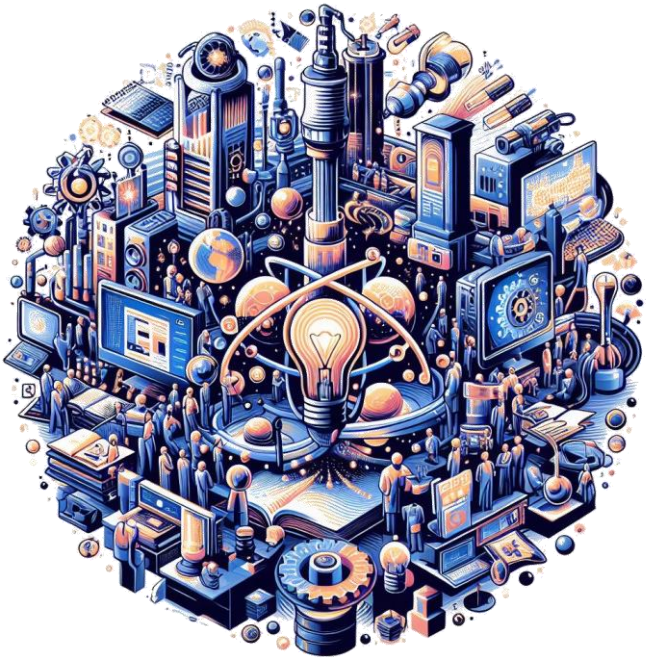
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТАВРІЙСЬКИЙ ДЕРЖАВНИЙ АГРОТЕХНОЛОГІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ ДМИТРА МОТОРНОГО

РАДА МОЛОДИХ УЧЕНИХ ТА ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

МАТЕРІАЛИ
XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА ПІДСУМКАМИ НАУКОВИХ ДОСЛІДЖЕНЬ 2023 РОКУ

ФАКУЛЬТЕТ ЕНЕРГЕТИКИ ТА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ



Запоріжжя 2024

УДК [620+621.3+004](043)
Т 13

XI Всеукраїнська науково-технічна конференція здобувачів вищої освіти ТДАТУ. Факультет енергетики та комп'ютерних технологій: матеріали XI Всеукр. наук.- техн. конф., 01-12 квітня 2024 р. Запоріжжя: ТДАТУ, 2024. 61 с.

У збірці представлено виклад тез доповідей і повідомлень, поданих на XI Всеукраїнську науково-технічну конференцію здобувачів вищої освіти Таврійського державного агротехнологічного університету імені Дмитра Моторного.

Тези доповідей та повідомлень подані в авторському варіанті.

Відповідальність за представлений матеріал несуть автори та їх наукові керівники.

Матеріали для завантаження розміщені за наступними посиланням:

http://elar.tsatu.edu.ua/?locale=uk
Електронний Інституційний репозитарій Таврійського державного агротехнологічного університету імені Дмитра Моторного

http://www.tsatu.edu.ua/nauka/n/rada-molodyh-vchenyh-ta-studentiv/
Сторінка Ради молодих учених та здобувачів вищої освіти ТДАТУ

Відповідальний за випуск: асистент Ганна Гешева

ЗМІСТ

Секція 1
ЕЛЕКТРОЕНЕРГЕТИКА, ЕЛЕКТРОТЕХНІКА ТА ЕЛЕКТРОМЕХАНІКА

Григоренко В. Я. Енергоменеджмент в Україні під час війни 5

Григоренко В. Я. Підвищення ефективності та модернізація засторілих будівель.....6

Грищенков О. С., Кот А. А. Зношення ізоляції асинхронного двигуна приводу робочої машини з гіперболічною механічною характеристикою в умовах провалу напруги 8

Коноваленко Є. О., Лопацький М. І. До питання оптимального визначення поняття «вимірювання» на основі моделювання.....11

Косяченко А. В. Попередження аварій в електричних мережах, що виникають під впливом ожеледі 14

