ISSN INTERNATIONAL STANDARD SERIAL NUMBER
ISSN 2782-4365
Проверить номер:

Научно-образовательный электронный журнал

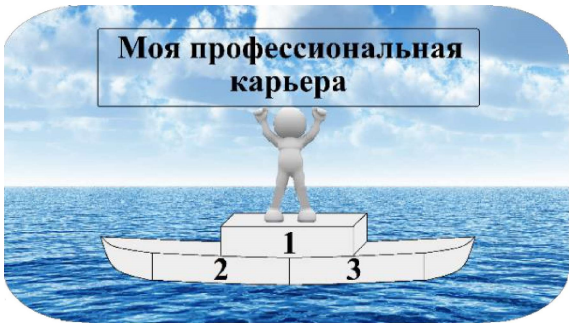
ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №61-1 (том 2)
(апрель, 2025)

Google Scholar
Проверить индексацию статьи. Сайт: mpcareer.ru/google

Свидетельство о регистрации СМИ №ЭЛ ФС 77-77927 от 19.02.2020 г.
РОСКОМНАДЗОР

Периодичность выпуска: 1 раз в неделю
Сайт: mpcareer.ru/oinv21veke. Почта: obrmpcareer@mail.ru



Международный научно-образовательный электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365
УДК 37
ББК 94

Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №61-1 (том 2) (апрель, 2025). Дата выхода в свет: 07.04.2025.

Сборник содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы образования (воспитателей, педагогов, учителей, руководителей кружков) и школьников, интересующихся вопросами, освещаемыми в журнале.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Рахматова Фотима Ганиевна	доктор философии по педагог. наукам (PhD), доцент
Рахмонов Азизхон Боситхонови	доктор педагогических наук, доцент
Таспанова Айзада Кенжебаевна	доктор философии (PhD) по экономическим наукам
Таспанова Жыгагул Кенжебаевна	доктор философии по педагог. наукам (PhD), доцент
Табашникова Ольга Львовна	кандидат экономических наук, доцент
Тўрабоева Мадинахон Рахмонжон қизи	кандидат педагогических наук, доцент
Тюрин Александр Николаевич	кандидат географических наук, доцент
Уразова Лариса Карамовна	кандидат исторических наук, доцент
Усубалиева Айнура Абдыжапаровна	кандидат социологических наук, доцент
Утегенова Жамила Джолмурзаевна	доктор философии по эконом. наукам, доцент
Фаттахова Ольга Михайловна	кандидат технических наук, доцент
Ширинов Отабек Тувалович	доктор психологических наук (PhD)
Хамдамова Ситора Сафаровна	Доктор философии в области философских наук, доцент
Ханбабаев Хакимжан Икрамович	доктор педагогических наук (DSc)
Худайкулов Хол Джумаевич	доктор педагогических наук, профессор
Худойбердиева Хурият Каримбердиевна	доктор философии (PhD) в социальной философии
Ширинов Отабек Тувалович	доктор психологических наук (PhD)
Эшназаров Журакул	кандидат педагогических наук, профессор
Эшназарова Фарида Журакуловна	доктор философии по философии (PhD)
Юнусова Бахора Ахтамжоновна	кандидат филологических наук, ассистент
Яхяева Сожида Абдурахимовна	доктор философии (PhD) в социальной философии

ФИО автора(-ов): *Nazarov Rahman Ovezovich*
Student, Oguz han Engineering and technology university of Turkmenistan
Название публикации: «CYBERSECURITY: PROTECTING THE DIGITAL WORLD»

Abstract

The pervasive integration of digital technologies into nearly every facet of modern life has created unprecedented opportunities and vulnerabilities. This abstract examines the critical field of cybersecurity, which encompasses the practices and processes designed to protect digital assets, including computer systems, networks, data, and software, from unauthorized access, use, disclosure, disruption, modification, or destruction.

Introduction to Cybersecurity

In the digital age, cybersecurity has become an essential field for safeguarding personal information, business assets, and even national security. Simply put, cybersecurity refers to the practice of defending computers, servers, networks, and data from malicious attacks, damage, or unauthorized access. As the world becomes increasingly interconnected, the need for robust security measures has never been more critical. Cybersecurity has evolved over decades. Early computer security efforts focused on preventing unauthorized access to mainframe systems. However, as the internet grew and new technologies emerged, the scope of cybersecurity expanded to address a wider variety of threats. Today, it's a dynamic and multifaceted field, encompassing everything from personal data protection to the defense of critical infrastructure.

The Future of Cybersecurity: As technology continues to advance, so too do the threats. The future of cybersecurity will be shaped by emerging trends, including the rise of artificial intelligence (AI), the growing number of connected devices, and the increasing sophistication of cyberattacks.

Emerging Threats: AI-powered cyberattacks are a growing concern, as cybercriminals are beginning to use machine learning algorithms to analyze vulnerabilities and automate attacks. Additionally, the rapid expansion of the

Internet of Things (IoT) presents new security challenges, as these devices often lack sufficient security measures.

Advancements in Security Technologies: On the defense side, cybersecurity technologies are constantly evolving. AI and machine learning are also being used to detect unusual patterns and potential threats more efficiently. Furthermore, advancements in quantum computing could revolutionize encryption methods, providing even more secure communication and data protection.

