sciendo

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **24**, No 3
Sofia • 2024 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2024-0030

Managing Cybersecurity: Digital Footprint Threats

Rumen Ketipov[1], *Roman Schnalle*[2], *Lyubka Doukovska*[1], *Dustin Dehez*[3]

[1]*Institute of Information and Communication Technologies - Bulgarian Academy of Sciences, Acad. G. Bonchev St., Bl. 2, 1113 Sofia, Bulgaria*
[2]*Bielefeld University, Universitätsstrasse 25, 33615 Bielefeld, Germany*
[3]*Secori advisors GmbH, Reuterweg 49, 60323 Frankfurt am Main, Germany*
E-mails: rketipov@iit.bas.bg roman.schnalle@uni-bielefeld.de
lyubka.doukovska@iict.bas.bg ddehez@secori.eu

***Abstract*:** *Managing cybersecurity and protecting data assets remain top priorities for businesses. Despite this, numerous data breaches persist due to malicious human actions, resulting in significant financial setbacks. However, many cybersecurity strategies overlook invisible or indirect threats within their scope, such as digital footprints. This paper examines the relationship between personality traits and user behavior concerning cybersecurity. The study suggests that human personality can be predicted using innovative techniques based on the digital hints individuals leave on the internet. Consequently, this information can be exploited for malicious actions against entities. As proposed, an effective strategy for improving behaviors and cultivating a security-oriented culture involves continually identifying relevant sources of cyber risks and implementing continuous awareness initiatives.*

***Keywords*:** *Information security management, Cybersecurity, Personality, Digital footprints, Human factor.*

1. Introduction

We live and do business in an uncertain world, where forces such as globalization, changing consumer expectation and perception, turbulence in the business environment, increased regulations and deregulations, and, not at least, the rapid and continuous development of technology create significant uncertainty. Whether small or large, private or public, domestic or international, enterprises nowadays operate in a risk-filled world and continue to extensively invest in technologies to counter cyber threats. However, even with the most advanced technologies, malicious cyber actors can gain access to sensitive data and critical infrastructure.

Organizations often struggle to understand and mitigate behavioral-based risks in Information Security (IS) by underestimating the human factor in their processes and management systems. Cyber attackers can manipulate the perceptions and minds of computer operators, rather than targeting the computer system itself, by using

techniques such as social engineering, cognitive hacking, and intelligence-based methods to impact human decision-making.

Nowadays, we conduct nearly every aspect of our lives online, including social interactions, entertainment, shopping, gathering and sharing information, booking holidays, and even work. Through these activities, we inadvertently leave digital traces that can be easily recorded, analyzed, and exploited, particularly in social engineering attacks. It is well-established that individual traits significantly shape human decision-making. The intricacies of human personality encompass various attributes, including behavioral, temperamental, emotional, and mental aspects, collectively defining the unique individual. Consequently, personality becomes the underlying catalyst influencing human choices, shaping perceptions, and guiding approaches in different situations.

Given that modern technologies, such as Machine Learning (ML), enable the prediction of human personality from online traces (see Section 3.1. Prediction of human personality), as well as the correlated behavior and decision-making (see Section 3.2. Prediction of user decision-making), cybersecurity professionals should reevaluate their threat landscape and the scope and approach of their awareness training. New and relevant threats must be continuously analyzed and identified, and clear expectations regarding information security must be communicated across the organization.

Taking into account the aforementioned aspects, this paper aims to review the human factor in information security and to explore whether various online traces can be analyzed to predict human personality. Additionally, it investigates if it is possible to predict certain decisions in specific situations and leverage these insights for information security purposes.

This understanding can assist information security managers and practitioners in rethinking and reassessing their systematic approach for continuous improvement and awareness programs, as increasing awareness of relevant security concerns is a crucial preventative measure.

2. Theories and models of personality measurement and analysis

Personality is commonly defined as an individual unique and relatively stable pattern of behavior, thoughts, and emotions that significantly impacts human behavior. These inherent factors contribute to the consistency of one's behavior, setting them apart from how others might behave in similar circumstances. Researchers find particular significance in studying these individual differences [1].