Кот А. А. Визначення робочої зони пристроїв контролю утворення ожеледі на проводах повітряних ліній напругою 6-10 кВ.....17

Кот А. А. Обгрунтування ресурсозберігаючої технології зсідання молока при сироварінні...20

Myhulia V. New technologies for gas purification.....22

Олійник Д. Є. Розробка структури комбінованого захисного пристрою низьковольтного динамічного навантаження.....24

Павлюк Д. О., Галько С. В. Аналіз сучасних когенераційних фотоелектричних технологій.....26

Перегінець В. В. Перспективи застосування світильників з індукційними лампами.....31

Рощіна А. А. Визначення залежності повних опорів динамічного навантаження від несиметріїї напруги на затискачах 33

Сало І. Г., Галько С. В. Аналіз технологій та машин для пертворення вітрової енергії в інші види енергії 34

Федоренко С. А., Герасименко Б. Є. Прикладні аспекти нейромережевого моделювання у теорії поняття рішень.....38

Секція 2
КОМП'ЮТЕРНІ НАУКИ

Алгаєв О. В., Науменко В. А. Онлайн-інструменти для визначення відбивної здатності гетероструктур 41

Величко С. Д. Опис алгоритмів ідентифікації обличь 43

Здобувач вищої освіти 8454721 Застосування алгоритму Форда-Фалкерсона для розв'язування практичних задач із різних галузей.....45

Здобувач вищої освіти 8591961 Застосування теорії графів.....46

Кеяседінов Р. С. Застосування GPS для військової навігації та управління 47

Кот А. А., Клименко К. М. Дослідження хмарності: вимірювання та вплив на енергетичні можливості сонячної енергії (на прикладі м. Запоріжжя) 48

Lubko D., Velychko S. Study of the peculiarities of using stem education in schools and universities of Ukraine 50

Lubko D., Meleshko A. Analysis of the principles of protection of confidential and private information to ensure the security of organizations and people 53

Лялюк І. Р. Вплив інтернету речей на повсякденне життя та бізнес-процеси 56

Ролин Д. М. Тренди дизайну інтерфейсів 58

And the main advantage of STEM education for schoolchildren and students is their preparation for real life. At the last World Economic Forum in Davos, one of the central topics was the dramatic change in the labour market. About 60% of current human professions can be replaced by robots, which is a huge challenge for humanity. And the STEM approach allows children to develop flexibility and critical, practical thinking. The ability to learn and embrace change comes to the fore, rather than the knowledge itself, which is now becoming outdated at an incredible rate. This gives parent's confidence in the future of their children, because after using STEM teaching, children will have a deep understanding of how to live in today's dynamic and frantic world.

References

1. Vesela N. O. Stem-osvita yak perspektyvna forma innovatsiynoyi osvity v Ukrayini. *STEM-osvita ta shlyakhy yiyi vprovadzhennya v navchal'no-vykhovnyy protses*: zb. materialiv I rehion. nauk.-prakt. veb-konf. (m. Ternopil′, 24 travnya 2017 r.). Ternopil′: TOKIPPO, 2017. S. 25-28. [in Ukr.].

2. Chaykovs′ka H. B. Osvita dlya staloho rozvytku ta STEM-osvity: spil′ni vektory. *Suchasni tsyfrovi tekhnolohiyi ta innovatsiyni metodyky navchannya: dosvid, tendentsiyi, perspektyvy*: materialy IKH Mizhnarodnoyi naukovo-praktychnoyi internet-konferentsiyi (m. Ternopil′, 28 kvitnya 2022 r.). Ternopil′: TNPU im. V. Hnatyuka, 2022. S. 42-44 [in Ukr.].

3. Yurzhenko V. V. Tekhnolohichna osvita i STEM-osvita: yikh protylezhnist′ i fenomenolohichni paraleli. *Naukovi zapysky* [Tsentral′noukrayins′koho derzhavnoho pedahohichnoho universytetu imeni Volodymyra Vynnychenka]. *Seriya: Pedahohichni nauky*. 2019. Vyp. 177(2). S. 163-167 [in Ukr.].

