https://doi.org/10.53656/math2024-1-6-art

Overview
Обзор

ARTIFICIAL INTELLIGENCE FOR GOOD AND BAD IN CYBER AND INFORMATION SECURITY

Nikolay Kasakliev, Elena Somova, Margarita Gocheva
University of Plovdiv "Paisii Hilendarski" — Plovdiv (Bulgaria)

Abstract. The contemporary digital world handles tremendous amounts of data, which are exposed to a variety of security threats. IT professionals are responsible for the protection of information systems, devices, networks, privacy of the collected data. The paper presents a literature review of artificial intelligence (AI) usage in information/cyber security. The main accent is set to the security threats and vulnerabilities. Some recommendations have been identified to increase the level of information security.

Keywords: artificial intelligence; information security; cyber security; security threats

1. Introduction

The digital world gives us constant connectivity across multiple channels and brings with it incredible amounts of transferred data and new forms of data management. As a result, people are constantly being monitored while consuming products, services, and content (Zarsky 2019). These possibilities have given rise to a variety of concerns, which include the protection of information systems, devices, networks, privacy of the collected data, and how they are stored and accessed. To address these concerns IT professionals use measures for information security or cyber security. These branches of computer science are similar but have some specifics.

Information security considers the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability (Nieles 2017). Cyber security is the practice of securing networks, devices, and data against unauthorized access or illegal usage, as well as the art of maintaining information confidentiality, integrity, and availability whereas cyber defensive mechanisms emerge at the application, network, host, and data levels (Zhang et al. 2022). No matter which aspect is considered, there is certainly an overlap between the two concepts, especially in data protection.

According to the National Institute of Standards and Technology (NIST), cyber security is a type of information security, but the two fields are not identical. For example, while information security affects data in print, electronic, or any other form, cyber security refers to only digital or electronic information or data. Therefore, in this study we will discuss security threats that affect both fields.

In recent years, threats to data have increased so much that people and systems have difficulties responding in time to cyberattacks, and therefore a new approach must be taken to improve protection. Today, many software security tools already use AI for incident response, disruption prediction, and performance monitoring. AI is a technology that can learn, understand, and act on the information it receives. It can identify and prioritize risks, enabling security professionals to instantly identify malware on their networks and develop an incident response strategy (Toxirjonovich 2022). (Alhayani et al. 2021) conclude that AI is an effective activity for reducing the impact of cyberattacks.

The main goal of the paper is to present a literature review of the AI usage in information/cyber security. Section 2 shows the research methodology. The main accent is set to the security threats and vulnerabilities as those using AI are discussed mostly in Section 3. The paper ends with a discussion and conclusion of the research (Section 4 and Section 5).

2. Methodology

The methodology of this research was to examine the state-of-art in the area of AI applications in Information/cyber security in two directions – first, security problems in software systems/applications, and second, technological realization of security threats and vulnerabilities.

The research questions to guide the search and analysis of the literature were defined:

RQ1. What are the main security problems in different software systems/applications?

RQ2. What are the major security threats and vulnerabilities faced by AI-powered applications and their technical realization?

RQ3. What are the protective AI approaches and tools in the domain of cyber security?

To collect the research papers, the following criteria were established:

- To use different academic search engines such as Academia.edu, ResearchGate, Google Scholar, and Semantic Scholar.
- Since this scientific field is relatively new, Internet pages with articles on the subjects should also be reviewed.

- The keywords to be searched for are: "AI", „Cyber threats", "Cyber security" and "Information Security".
- Only papers published in the last ten years are selected.
- Only publications written in English are included in this review.

3. AI in cyber security

According Europarl[1] AI is the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity. As mentioned in (Fetzer 1990) the problem of easy defining has two parts – artificial and intelligence, since securing an adequate grasp of the nature of the artificial would do only as long as we were already in possession of a suitable understanding of the idea of intelligence.

AI is the science and engineering of making intelligent machines, especially intelligent computer programs or systems of all kinds (Adamopoulos et al. 2023). Despite the rapid development, there is a debate as to whether today's AI systems are capable of thinking and feeling like a humans. A former Google expert claims that the Gemini chatbot is sentient due to the emotions that it expresses reliably and in the right context. Other experts claims that we are far away from the development of artificial general intelligence (AGI) or even that this is in principle impossible (Fjelland 2020). It is related to the task of using computers to understand human intelligence, but AI does not have to confine itself to biologically observable methods (McCarthy 2007).