Numerous theoretical perspectives within the field of psychology explore various ideas about the development and formation of human personality. Some prominent approaches to understanding human traits include Sigmund Freud's psychoanalytical personality theory [2], Rogers' Person-centered Theory [3], Hans J. Eysenck's Three-Factor Theory [4], and the Five-Factor Theory of Personality, commonly known as the Big Five [5, 6]. The Big Five model, recognized as a contemporary measuring framework [7, 1], identifies and assesses human nature based primarily on biologically determined factors: Openness to experience,

Conscientiousness, Extraversion, Agreeableness, and Neuroticism/ Emotional stability [6, 8, 5].

The practical application of the Big Five framework is hindered by its extensive nature, comprising 240 elements. Consequently, the literature introduces several validated questionnaires that abbreviate and effectively utilize the Traits theory of personality [9]. One such alternative is the HEXACO framework, which preserves the original factors of the Five-Factor model while incorporating the crucial dimension of "honesty/humility" assessing the extent to which individuals prioritize others' interests over their own [10]. Another example is the RIASEC model, which assesses personality based on six main traits: realistic, investigative, artistic, social, entrepreneurial, and conventional [11].

In the United States, the Myers-Briggs Type Indicator (MBTI) stands out as one of the most widely used tests, particularly in the selection of workers. The MBTI posits that distinct personalities perceive the world differently, and the resulting profiles highlight attitudes, decision-making mechanisms, and interactions with the environment. MBTI doesn't evaluate personalities in terms of positive or negative judgments [12].

Additionally, the Ten-Item Personality Inventory by Gosling [1] is also rooted in the Big Five personality dimensions. However, it streamlines the assessment with only ten questions, providing two descriptors for each factor.

The acknowledgment that individuals sharing similar personality profiles often exhibit comparable behaviors suggests a correspondence in their inclinations and priorities. Given the diversity of personality traits, which distinguish individuals in their behaviors and preferences, it follows that each person approaches decision-making differently. Some individuals rely on their intuitions, while others prefer to deliberate on various alternatives before making a conscious decision.

The specific characteristics of personality exert significant influence not only on human character, attitudes, and habitual tendencies but also on the complexities of their decision-making processes [13].

3. Relationship between personality traits and decision-making

As mentioned above, human decision-making is not always based on principles of rationality. Instead, it is often influenced by personality, which becomes the basis of individual behavior in all its aspects. People with similar traits tend to exhibit a high tendency to behave in a particular way and to use a similar decision-making style in certain situations.

In practice, there are two main approaches where ML technology plays a crucial role in analyzing and predicting personality traits. On the one hand, analyzing large datasets is extremely useful for the development and validation of theories in psychology. For example, a vast amount of behavioral data on the internet, especially from social media, can be used to predict users' personality profiles. On the other hand, individual specifics can be used as predictors of decision-making in daily life, such as consumer behavior on the internet or business outcomes.

3.1. Prediction of human personality

Nowadays, people publish a huge amount of content that depicts their emotions and feelings through likes, dislikes, comments, photos, videos, tweets, reels, and more.

Often, online customers leave information about themselves, such as gender, age, education, and other sociodemographic characteristics, profession, political orientation, frequent use of certain functions in the purchasing process, method of payment, product type interests, and so on.

In all these digital hints, patterns can be recognized that reveal aspects of users' personalities. Applying Artificial Intelligence (AI) technique makes this possible.

Several studies have explored the relationships between personality traits and social network user profile features using ML. Below are some prominent examples.

Back in 2011, Golbeck, Robles and Turner [14] studied the specifics of personality based on data collected from users' Facebook profiles and applied ML algorithms.

Similarly, in 2011 Gosling et al. [15] identified several relationships between personality traits and the use of individual Facebook features. For instance, they reported a positive relationship between extroversion and the frequency of Facebook use and engagement. These findings align with Costa and McCrae's theory [6] that more extroverted individuals seek social engagement. In the online environment, extroverted individuals leave behind behavioral traces, such as a greater number of friendships, more comments, posts, and photos.

A study led in 2014 by Professor Kosinski et al. [16], applying the standard Five-Factor Model, focused on individual differences in internet behavior and personality preferences. Kosinski and his colleagues examined a sample of more than 350 000 US Facebook users. They analyzed how users' online behavior, captured by their website choices and profile characteristics, relates to their personality as measured by the Five-Factor Model. To predict personality based on multiple profile features, the team used Linear Regression and examined their results using 10-fold cross-validation.