4. Yel′nykova H . STEM-osvita v konteksti adaptyvnoho pidkhodu. Adaptyvne upravlinnya: teoriya i praktyka. *Pedahohika*.2018. Vyp. 4 [in Ukr.].

5. Barna O. V., Balyk N. R. Vprovadzhennya STEM-osvity v navchal′nykh zakladakh: etapy ta modeli. *STEM-osvita ta shlyakhy yiyi vprovadzhennya v navchal'no-vykhovnyy protses*: zbirnyk materialiv travnya I rehional′noyi naukovo-praktychnoyi veb-konferentsiyi, Ternopil′, 24 2017 r. Ternopil′: TOKIPPO, 2017. S. 3-8 [in Ukr.].

ANALYSIS OF THE PRINCIPLES OF PROTECTION OF CONFIDENTIAL AND PRIVATE INFORMATION TO ENSURE THE SECURITY OF ORGANIZATIONS AND PEOPLE

Lubko D., di75ma@gmail.com, **Meleshko A.**, Meleshko.alexandr.d@gmail.com
Dmytro Motornyi Tavria State Agrotechnological University

Data protection is a set of methods and tools that ensure the integrity, confidentiality and availability of information in the face of natural or artificial threats, the implementation of which may cause damage to the owners and users of information.

The basic principles of information and data protection include [1-5]:

1. Network segmentation. Dividing the network into segments helps limit the spread of possible threats, thus preserving important resources and private data.

2. Protection against intrusions. Use of firewalls, detection systems and other means to detect and block unauthorised intrusions.

3. Protection against malicious software. Installing anti-virus software and other security tools aimed at detecting and removing malware.

4. Data encryption. The use of encryption to protect confidential information to prevent unauthorised persons from accessing it.

5. Password and identification security. Use strong passwords, two-factor authentication and other methods to prevent unauthorised access to systems.

6. Security audit. Conducting a systematic audit and vulnerability assessment to identify potential security issues and vulnerabilities.

7. Training and user awareness. Educate users about safety rules, threat awareness and safety procedures to reduce the risk of human error.

8. Regular updates and patches. Keeping the software up-to-date and addressing identified vulnerabilities to prevent exploitation.

9. Physical security. Protection of physical access to server rooms, computers and other equipment containing confidential (or private) information.

10. Data retention and backup policy. Develop a data retention policy, make regular backups and store them in secure locations.

11. Securing wireless networks. Ensuring the security of wireless networks through the use of encryption, authentication and other methods.

12. Double verification. Use two-factor authentication and double-check to increase security when logging into systems and resources.

13. Access to information policy. Developing a clear policy that defines who has access to certain information and taking measures to control this access.

14. Protection against social engineering. Educate users about social engineering and other manipulation techniques to avoid leakage of confidential information.

15. Activity monitoring and analysis. Continuous monitoring of network and system activity to detect anomalous activity and potential security threats.

16. Regular training and testing. Conduct regular training and testing of security practices to ensure that staff are prepared to respond to various incidents.

17. Protection of personal data. Compliance with the requirements of the legislation on personal data protection and development of confidentiality and security policies for this data.

18. Protection against internal threats. Awareness of the possibility of an internal threat and taking measures to prevent the leakage of confidential information.

19. Incident response strategy. Developing an incident response strategy and plan to effectively detect, respond to and restore security after incidents.

20. Continuous improvement. Systematic review and improvement of security measures, taking into account new threats, technologies and strategies.

These principles are important for creating a comprehensive information and data protection strategy that will ensure a high level of security in the modern digital environment. These principles can also be adapted and expanded to meet the specific needs and requirements of organisations or individual users.