Over the years, vast amounts of information have been collected to provide correct analysis and predictions (Yang et al. 2023). The development of AI is reaching critical points, increasing the influence of technologies related to virtual and augmented reality and integrating smart tools into various services, objects, and applications. These technologies are neural networks, big data, machine learning, data mining, computer vision, algorithms, and models (Marinov 2017).

3.1. The usage of AI for good and bad

Nowadays, the number of cyberattacks has increased both on different devices (enterprise, desktop, mobile, and IoT) and of different types (computer viruses, DDoS attacks, data breaches, cyberterrorism, phishing, etc.) – see for example Panda security[2].

In the past few years, cybersecurity researchers have started to explore AI approaches to improve cybersecurity. AI technologies, such as machine learning, can be used in cybersecurity to construct smart models for implementing malware classification, intrusion detection and threatening intelligence sensing (Li 2018). Machine learning algorithms are trained using vast

amounts of data, including historical threat data and data from the network and endpoints, to identify patterns that are difficult for humans to recognize (Moisset 2023). There is a concern that machine learning methods can easily be manipulated by providing deceptive input, known as adversarial attacks.

By continuously monitoring and analysing patterns, AI algorithms can detect deviations that may indicate potential threats, such as unauthorized access or abnormal user activities (Masum 2023). Likewise, cybercriminals are also using AI to launch increasingly sophisticated cyberattacks while hiding their tracks (Zeadally et al. 2020).

3.2. Main security problems in different applications

Security threats and vulnerabilities appear in different software systems/ applications.

1) Technology based Social engineering. Social Engineering (SE) is considered to be one of the most common problems facing information security today because attacks can be detected but not stopped (Salahdine 2019). SE is a manipulation technique that exploits human error to gain private information, access protected systems, spread malware, or other dangerous activity. SE attacks have many technology-based forms: phishing, vishing, baiting, and pretexting which can be enhanced by the power of AI.

2) Artificial Intelligent Chatbots Usage. One of the applications of AI is the creation of bots. A bot is a computer program that operates as an agent for a user or other program to simulate a human activity (Ukov 2022), while chatbots are computer programs designed only to simulate human conversation (text or speech) through AI, natural language processing, and machine learning technologies (Adamopolou 2020).

Chatbots can be Informative, Conversational, Task-based, and Rule-based (Adamopolou 2020). Today the most popular chatbots are ChatGPT, Google Bard, and Jasper Chat based on Generative AI, which use algorithms to generate new outputs based on the data they have been trained on (Routley 2023).

Chatbots face various security threats, including malicious input, user profiling, contextual attacks, and data breaches. Cybercrime has many aspects and problems in chatbots and can evolve into activities like intellectual property, stealing an identity, violating someone's privacy, data theft, malware development, phishing, vishing, spam, and misinformation (Bossler 2019). An example of intellectual property infringement is that ChatGPT can now generate Windows 10 and 11 keys for free (Tech desk 2023).

3) Political information security issues. The impact of AI on politics[3] will be profound or even can create political upheaval (Gallego 2022). AI may potentially be used to create incredibly persuasive deep fake videos, audio recordings and written content that has the potential to disseminate

inaccurate information, fabricate false news stories, and manipulate public sentiment (Thompson 2023).

Some researchers speculated that the ease with which a huge number of texts can be produced to support a political thesis, even an unfounded or a tendentious one, may multiply the manipulation of public opinion (Farina 2023).

The use of AI in politics has its positives. AI systems have the potential to increase political legitimacy by identifying pressing societal issues, forecasting potential policy outcomes, and evaluating policy effectiveness (Starke 2020). Another study finds that it is not easy to predict whether the development of AI-based technologies will radically change the existing political paradigm, but it could empower more diffused forms of political participation beyond elections (Savaget et al. 2019).