The results obtained by Kosinski demonstrated that people with a high degree of openness are more likely to use Facebook as a communication tool and utilize a greater number of features. Individuals low in conscientiousness tend to join more groups and like more things. Interestingly, conscientious individuals not only joined groups less often but also used the "like" function less frequently. The research also shows that 25% of spontaneous users have more than 210 likes, while the same value for more conscientious users is lower by a third (140 likes). Extroverts are more inclined to reach out and communicate with other users, share more actively about their lives, and attend more organized events. Neuroticism was positively correlated with the number of likes, indicating that more emotional users tend to use the "like" function more often. While 75% of emotionally stable users have fewer than 150 likes, 75% of the most emotional users have more than 220 likes, suggesting that neurotic individuals are more likely to share personal information on Facebook [16].

The work of Lima and De Castro [17] also introduces an approach based on the Big Five model for predicting personality traits based on data from the traces people leave on social media. They create the so-called PERSOMA (PERsonality in

SOcial Media datA) model, which is based on the volume of messages published on Twitter to make a user profile based on linguistic analysis. By applying three ML algorithms (Naive Bayes, Support Vector Machines, and Multilayer Perceptron Neural Networks), the authors found that the traits of extroversion, agreeableness, and neuroticism could be predicted more accurately than others. However, this might be due to the initial labeling instrument used in the semi-supervised learning approach, which is primarily grammar-based and does not fully account for social behavior as addressed by their proposed method.

Professor Büttner at the University of Aachen, Germany, led a study in 2017 to investigate the influence of user personality on the use of career platforms, specifically the XING platform, and to determine which ML algorithms are best suited for this purpose [18]. The study was conducted with 395 participants using XING, and the TIPI test was applied to assess personality according to the Big Five. The results of the scientific research show that algorithms based on the decision tree model are the most suitable for this purpose. For example, the classification with Random Forests achieved one of the best results (61.9%) in predicting user personality, and C 5.0, another tree algorithm, achieved a result of 68.4%. The calculations included characteristics such as users' professional interests, number of groups joined, number of status updates, photo uploads, frequency and duration of platform use, visits to other profiles, number of comments and messages left, and number of contacts. The study demonstrated that ML could offer an innovative solution for analyzing users' personality traits based on professional social media, and the results could be used for electronic recruitment. w for the prediction of not only a candidate's suitability for professional requirements but also their compatibility with the company's philosophy, communication style, and organizational culture. The author nevertheless draws attention to the ethical issue in this case: potential candidates or current employees should not be discriminated against because of their personality, communication behavior, or political beliefs.

3.2. Prediction of user decision-making

As stated above, personality traits significantly influence our preferences and account for the diverse range of human behaviors and decisions. Concurrently, ML enables reliable estimation of user preferences based on individual characteristics.

One interesting study is the TITAN project, sponsored by the Italian Ministry of Universities and Research. In 2018 Bologna et al. [9] developed a recommendation system model for e-commerce that adapts product and service offers based on both user interests and personality traits. This model utilizes a Neural Network, incorporating the user's profile according to the RIASEC model as input data. The authors claim that this approach is effective for predicting user personality in e-commerce. For example, a financial manager might exhibit characteristics such as analytical/researcher, enterprising, and traditionalist/conventional (Investigative, Enterprising, and Conventional – IEC) [9].

Another valuable study in this domain in 2019 was led by Kazemenia, Kaedi and Ganji [19], which examines decision-making behavior in online shopping using a sample of 194 individuals. This study includes the extraversion

scale from the Big Five personality traits and finds that highly extroverted online shoppers tend to buy accessories that complement their purchases. The authors used Multiple Linear Regression and optimized Decision Trees to forecast user preferences based on personality and decision-making styles.

In 2017 Bayram and Aydemir [20] employed the General Decision-Making Style Questionnaire (GDMSQ) and the Big Five Inventory, revealing that extraversion positively correlates with rational and intuitive decision-making styles while negatively correlating with avoidant decision-making styles. The regression analysis also revealed that agreeableness positively influenced intuitive and dependent decision-making styles. The conscientiousness trait had a positive impact on rational decision-making but negatively affected avoidant and spontaneous decision-making styles. Neuroticism positively influenced intuitive, dependent, and spontaneous decision-making styles. Lastly, openness positively impacted rational decision-making style.

