement the analysis, underscoring the need for a comprehensive approach to cyber protection.

Г.8.5. СЪВРЕМЕНИ КИБЕРАТАКИ В СЕКТОРА НА ЗДРАВЕОПАЗВАНЕТО. ПРАКТИЧЕСКИ МЕТОДИ ЗА ПРЕВЕНЦИЯ И ЗАЩИТА, **Янков.И** ,Сборник доклади: VIII Национална научна конференция с международно участие ТК Ловеч „TechCo 2024”, 28 юни 2024, гр. Ловеч, представяне с доклад (с.148-152). Конференцията е включена в НАЦИД

Резюме:
Докладът анализира нарастващите киберзаплахи в сектора на здравеопазването, включително рансъмуер атаки, фишинг и измами с електронна поща. Тези атаки застрашават както сигурността на данните, така и оперативната непрекъснатост на здравните организации. Представят се практически методи за превенция, като редовно архивиране на данни, внедряване на многофакторна автентикация, обучение на персонала и използване на напреднали защитни технологии. В доклада се подчертава значението на мониторинга и бързата реакция при инциденти. Заключението препоръчва стратегически подход към киберсигурността, за да се осигури надеждността на информационните системи и безопасността на пациентите.

Abstract:
The report analyzes the increasing cyber threats in the healthcare sector, including ransomware attacks, phishing, and email fraud. These attacks endanger both data security and the operational continuity of healthcare organizations. Practical prevention methods are presented, such as regular data backups, implementation of multi-factor authentication, staff training, and the use of advanced security technologies. The report highlights the importance of monitoring and rapid incident response. The conclusion recommends a strategic approach to cybersecurity to ensure the reliability of information systems and the safety of patients.