МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

© Національний університет
«Одеська юридична академія», 2023

Чикунов Павло Олександрович
Застосування патернів проєктування у процесі конструювання програмного забезпечення 606

Щербина Юрій Володимирович,
Казакова Надія Феліксівна
Проблеми захисту великих даних 609

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Горбаченко Станіслав Анатолійович
Інформаційно-геометричні підходи в менеджменті кібербезпеки . . . 612

Василенко Микола Дмитрович,
Слатвінська Валерія Миколаївна
Забезпечення кіберзахисту кіберрозвідки 614

Ахмаметьєва Ганна Валеріївна
Використання хмарних ресурсів при викладанні спеціальних дисциплін в галузі інформаційних технологій в умовах військового стану 616

Бойко Віктор Дмитрович
Інструменти моделювання та аналізу даних у навчальному та дослідному процесі 618

Кухаренко Сергій Вікторович,
Стаднік Денис Андрійович
Забезпечення безпеки вебсерверів 622

Чепурна Олена Євгенівна,
Кулешова Євгенія Романівна
Сучасні математичні методи оптимізації заходів кібербезпеки 625

Баландіна Наталія Миколаївна
Алгебраїчна нелінійність S-блоків конструкції Ніберг при їх представленні функціями багатозначної логіки 627

Слатвінська Валерія Миколаївна
Цифровізація суспільства за допомогою gpt4 631

Drobchak Alla,
Kovalchuk Kostyantyn
Methods of information hygiene of citizens of Ukraine for the purpose of preventing cybercrime activities 633

Слатвінська Валерія Миколаївна,
Дрига Артем Вадимович
Організація змагань по типу Capture The Flag з напрямку Web В НУ «ОЮА» 637

6. Розвиток медицини: Штучний інтелект може бути використаний для збору та аналізу медичних даних, що допомагає у розробці нових методів лікування та діагностики хвороб.

Отже, з урахуванням складності та ризиків, пов'язаних з використанням інтелектуальних систем, важливо звернути увагу на етичні та соціальні наслідки впровадження цих технологій у суспільство.

Список використаних джерел:

1. LIVE session на тему «Chat GPT» від J. Scott Christianson на сайті Ukraine global faculty від 25.04.2023. URL: https://ugfacademy.mylearnworlds.com/course/chat-gpt
2. Єршова О. Л., Бажан Л. І. Штучний інтелект – технологічна основа цифрової трансформації економіки. *Статистика України*. 2021. № 3. С. 47-59. Doi: 10.31767/su.3(94)2021.03.06.
3. Радзієвська О. Г. Права та безпека особи в умовах соціальних і цифрових трансформацій. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : матеріали Всеукр. наук.-практ. конф., м. Київ, 2 грудня 2021 р. / наук. кер. О. А. Баранов ; упоряд.: В. М. Фурашев, С. О. Дорогих. – Київ – Одеса : Фенікс, 2021. С. 96–100.
4. Штучний інтелект в «Дії»: Мінцифри спілкується з OpenAI. URL: https://www.epravda.com.ua/news/2023/04/28/699579/

Ключові слова: цифровізація, GPT-4, штучний інтелект.
Key words: digitalization, GPT-4, artificial intelligence.

DROBCHAK ALLA

National University "Odesa Law Academy",
Senior Lecturer of Socio-political and Economic Department of Kryvyi Rih Faculty

KOVALCHUK KOSTYANTYN

National University "Odesa Law Academy",
holder of higher education

METHODS OF INFORMATION HYGIENE OF CITIZENS OF UKRAINE FOR THE PURPOSE OF PREVENTING CYBERCRIME ACTIVITIES

Cyber security is an important element of ensuring national security, as virtual space is becoming an increasingly important element of influence on public sentiment and encroachment on the imbalance of situations in the country. The article examines the problem of cyber security in the context of the individual, society and the state.

Today, virtual space has become a very important battlefield. Cybercrime, cyber terrorism and cyber war have become an integral part of the modern world. According to the Ukrainian Cyber Security Center of the Ministry of Internal Affairs of Ukraine, criminal groups use cyber attacks to commit crimes such as fraud, theft, distribution of malicious software, export

(ransom) and much more. In addition, cybercriminals use virtual space for espionage, reconnaissance and cyber attacks on the country's infrastructure. Thus, cyber security is an important element of ensuring the national security of Ukraine.

Personal cyber security is the protection of personal information stored on various electronic devices, such as computers, smart phones, tablets, and others. Cybercriminals can gain access to these devices and use the information stored on them for their own benefit. For example, they can use passwords stored on devices to access bank accounts or steal personal information that can be used for fraud and other crimes. Since today most people have access to the Internet and use various electronic devices, personal cyber security has become one of the most pressing issues.

To protect your personal information from cybercriminals, you need to follow a few simple rules:

1. Use complex passwords that contain letters, numbers, and symbols. Do not use the same password for different services.
2. Update the software on your electronic devices. Many software vulnerabilities that can be exploited by cybercriminals are fixed in new versions of programs.
3. Do not open links and files from unknown or suspicious senders. They may contain malware.
4. Use antivirus software to help protect your electronic devices from malware and other threats.
5. Do not send your personal information through untrusted communication channels such as e-mail or social media messages. It is better to use secure communication channels, for example, encrypted e-mail or messengers with end-to-end encryption.
6. Follow the principles of "principle of least permission" and "principle of necessity". Do not give access to your personal information and electronic devices to anyone except those who need it. Don't store too much information on your electronic devices to reduce the risk of theft.
7. Use two-factor authentication to access important information such as bank accounts or email inboxes. This will help increase the level of security and protect your data from unauthorized access.