A study conducted at the Bulgarian Academy of Sciences involving 226 respondents explored the relationship between fundamental personality dimensions and users' preferences in field of online shopping. Participants' personal profiles were established using the TIPI test, and their risk aversion was assessed with the Risk Averseness Scale of Donthu and Gilliland [21]. Additionally, information about their website feature preferences was collected. A bivariate analysis was then conducted to examine linear relationships between variables. To develop predictive equations, the study identified significant relationships between the six independent variables and various online store functionalities (dependent variables). Three ML models – Linear Regression, Decision Trees, and Random Forest – were proposed to forecast customers' needs, expectations, and preferences on the internet. Based on evaluation metrics, the Random Forest Model, optimized using genetic programming, provided the most accurate predictions of consumer behavior according to their personality traits. The study successfully demonstrates that user needs and expectations can be predicted with high accuracy in the domain of e-Commerce [22, 23].

4. The human factor in the cybersecurity threat landscape

The cybersecurity threat landscape is constantly changing as malicious cyber actors develop new and innovative techniques to exploit known or newly discovered vulnerabilities. Following Verizon's 2023 Data Breaches Investigations Report [24], 74% of all data breaches involved the human element. People were involved either through errors, the use of stolen credentials, or social engineering, whereat business email compromise attacks, essentially a form of pretexting, have nearly doubled in frequency, constituting over 50% of incidents categorized under the social engineering pattern.

Other studies also confirmed that social engineering, particularly spear phishing, continues to be a favored technique for attackers to carry out their malicious activities, whereby financial institutions were prominently targeted by phishers

worldwide in the last quarter of 2022, followed by SaaS/ webmail, and social media [25, 26].

According to the Microsoft Digital Defense Report 2023 [27] the first quarter of 2023 saw a more than tenfold increase in attempted attacks compared to the same period in 2022, rising from around 3 billion per month to over 30 billion (an average of 4000 password attacks per second targeting Microsoft cloud identities). The most targeted sectors in Europe include, among others, government, communications, finance, and energy.

On the other hand, the report highlights the growing trend of entities shifting toward cloud-based infrastructure, accompanied by an increase in associated risks. Cloud platforms provide global reach and scalability, enabling businesses to expand rapidly and access markets worldwide. However, this also requires that the cloud provider's infrastructure be robust and secure enough to meet these demands without compromising security or compliance. As more companies migrate their critical infrastructure to cloud-based platforms, the landscape of information security undergoes significant changes. This shift underscores the need for more comprehensive assessments of cloud service providers and an expanded scope for Information Security Management Systems (ISMS), encompassing both technological and legal aspects.

The report also highlights that the fundamentals of phishing have remained consistent over time, with approximately 90% of phishing attacks involving social engineering. These attacks typically use email to trick victims into revealing sensitive information, clicking malicious links, or opening harmful files. Business Email Compromise (BEC) attempts are observed daily, leveraging social engineering or computer intrusion techniques. The incidence of BEC attacks has surged, with over 156 000 daily attempts recorded between April 2022 and April 2023. Microsoft notes significant growth in the threat landscape as more attackers employ increasingly sophisticated techniques to compromise a growing footprint of services, devices, and users.

Information security cannot be solely achieved through technical measures; it depends on human actions and decisions. Therefore, trained personnel play a crucial role in protecting against cyber attacks. As stated by the German Federal Office for Information Security (BSI), “IT security is only as good as the person using the systems” [28]. Referring to a study by William Triplett (Department of Cybersecurity Leadership, Capitol Technology University) [29], humans form the weakest link in the rising number of cyberattacks and future research in cybersecurity would benefit from studying human behavioral factors using cognitive theories.

Artificial intelligence is continuously developing, and AI-powered attacks are expected to increase, driven by generative and predictive AI. Cybercriminals will leverage AI resp. ML techniques to automate and enhance their capabilities, making attacks more sophisticated and adaptive. Consequently, AI will play a significant role in defense evasion. Cybersecurity professionals must recognize the rapidly evolving threat landscape and reassess their holistic security strategies to stay safeguarded against new threats based on intelligent techniques. Entities must stay current and well-informed about the latest research and advancements in the realm of AI-driven

security threats and methods to prevent or mitigate these exploits. They should conduct regular security assessments to identify vulnerabilities and ensure their infrastructure remains compliant and secure.