Global Collaboration: As cyber threats are often international in scope, collaboration between countries, organizations, and individuals will be essential for developing effective strategies. Sharing threat intelligence, establishing international cybersecurity standards, and cooperating on law enforcement efforts will be key to addressing the global nature of cybercrime.

Termines explanation:

1. Cybersecurity: Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks, theft, damage, or unauthorized access. It encompasses a wide range of measures and practices, such as firewalls, encryption, and threat monitoring, to safeguard data and infrastructure from malicious activity.

Malware : Short for *malicious software*, malware is a general term used to describe any software intentionally designed to harm or exploit a computer or network. Types of malware include:

- **Viruses**: Programs that attach themselves to legitimate files and spread to other programs and files.
- **Worms**: Self-replicating programs that spread without user intervention, often causing widespread damage.
- **Trojan horses**: Programs that appear legitimate but carry out malicious actions once installed.
- **Ransomware**: A type of malware that locks a user's system or data and demands payment (ransom) for its release.

- **Spyware**: Software that secretly gathers information about a user without their knowledge.

Phishing: is a type of cyber attack where attackers impersonate legitimate organizations or individuals to trick people into revealing sensitive information like passwords, credit card numbers, or personal details. Phishing is often carried out via deceptive emails, text messages, or websites.

Firewall : is a security system designed to monitor and control incoming and outgoing network traffic. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet). Firewalls can be hardware-based or software-based and help prevent unauthorized access to a computer or network.

Encryption: is the process of converting data into a code to prevent unauthorized access. It ensures that even if data is intercepted during transmission, it cannot be read or altered without the decryption key. Encryption is essential for securing sensitive information, especially in online transactions.

Multi-Factor Authentication: is a security measure that requires users to provide two or more verification factors before gaining access to a system. These factors typically fall into one of three categories:

- Something you know (e.g., a password or PIN)
- Something you have (e.g., a mobile device, security token, or smart card)
- Something you are (e.g., a fingerprint, retina scan, or voice recognition) MFA adds an additional layer of security, making it harder for attackers to gain unauthorized access.

DDoS (Distributed Denial of Service) Attack: occurs when multiple compromised computers are used to flood a network, server, or website with traffic, overwhelming its resources and causing it to crash or become unavailable to legitimate users. DDoS attacks are often used to disrupt services or distract from other malicious activities.

Social Engineering: refers to the psychological manipulation of individuals to gain access to sensitive information or systems. It relies on exploiting human behavior and trust rather than technical vulnerabilities. Phishing is a common form of social

engineering, but other methods include pretexting (creating a fake scenario to obtain information) and baiting (enticing a user to take an action that compromises security).

Zero-Day Exploit: refers to a security vulnerability in software or hardware that is unknown to the developer or vendor and, therefore, unpatched. These vulnerabilities are highly valuable to attackers because there is no existing fix or protection. Cybersecurity professionals aim to identify and patch such vulnerabilities before they can be exploited.

Insider Threat: is a security risk that comes from people within an organization, such as employees, contractors, or business partners. These individuals may intentionally or unintentionally misuse their access to systems, networks, or data. Insider threats can include data theft, sabotage, or unintentional security breaches.

Penetration Testing (Pen Testing, or "pen testing," is the practice of testing a system, network, or application to identify vulnerabilities that could be exploited by attackers. Ethical hackers or security professionals simulate cyberattacks to assess the security of a system and help organizations patch weaknesses before they can be targeted by malicious actors.

Data Breach: occurs when sensitive or confidential data is accessed, disclosed, or stolen without authorization. This can involve personal information, credit card details, medical records, intellectual property, or corporate secrets. Data breaches often result in significant financial losses, reputational damage, and legal consequences.

Advanced Persistent Threat (APT): is a prolonged and targeted cyberattack where an attacker gains unauthorized access to a network and remains undetected for an extended period. APTs are often carried out by nation-state actors or well-funded hacker groups aiming to steal sensitive data, spy on organizations, or disrupt critical infrastructure.

Vulnerability: is a weakness in a system, application, or network that can be exploited by attackers to gain unauthorized access, cause damage, or disrupt operations. Vulnerabilities can exist in software, hardware, or even organizational processes and are typically identified and patched through regular security updates and testing.

Patch Management : is the process of regularly applying software updates and security patches to address vulnerabilities and fix bugs. These patches are essential to protect systems from attacks that exploit known weaknesses. Effective patch management is a key aspect of maintaining cybersecurity.

Conclusion: The digital landscape is constantly evolving, and so too is the world of cybersecurity. As cyber threats become more sophisticated and widespread, it's essential for organizations and individuals to stay informed and adopt robust security measures. The key to effective cybersecurity lies in a combination advanced technologies, proper training, and an unwavering commitment to protecting valuable dataUltimately, securing the digital world is an ongoing journey, not a destination. It requires a continuous commitment to learning, adapting, and investing in both technological and human capabilities. By embracing a holistic and proactive approach, fostering collaboration, and prioritizing ethical considerations, we can collectively build a more secure and resilient digital future for all. The protection of our digital world is not just a technical imperative; it is a societal one, essential for fostering trust, enabling innovation, and safeguarding the very fabric of our modern lives..

Reference:

Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/

National Institute of Standards and Technology (NIST) Cybersecurity Framework: https://www.nist.gov/cybersecurity-framework

Center for Internet Security (CIS): https://www.cisecurity.org/

(ISC)²: https://www.isc2.org/

ISACA: https://www.isaca.org/

SANS Institute: https://www.sans.org/

Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/