4) Disruption of the Information Infrastructure. An organization's Information infrastructure can be threatened by internal and external threats that can be implemented with the help of AI technologies. Normal business operations may be disrupted, stopped or anomalies may appear that may lead to security disasters even on Critical Information Infrastructures (CII) such as telecommunications, air transportation, the financial sector, the electric power grid, and many other services important for the economy and daily activity (Wilson 2014).

Often security threats are detected by identifying abnormal operations and anomalies. This is done through the use of intrusion detection systems (Kaur 2023) or security events logging. Security log analysis is the process of reviewing automatically computer-generated event logs to proactively identify security threats or other risks. Usually, they rely on signature-based systems that are limited in their ability to identify new and emerging threats or on programmers to manually inspect them by keyword search and regular expression match (Cao 2017). Powered by AI security log analysis can use unsupervised machine learning algorithms that can detect suspicion patterns and anomalies and analyse large volumes of data in real-time (Debnath et al. 2018).

3.3. Security attack threats

The most well-known security attack approaches connected to the AI are DDoS attacks, data theft, malware, phishing emails, vishing, and spam.

1) DDoS attacks. Distributed denial of service (DDoS) attacks has been increasing due to the rapid development of computer networks and cloud infrastructures. According to Microsoft, there were from 680 to 2215 attacks per day in 2022 that they were able to mitigate[4]. Usually, botnets play a main role and pose a major threat to network security as they are widely used for many crimes such as DDoS attacks (Hoque 2015). Recently, the

rise of AI-based botnets has drawn attention. AI-powered botnets can adapt, learn, and autonomously execute attacks (Dutt 2018). AI-powered botnets can mimic human behaviour, so that traditional security systems struggle to differentiate between legitimate users and malicious bots, allowing these botnets to operate undetected (Rama krishna 2023).

2) Data theft. Personal data, whether printed or electronic, is very important to every user and is protected with regulations such as GDPR that require adequate personal data protection (PDP) systems (Noninska 2022). Attackers use various tools and techniques to steal data including recently developed technologies using AI such as chatbots. ChatGPT's ability to impersonate others, write flawless text, and create code can be misused by anyone with malicious intent[5]. Data theft can be done more easily if chatbots use voice. Recently developed text-to-speech AI models (Microsoft VALL-E) can mimic voices by using audio samples to create a necessary replica. The company claims this chatbot can mimic any voice, including emotional tone, vocal cadence, and even background noise (Richey 2023).

3) Malware development. Researchers have found that AI-powered tools can aid in malware development. For example, in (Ben-Moshe 2022) is stated that a user with a rudimentary knowledge of malicious software could use tools like the AI-based system Codex, which translates natural language to code, to write functional malware in Python.

Ransomware is one of the routine threats to any organization's data security. It deals with some complex algorithms, and it's basically designed to block system files and wants ransom to provide the victims with the decryption key so that they can access the blocked content (Singh 2017). Specialists with help from ChatGPT managed to create ransomware code that can encrypt common data format files including running MS SQL database files and saving private (decryption) keys to remote servers (Sockley 2023).

4) Phishing emails. There is a legitimate concern that hackers will use AI-powered tools to write phishing emails that read like they were written by a professional. Researchers (Ben-Moshe 2022) found that ChatGPT could be used to easily create phishing emails.

Recent news shows that hackers are now developing their own malicious tool called WormGPT, which is described as "similar to ChatGPT but has no ethical boundaries or limitations" (Osborne 2023). Its primary use is for phishing and business email compromise (BEC) attacks.

5) Vishing. The term "vishing" is derived from a combination of "voice" and "phishing" (Yeboah-Boateng 2014). Scammers call potential victims, often using prerecorded robocalls, pretending to be a legitimate company to solicit personal information from a victim. With the help of AI-based tools scammers even can generate voices or clone them.

6) Spam. Spam is one of the major problems of today's Internet, bringing financial damage to companies and annoying individual users (Blanzieri 2008). Criminals who send spam usually take a few minutes to write the text and send it to hundreds and thousands. With generative AI, they can speed up their work by generating spam text instantly. Luckily, AI using Deep Learning Algorithms emerged as a powerful technique for spam detection due to its ability to automatically learn relevant features from raw data (Shoba et al. 2023).