5. Human-centric cybersecurity

For all types of organizations, continuous adaptation of risk management approaches is necessary to understand the risks involved in achieving objectives. Establishing a risk-challenge culture, where the human factor is pivotal, is crucial in the process of establishing any ISMS.

Human-centered security is an approach that recognizes the crucial role of the human factor in cybersecurity. It focuses on understanding and adapting to human behavior, psychology, and interactions, aiming to promote a security-conscious culture among employees, reduce human errors, and effectively manage cyber risks. This approach aims to foster a culture of collaboration, and shared responsibility.

Information shared on social web platforms can pose significant cyber threats due to risks such as phishing, data mining using ML, credential theft, corporate espionage, malware distribution, reputation damage, and location tracking. Mitigation strategies should focus on methodical analysis, user education, technical controls, and policy governance.

Organizations must stay up to date with scientific findings, innovative technologies, and emerging approaches to adequately identify and assess relevant threats and vulnerabilities. Associated risks must be identified, and appropriate protective and preventive measures must be implemented accordingly. Consequently, they must continually rescope and update their awareness programs (Fig. 1).

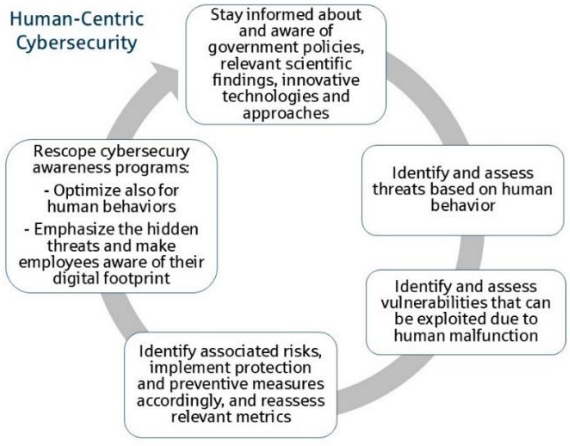

Fig. 1. Human-centric approach

It seems like cybersecurity frameworks and regulators have become increasingly aware of the crucial role of the human perspective in achieving desired cybersecurity levels, too. For instance, the ISO 27001:2022 Annex controls have undergone restructuring and consolidation to address current security challenges. The

updated Annex A control set reflects risks and their corresponding controls across Organizational, People, Physical, and Technological domains. The People controls encompass secure human resources management, personnel security, and awareness and training. In the latest ISO Norm 27001:2022, Control 5.7 highlights the importance of Threat Intelligence. It requires organizations to collect, analyze, and generate threat intelligence related to information security threats [30]. This involves identifying the tactics, techniques, and procedures employed by attackers to infiltrate compromise targets, thereby facilitating more targeted defense strategies. Such information can be sourced internally or externally, including from vendor reports, government agency announcements, relevant scientific studies, and other credible sources.

According to the Digital Operational Resilience Act (DORA) [31, 32], Article 8 mandates that financial entities must continually identify all sources of Information and Communication Technology (ICT) risk (Fig. 2). They are required to assess cyber threats and ICT vulnerabilities pertinent to their ICT-supported business functions, information assets, and ICT assets. A central aspect of DORA involves the stipulations for ICT risk management. These requirements aim to bolster companies' resilience against cyber threats, ensuring the continuity of their operations.

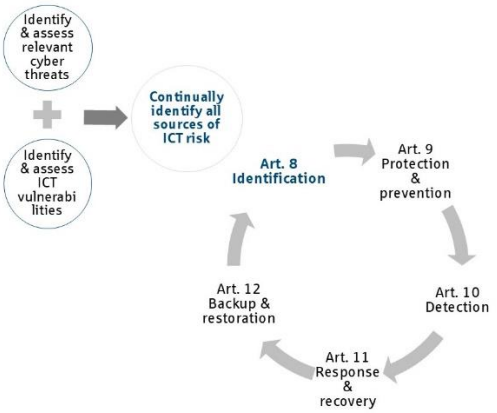

Fig. 2. DORA: Continually risk identification

Industry 4.0 presents new challenges for cybersecurity professionals. The advancement of technology necessitates updated perspectives, focus, and attention to various risk exposures. Industry 4.0 is characterized by an enormous amount of data and information, which is diverse in nature and can be combined in various ways. Intelligent data processing procedures enable real-time processing at different levels and deliver relevant conclusions. This increases risk exposure, as risks become more interconnected and can form global networks of vulnerabilities, often involving unknown sources [33].