Next, let's look at the existing classes of information security. In the field of information security, there are several security classes that are used to classify data and systems according to their importance and sensitivity. These security classes help organisations design and implement effective security measures to protect their data. Unfortunately, the number of cybercrimes is growing every day, and a large proportion of these crimes is identity theft. Most often, this happens due to negligence and lack of awareness of users. That is why all this is a problem that needs to be addressed both personally and collectively. Today, cybersecurity can be seen as an important aspect of any state's policy in the context of the global information space, widespread communication and interaction via the Internet. To ensure its adequate provision, appropriate information security technologies, legislation at the state level, hardware and software, etc. are being developed [2].

One of the most common security classes is the confidentiality classification. This classification is based on how important the information is to the organisation and whose interests it protects. Data is classified as confidential, private, public or public. Confidential information is the most sensitive and requires the highest level of protection. This includes: state secrets, trade secrets and personal information, such as financial data or medical records; data about life-support systems, such as energy or water networks; data about critical infrastructure, such as transport or communications systems; data about research or development that could be used by competitors; data about strategic plans and marketing objectives that could be used to gain a competitive advantage; data about intellectual property that is highly

Let's analyse the security measures to protect confidential information: data encryption (use of modern encryption algorithms to protect confidential data); strict access control (limiting access to confidential information to authorised users only); security administration (development and implementation of a security policy that is appropriate to the nature of the data and threats); security awareness (regular training of staff on data security).

Let us also consider the existing levels of security. In short, they have three main blocks: international security, national security and personal security.

To protect confidential information, organisations should apply the following security standards: ISO/IEC 27005 (an international standard that defines requirements for an information security management system); NIST SP 800-53 (a standard of the US National Institute of Standards and Technology that defines requirements for an ISMS for government agencies); PCI DSS (a standard for payment card security requirements).

Private information is less sensitive but still requires protection. This information includes: data on employees, customers or suppliers that could be used for fraud or other crimes; data on marketing campaigns or market research that could be used by competitors; intellectual property data (e.g. copyrights to musical, poetry or prose works, paintings, etc.).

Next, let's analyse the critical threats to private information, including: phishing attacks on employees (unauthorised access to private data through manipulation of personnel); data loss due to careless handling and negligent use of personal information by employees; security measures to protect private information; security training (regular training of personnel on phishing techniques and personal security); regular security audits (periodic review of access and data protection policies); security administration (development and implementation of security plans); and

In order to protect private information, organisations (as well as individuals) are required (or recommended) to apply security standards such as: ISO/IEC 27001; NIST SP 800-53; HIPAA (a standard that defines the requirements for the protection of medical data).

Publicly available information is not sensitive and does not require special protection.

This information includes: information about goods and services, news and other data; data that has been published in publicly available sources. Threats to publicly available information may be less dramatic than to confidential or private information, but are still important to ensure the security of this category [4]. Namely, the use of data without permission (unauthorised use of publicly available information for advertising, fraud or other purposes; loss or damage to data, loss or damage to publicly available information can lead to losses for the organisation or users).

Data classification can be used to design and implement security measures: sensitive information (an organisation can use encryption to protect sensitive information, such as financial data or medical records; the organisation can also use strict access control rules to limit access to sensitive information to authorised users); private information (an organisation can use security training to raise awareness of phishing attacks and other

Security classes are a powerful tool that can help organisations protect their data. Understanding security classes and their application is important for anyone who works with information. Critical threats to private information can be diverse and come from a variety of sources, and they are constantly evolving as new technologies and hacking techniques emerge.

Conclusions. Threats to private information can come from a variety of sources, and it is important to have a broad set of security measures in place to protect data. This may include cryptographic encryption, two-factor authentication, regular security audits, social engineering training for staff, and regular updates to information and data protection systems.

General security measures, such as using strong passwords, regular software updates, using encryption, and training staff on social engineering, can help protect corporate and private information from these threats and ensure that organisations and people's information is well and securely protected.