4. Discussion

The paper highlights that AI can be successfully used for various cybersecurity threats. There is a clear need to use AI-related technologies to overcome these threats and develop procedures, policies and tools that can significantly increase information security. Recommendations that can be made in this direction are as follows:

- increase investments in AI-powered network monitoring tools that can track user behaviour, detect anomalies, identify unknown threats, and react accordingly;
- adapt and improve the Information Security Programs (ISP) according to new threats;
- introduce preventive measures such as training users to recognize AI-generated content, and the importance of human behaviour while using chatbots;
- improve skills of the Information Security Team.

The need to develop a regulatory framework (including Ethical Conduct) for AI developers also comes into focus. Ethical and practical concerns that will be included in the regulatory documents are very important to ensure sustainable and responsible development of the AI applications/systems in all aspects.

The role of AI in information and cyber security cannot be assessed unambiguously. The table 1 shows some of the advantages and disadvantages in the field of information and cyber security.

Table 1. Advantages and disadvantages of AI in information and cyber security

Advantages	Disadvantages
Faster threat detection Automating incident response Improved network security Improved accuracy and efficiency of security systems Behavioural analytics Improved AI-enabled authentication Identifying abnormal operations and anomalies	Data theft Malware development Privacy breaches Phishing, vishing, baiting, spam and pretexting enhanced by AI Manipulating public sentiment by deep fake videos, audio recordings and written content Sophisticated DDoS attacks Adversarial Attacks by manipulation of machine learning models

5. Conclusion

The paper explores the potential application of AI to implement cyberattacks of various types, as well as some approaches to detect and overcome them also with the help of AI. The state-of-art review, made of numerous research papers and internet pages, provides the answers to the research questions. The analysis of the review shows that there are legitimate concerns that AI can be successfully used for sophisticated cyber-attacks even by inexperienced cyber criminals. Some recommendations to increase information security are given. The need to develop a regulatory framework for AI developers is also discussed.

NOTES

1. Europarl, 2020. What is artificial intelligence and how is it used? URL: https://europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used
2. Panda security, 2021. 11 Emerging Cybersecurity Trends in 2021, panda, 12 April 2021. URL: https://pandasecurity.com/en/mediacenter/tips/cybersecurity-trends
3. Tech desk, 2023. ChatGPT can generate working Windows 11 keys, tribune, 19 June 2023. URL: https://tribune.com.pk/story/2422477/chatgpt-can-generate-working-windows-11-keys

4. Microsoft security, 2022. DDoS attack trends and insights, 2022 in review. URL: https://microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/Security-Insider_DDoS-Infographic.pdf
5. Malwarebytes, 2023. What is ChatGPT? AI Chatbots Security: Are AI chatbots safe to use? URL: https://www.malwarebytes.com/cybersecurity/basics/chatgpt-ai-security

REFERENCES

ADAMOPOULOS, I., ILIAS, A., MAKRIS, C., STAMATIOU, Y., 2023. Intelligent surveillance systems on the Internet of Things based on secure applications with the IBM cloud platform. *Int. Jourhal on Information Technologies & Security*, vol. 15, no. 2, 2023, pp. 59 – 74. https://doi.org/10.59035/XVRS3592

ADAMOPOULOU, E., MOUSSIADES, L., 2020. An Overview of Chatbot Technology. *Artificial Intelligence Applications and Innovations 2020*, Neos Marmaras, Greece. https://doi.org/10.1007/978-3-030-49186-4_31

ALHAYANI, B., MOHAMMED, H.S., CHALOOB, I.Z., AHMED, J.S., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*. ISSN 2214-7853. https://doi.org/10.1016/j.matpr.2021.02.531

BEN-MOSHE, SH., GEKKER, G., COHEN, G., 2022. *AI that can save the day or hack it away*. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

BLANZIERI, E., BRYL, A., 2008. A survey of learning-based techniques of email spam filtering. *Artificial Intelligence Review*, vol. 29, pp. 63 – 92. https://doi.org/10.1007/s10462-009-9109-6

BOSSLER, A., BERENBLUM, T., 2019. Introduction: new directions in cybercrime research. *Crime and Justice*, vol. 42, no. 5, pp. 495 – 499. https://doi.org/10.1080/0735648X.2019.1692426