It is a fact that many security issues with Large Language Models (LLMs) stem from the simple reality that their inner workings are a black box. This lack of clarity in how AI makes decisions is a key source of the associated risks. This underscores

the need for appropriate protective measures, where awareness will continue to play a critical role.

6. Conclusion and recommendations

It can be summarized that the present work successfully achieves its objectives by exploring several studies that demonstrate how our digital footprints can be analyzed to construct our personality profiles. This information can be exploited to manipulate decision-making processes across various domains.

Based on this knowledge, it is evident how crucial the key role of humans is in the process of scoping and building an ISMS. When analyzing the threat landscape, this aspect must be considered, and awareness programs should also incorporate this understanding.

Advanced technologies enable us to create our digital world, but they also increase our vulnerability to information security threats. As we conduct many of our daily activities online, it is crucial for awareness programs to emphasize securing employees' digital footprints. This includes regularly reviewing privacy settings on social media platforms to ensure that only necessary information is visible to others. Employees should consider whether any public information could be misused to harm their employer and avoid sharing excessive personal details that could build a detailed profile of their personality.

It is essential to scrutinize shared information to prevent the unauthorized outflow of technical know-how and internal knowledge, personalized spear phishing attacks, targeted identity theft, theft of other sensitive information through intelligent methods, targeted bullying and cyberstalking, and potential influence on professional decisions. It is important to remember that once information is published online, it is almost impossible to delete. Our digital footprints remain stored and can be analyzed, potentially influencing our actions based on this data. Therefore, sharing tasks and information about professional activities on social networks should be avoided.

References

1. Gosling, S. D., P. J. Rentfrow, W. B. Swann. A Very Brief Measure of the Big-Five Personality Domains. – Journal of Research in Personality, Vol. **37**, 2003, No 6, pp. 504-528.
2. Freud, S. Three Essays on the Theory of Sexuality. Imago Publ., Co., 1949.
3. CogniFit. Theories of Personalities: Everything You Need to Know. 2018 (06.2024). **https://blog.cognifit.com/theories-of-personalities**
4. Eysenk, H. J. Dimensions of Personality. Methuen, London, 1947.
5. Goldberg, L. The Structure of Phenotypic Personality Traits. – American Psychologist, Vol. **48**, 1993, No 1, pp. 26-34.
6. Costa, P. T., Jr., R. R. McCrae. Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) Professional Manual. Odessa, FL: Psychological Assessment Resources, 1992.
7. Buettner, R. Predicting User Behavior in Electronic Markets Based on Personality-Mining in Large Online Social Networks. – Electronic Markets, Vol. **27**, 2017, No 3, pp. 247-265.
8. McCrae, R. R., O. P. John. An Introduction to the Five-Factor Model and Its Applications. – Journal of Personality, Vol. **60**, 1992, No 2, pp. 175-215.