References

1. Lubko D. V., Sharov S. V. Rozrobka ta vykorystannya snifera yak povne zabezpechennya bezpeky T·SR z′yednannya. Systemy obrobky informatsiyi. *Zbirnyk naukovykh prats′*. 2017. Vyp. 5 (151). C. 138-144 [in Ukr.].

2. Bohush V., Yudin O. Informatsiyna bezpeka derzhavy / Hol. red. YU. O. Shpak. Kyyiv: Vydavnytstvo «MK-Pres», 2005. 432 s. [in Ukr.].

3. Luzhets′kyy V. A., Kozhukhivs′kyy A. D., Voytovych O. P. Osnovy informatsiynoyi bezpeky: navchal′nyy posibnyk. Vinnytsya: VNTU, 2013. 221 s. [in Ukr.].

4. Michaelsen J. R., Vacca J. W. Information security risk management: A guide to managing risks to information assets. Springer, 2018.

ВПЛИВ ІНТЕРНЕТУ РЕЧЕЙ НА ПОВСЯКДЕННЕ ЖИТТЯ ТА БІЗНЕС-ПРОЦЕСИ

Лялюк І. Р., yuliya.kholodnyak@tsatu.edu.ua

Таврійський державний агротехнологічний університет імені Дмитра Моторного

У сучасному світі зростає важливість використання технологій, які забезпечують зв'язок між фізичними пристроями та забезпечують їхню взаємодію через Інтернет. Однією з таких технологій є Інтернет речей (Internet of Things або IoT), яка визначається як мережа фізичних об'єктів, які оснащені вбудованими технологіями зі здатністю збирати та обмінюватися даними. Розглянемо, як IoT впливає на наше щоденне життя та бізнес-процеси, і які можливості та виклики вона ставить перед нашим суспільством.

Інтернет речей - це концепція, яка полягає в з'єднанні фізичних об'єктів через мережу Інтернет, щоб вони могли збирати та обмінюватися даними. Ці об'єкти можуть включати все, від простих датчиків до складних пристроїв, які вбудовані у різні аспекти нашого повсякденного життя та бізнесу.

Інтернет речей (IoT) базується на комплексі технологій, які дозволяють фізичним об'єктам підключатися до Інтернету, обмінюватися даними та взаємодіяти з навколишнім середовищем. Основні технології, що лежать в основі IoT, включають наступні.

Бездротові мережі. Використання бездротових технологій, таких як Wi-Fi, Bluetooth, Zigbee, або NB-IoT, дозволяє підключати пристрої до Інтернету без потреби в проводах, що робить їх більш мобільними та доступними.

Датчики. Датчики є ключовою складовою частиною IoT, оскільки вони дозволяють збирати дані з навколишнього середовища. Ці дані можуть включати інформацію про температуру, вологість, рух, освітлення та багато іншого.

Хмарні технології. Використання хмарних сервісів для зберігання та обробки даних є невід'ємною частиною IoT. Хмарні ресурси забезпечують масштабованість, доступність та безпеку даних, що збираються пристроями IoT.

Штучний інтелект. Впровадження штучного інтелекту дозволяє пристроям IoT вчитися зі зібраних даних та робити автоматичні висновки. Це дозволяє вдосконалювати функціональні можливості пристроїв та оптимізувати їх роботу.

Використання IoT в повсякденному житті та бізнесі вносить значні переваги. По-перше, автоматизація процесів та оптимізація ресурсів завдяки збору та аналізу даних з пристроїв IoT дозволяє підвищити продуктивність та знизити витрати. По-друге, у повсякденному житті IoT пристрої, такі як розумний дім, роблять наше життя зручнішим та комфортнішим, дозволяючи контролювати різні аспекти нашого оточення за допомогою смартфона або голосових помилок. Ще однією перевагою є використання IoT для моніторингу та захисту різних аспектів нашого життя, включаючи відеоспостереження, системи безпеки вдома та відстеження медичних показників. Впровадження IoT створює нові можливості для розвитку бізнесу, такі як послуги на основі підписки, аналіз даних клієнтів та індивідуальне