CAO, Q., QIAO, Y., LYU, Z., 2017. Machine learning to detect anomalies in web log analysis. *Proceedings 3rd IEEE ICCC*, Chengdu, China, pp. 519 – 523. https://doi.org/10.1109/CompComm.2017.8322600

DEBNATH, B., SOLAIMANI, M., GULZAR, M.A.G, ARORA, N., LUMEZANU, C., XU; BO ZONG, J., ZHANG, H., JIANG, G., KHAN, L., 2018. LogLens: A Real-Time Log Analysis System. *IEEE 38th ICDCS*, Vienna, Austria, pp. 1052 – 1062. https://doi.org/ 10.1109/ICDCS.2018.00105

DUTT, D., 2018. *Reducing the impact of AI-powered bot attacks*. https://www.csoonline.com/article/565036/reducing-the-impact-of-ai-

powered-bot-attacks.html
FARINA, M., LAVAZZA, A., 2023. ChatGPT in society: Emerging issues. *Frontiers in Artificial Intelligence*, vol. 6. https://doi.org/10.3389/frai.2023.1130913
FETZER, J.H., 1990. What is Artificial Intelligence?. In: *Artificial Intelligence: Its Scope and Limits. Studies in Cognitive Systems*, vol. 4, pp. 3 – 27. Springer, Dordrecht. ISBN 978-0-7923-0548-4. https://doi.org/10.1007/978-94-009-1900-6_1
FJELLAND, R., 2020. Why general artificial intelligence will not be realized. *Humanities & Social Science Communication*, vol. 7, art. 10. https://doi.org/10.1057/s41599-020-0494-4
GALLEGO, A., KURER, T., 2022. Automation, Digitalization, and Artificial Intelligence in the Workplace: Implications for Political Behavior. *Annual Review of Political Science*, vol. 25, pp. 463 – 484. https://doi.org/10.1146/annurev-polisci-051120-104535
HOQUE, N., BHATTACHARYYA, D., KALITA, J., 2015. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242 – 2270. https://doi.org/10.1109/COMST.2015.2457491
KAUR, R., GABRIJELČIČ, D., KLOBUČAR, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, vol. 97. https://doi.org/10.1016/j.inffus.2023.101804
LI, J., 2018. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, vol.19, pp. 1462 – 1474. https://doi.org/10.1631/FITEE.1800573
MARINOV, R., 2017. *Intelligent and Neural Networks*. https://ebox.nbu.bg/mascom18/view_lesson.php?id=2
MASUM, M., 2023. *AI Cybersecurity, Artificial Intelligence Cybersecurity*. https://doi.org/10.13140/RG.2.2.36172.80009
MCCARTHY, J., 2007. *What is artificial intelligence?* http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html https://hub.cnetworks.info/wp-content/uploads/2023/07/whatisai.pdf
MOISSET, S., 2023. *How Security Analysts Can Use AI in Cybersecurity*. https://freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/
NIELES, M., DEMPSEY, K., PILLITTERI, V., 2017. An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. https://doi.org/10.6028/NIST.SP.800-12r1
NONINSKA, I., ROMANSKY, R., 2022. Organization of Technological Structures for Personal Data Protection. *International Journal on*