9. B o l o g n a, C., A. C. D e R o s a, A. D e V i v o, M. G a e t a, G. S a n S o n e t t i, V. V i s e r t i. Personality-Based Recommendation in e-Commerce. – In: Proc of 1st Workshop on Emotions and Personality in Personalized Services Conference: EMPIRE 2013 Workshop, 2018.
10. A s h t o n, M. C., K. L e e. The Prediction of Honesty-Humility-Related Criteria by the HEXACO and Five-Factor Models of Personality. – Journal of Research in Personality, Vol. **42**, 2008, No 5, pp. 1216-1228.
11. H o l l a n d, J. L. Making Vocational Choices: A Theory of Vocational Personalities and Work Environments. 3rd Edition. Odessa, FL: Psychological Assessment Resources, 1997.
12. MBTI Foundation**.** MBTI Basics. 2024 (06.2024). **https://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/home.htm?bhcp=1**
13. M C L e o d, S. Theories of Personality, Simply Psychology. 2024 (05.2024). **https://www.simplypsychology.org/personality-theories.html**
14. G o l b e c k, J., C. R o b l e s, K. T u r n e r. Predicting Personality with Social Media. – In: Proc. of Conference on Human Factors in Computing Systems ACM SIGCHI, 2011, pp. 253-262.
15. G o s l i n g, S. D., A. A. A g u s t i n e, S. V a z i r e, N. H o l z m a n, S. G a d d i s. Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. – Cyberpsychology, Behavior, and Social Networking, Vol. **14**, 2011, No 9, pp. 483-488.
16. K o s i n s k i, M., Y. B a c h r a c h, P. K o h l i, D. S t i l l w e l l, T. G r a e p e l. Manifestations of User Personality in Website Choice and Behaviour on Online Social Networks. – Machine Learning, Vol. **95**, 2014, pp. 357-380.
17. L i m a, A. C. E. S., L. N. D e C a s t r o. A Multi-Label, Semi-Supervised Classification Approach Applied to Personality Prediction in Social Media. – Neural Networks, Vol. **58**, 2014, pp. 122-130.
18. B ü t t n e r, R. Prädikative Algorithmen zur Persönlichkeitsprognose auf Basis von Social-Media-Daten. – Personal Quarterly, 2017, pp. 22-27.
19. K a z e m i n i a, A., M. K a e d i, B. G a n j i. Personality-Based Personalization of Online Store Features Using Genetic Programming: Analysis and Experiment. – Journal of Theoretical and Applied Electronic Commerce Research, Vol. **14**, 2019, No 1, pp. 16-29.
20. B a y r a m, N., M. A y d e m i r. Decision-Making Styles and Personality Traits. – International Journal of Recent Advances in Organizational Behaviour and Decision Sciences, Vol. **3**, 2017, pp. 905-915.
21. D o n t h u, N., D. G i l l i l a n d. The Infomercial Shopper. – Journal of Advertising Research, Vol. **36**, 1996, pp. 69-76.
22. P o p c h e v, I., R. K e t i p o v, V. A n g e l o v a. Risk Averseness and Emotional Stability in e-Commerce. – Cybernetics and Information Technologies, Vol. **21**, 2021, No 3, pp. 73-84.
23. K e t i p o v, R., V. A n g e l o v a, R. S c h n a l l e, L. D o u k o v s k a. Predicting User Behavior in e-Commerce Using Machine Learning. – Cybernetics and Information Technologies, Vol. **23**, 2023, No 3, pp. 89-101.
24. Verizon. Data Breach Investigations Report. 2023 (05.2024). **https://www.verizon.com/business/resources/reports/dbir/2023**
25. European Union Agency for Cybersecurity. Enisa Threat Landscape 2022. 2023 (05.2024). **https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022**
26. Statista. Phishing Most Targeted Industry Sectors Worldwide Q4 2022. 2023 (04.2024). **https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/**
27. Microsoft. Microsoft Digital Defense Report 2023. 2023 (04.2024). **https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023**
28. Federal Office for Information Security. Cyber Security Recommendations by Attack Targets. Human Factors. 2023 (04.2024). **https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/faktor-mensch_node.html**
29. T r i p l e t t, W. J. Addressing Human Factors in Cybersecurity Leadership. – Cybersecurity and Privacy, Vol. **2**, 2022, No 3, pp. 573-586.

30. E d w a r d s, M. ISO 27001:2022 Annex a Explained. 2024 (04.2024).
https://www.isms.online/iso-27001/annex-a/
31. European Insurance and Occupational Pensions Authority. Digital Operational Resilience Act (DORA). 2023 (05.2024).
https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
32. Federal Financial Supervisory Authority. DORA: The Countdown Has Begun. 2024 (05.2024).
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2024/fa_bj_2402_DORA_en.html
33. P o p c h e v, I., I. R a d e v a, I. N i k o l o v a. Aspects of the Evolution from Risk Management to Enterprise Global Risk Management. – Engineering Sciences, Vol. **LVIII**, 2021, pp. 16-30.

Received: 25.06.2024; Second Version: 08.08; Third Version: 12.08.2024;
Accepted: 13.08.2024 fast track)