In addition, it is worth remembering that cyber security does not depend only on the actions of individuals, but also on the actions of organizations and government institutions. For example, companies must ensure the security of their databases and other electronic systems that contain personal customer information. Government institutions should adopt cyber security laws and policies that ensure the security of citizens' personal data.

In addition to threats to personal information, cybercriminals can also use electronic devices to attack infrastructure and critical systems. For example, hackers can use the assembly of botnets to overload websites, hijack surveillance cameras, intercept critical information, and even block critical communications systems.

To prevent such attacks, it is important to ensure the cyber security of critical infrastructures and systems such as energy networks, financial institutions, medical systems and others. This can be achieved through the

development and implementation of cyber security standards, the use of modern encryption and authentication methods, and increased control and oversight of network connections.

In addition, cyber security should be considered when using smart devices and the Internet of Things (IoT). These devices may contain vulnerabilities that can be used to attack networks and other devices. For example, cybercriminals can exploit vulnerabilities in home automation systems to gain access to doors and windows, or use unsecured network cameras to spy.

To ensure the cyber security of smart devices and IoT, users must ensure Wi-Fi network security and use strong passwords to access devices. In addition, it is important to install software updates that fix detected vulnerabilities and to limit access to devices by setting individual access rules and firewalls.

Even with all measures to ensure cyber security, it cannot be guaranteed that an attack will not happen. That's why it's important to have a disaster recovery plan in place to quickly restore systems and networks after an attack. This can be achieved by backing up data, developing recovery plans, and running regular disaster recovery tests.

In addition, public cyber security is important to keep in mind, as cybercriminals can use widespread social media and other online resources to launch attacks. This can be done through phishing attacks, sending emails with malicious attachments or links to fake websites that require personal information. Such attacks can lead to leakage of personal information, theft of money and other negative consequences.

Therefore, users should be careful when opening e-mail and communicating on social networks. It's important to check the sender's address and not open attachments that look suspicious. In addition, it is important to use anti-virus software and ad-blocking programs to prevent network attacks.

In solving cyber security problems, it is important to pay attention to technical and organizational measures that ensure the security of electronic systems and networks. One of such organizational measures is the establishment of rules for access to information and files, which ensures the protection of confidential information from unauthorized access.

Organizations must develop strict access policies to ensure that only authorized users have access to sensitive information and systems. It is advisable to set different levels of access for different users to limit access to information only at the required level.

It is also important to use firewalls, which allow you to monitor network traffic and block dangerous connections. Firewalls can be configured to block certain types of traffic, set rules for network access, and check login requests.

There are also various types of encryption that ensure the security of information during its transmission. The most common types of encryption are SSL (Secure Sockets Layer) and TLS (Transport Layer Security). These protocols encrypt the data transmitted between computers, thereby ensuring the confidentiality of information and protection against unauthorized access.

Organizations can also use different types of software to protect against malware and viruses. Antivirus programs allow you to detect and block malicious programs that can cause damage to systems and data.

To provide more effective protection, organizations can use monitoring and intrusion detection systems (IDS / IPS). These systems allow you to detect and block attempts at unauthorized access to the network and systems.

However, despite all security measures, there is a risk of an internal threat, that is, the possibility of abuse of trust by employees of the organization. Therefore, it is important to conduct regular security audits to identify potential problems and vulnerabilities in an organization's systems and networks.

Ensuring information security is an ongoing process as threats become more sophisticated and inventive. Therefore, organizations must constantly improve their methods and approaches to protect against malicious attacks and ensure the security of their systems and data.

In a world where information is becoming increasingly important and valuable, protecting information and systems is an integral part of any organization's operations. The right security strategy and the use of modern technologies help protect against malicious attacks and preserve data privacy.

Organizations must understand that not having an appropriate security strategy can lead to serious consequences, such as data loss, privacy breaches, financial losses and reduced customer trust. It is therefore important that organizations take information security seriously and invest in the security of their systems and data.

In addition, training employees about security rules and the risks associated with careless use of information is also an important element of a security strategy. Every employee needs to know how to protect their data and the information they receive in the course of their work, and how to respond accordingly to potential security threats.

Therefore, ensuring information security is an important component of the activity of any organization, because data security is a necessary condition for successful work and development. Understanding the threats and taking the necessary steps to prevent them will help organizations protect their systems and data from malicious attacks and other threats.

The article draws attention to the importance of information security for any organization. The lack of an appropriate strategy can lead to serious consequences, such as data loss, privacy violations, financial losses and reduced customer trust. However, investing in the security of your systems and data, as well as training employees about security rules and the risks associated with careless use of information, can prevent such negative consequences. Therefore, ensuring information security is an important component of any organization's activities, and organizations must take it seriously and take the necessary measures to prevent threats.

Key words: cyber security, information, electronic devices, cybercriminals, passwords, software, vulnerabilities, malware, antivirus software, secure communication channels.

Ключові слова: кібербезпека, інформація, електронні пристрої, кіберзлочинці, паролі, програмне забезпечення, уразливості, шкідливе програмне забезпечення, антивірусне програмне забезпечення, безпечні канали зв'язку.