Information Technologies and Security, vol. 14, no. 1, pp. 97 – 106.
OSBORNE, CH., 2023. *WormGPT: What to know about ChatGPT's malicious cousin*. https://zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin
RAMA KRISHNA, S., 2023. T*he Dark Side Unleashed: The Threat of AI-Powered Botnets*. https://www.linkedin.com/pulse/dark-side-unleashed-threat-ai-powered-botnets-dr-s-rama-krishna
RICHEY, E., 2023. *4 ways scammers are using AI chatbots to steal data*. https://explore.quantumfiber.com/ways-scammers-use-ai-chatbots-to-steal/
ROUTLEY, N., 2023. What is generative AI? An AI explains. *World Economic forum*. https://www.weforum.org/agenda/2023/02/generative-ai-explain-algorithms-work
SALAHDINE, F., KAABOUCH, N., 2019. Social Engineering Attacks: A Survey. *Future Internet*, vol. 11, no. 4. https://doi.org/10.3390/fi11040089
SAVAGET, P., CHIARINI, T., EVANS, S., 2019. Empowering political participation through artificial intelligence. *Science and Public Policy*, vol. 46, issue 3, pp. 369 – 380. https://doi.org/10.1093/scipol/scy064
SINGH, A.P., 2017. *Ransomeware: a high profile attack. IRJET*, vol. 04 issue: 02. e-ISSN: 2395 -0056. https://irjet.net/archives/V4/i2/IRJET-V4I2365.pdf
STARKE, C., LÜNICH, M., 2020. Artificial intelligence for political decision-making in the European Union: Effects on citizens' perceptions of input, throughput, and output legitimacy. *Data & Policy*, vol. 2. https://doi.org/10.1017/dap.2020.19
STOCKLEY, M., 2023. *ChatGPT happy to write ransomware, just really bad at it*. URL: https://www.malwarebytes.com/blog/news/2023/03/chatgpt-happy-to-write-ransomware-just-really-bad-at-it
THOMPSON, S., 2023. *Artificial intelligence's impact on elections and democracy could be very real*. https://techinformed.com/artificial-intelligences-impact-on-elections-and-democracy-could-be-very-real/
TOXIRJONOVICH, O. N., FOZILOVICH, Y. O., 2022. Artificial Intelligence and its Application in Information Security Management. *Central Asian Journal of Theoretical and Applied Science*, vol. 3, no. 4, pp. 90 – 97. https://cajotas.centralasianstudies.org/index.php/CAJOTAS/article/view/451?__cf_chl_tk=zPJTpLHrpTzY3LenW86sdtvUAfZda5HM04F38DAv2S0-1707907898-0-4069
UKOV, T., TSOCHEV, G., 2022. Machine learning algorithm for intelligent bots in multiplayer video game: A case study. *Int. Journal on Information Technologies and Security*, vol. 14, no. 4, pp. 67 – 78.

http://ijits-bg.com/2022.v14.i4.07
WILSON, C., 2014. Cyber Threats to Critical Information Infrastructure. In: Chen, T., Jarvis, L., Macdonald, S. (eds) *Cyberterrorism*. Springer, New York. https://doi.org/10.1007/978-1-4939-0962-9_7
YANG, J., CHEN, Y.-L., POR, L.Y., KU, C.S., 2023. A Systematic Literature Review of Information Security in Chatbots. *Applied Sciences*, vol. 13. https://doi.org/10.3390/app13116355
YEBOAH-BOATENG, E.O., AMANOR, P.A., 2014. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4. ISSN 2079-8407.
ZARSKY, T.Z., 2019. Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law*, vol. 20, no. 1, pp. 157 – 188. https://doi.org/10.1515/til-2019-0006
ZEADALLY, S., ADI, E., BAIG, Z., KHAN, I.A., 2020. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access* vol. 8, pp. 23817 – 23837. https://doi.org/10.1109/ACCESS.2020.2968045
ZHANG, Z., HAMADI, H.A., DAMIANI, E., YEUN, C.Y., TAHER, F., 2022. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, vol. 10, pp. 93104 – 93139. https://doi.org/10.1109/ACCESS.2022.3204051

✉ **Dr. Nikolay Kasakliev, Assist. Prof.**
ORCID iD: 0000-0003-4010-144X
Department of Computer Science
Faculty of Mathematics and Informatics
University of Plovdiv "Paisii Hilendarski"
4000 Plovdiv, Bulgaria
E-mail: kasakliev@uni-plovdiv.bg

✉ **Dr. Elena Somova, Assoc. Prof**
ORCID iD: 0000-0003-3393-1058
Department of Computer Science
Faculty of Mathematics and Informatics
University of Plovdiv "Paisii Hilendarski"
4000 Plovdiv, Bulgaria
E-mail: eledel@uni-plovdiv.bg

✉ **Dr. Margarita Gocheva, Chief Assist. Prof.**
ORCID iD: 0000-0002-7739-5915
Department of Computer Science
Faculty of Mathematics and Informatics
University of Plovdiv "Paisii Hilendarski"
4000 Plovdiv, Bulgaria
E-mail: gocheva@uni-plovdiv.bg