Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, computer science, mechanics series, 2024, Vol. 149, №4, P. 6-21.
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

Article
IRSTI: 06.54.31

DEVELOPMENT OF A PENETRATION TESTING METHODOLOGY FOR WIRELESS NETWORKS TO ENHANCE SMART CITY SECURITY IN KAZAKHSTAN [1]

T.K. Zhukabayeva [1], A.D. Adamova [2*], N.Y. Karabayev [3], V.A. Desnitsky [4], N.S. Glazyrina [5]

[1,2,3,5] *L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan*
[4] *St. Petersburg Federal Research Center of the Russian Academy of Sciences, 39, 14th line V.O., St. Petersburg, 199178, Russia*
*(*corresponding author: aigul.dyusenbinovna@gmail.com)*

Abstract. Modern cities are increasingly adopting information technologies and becoming "smart". It is important to note that with the development of technology, the potential for cyber attacks also increases. This paper examines the significant problem of wireless network cybersecurity in smart cities of Kazakhstan. The study proposes a comprehensive penetration testing approach to identify and mitigate vulnerabilities in wireless networks. This approach includes a strategy that promotes security in the smart city ecosystem and supports Kazakhstan's overall efforts to protect urban infrastructure. Particular attention is paid to the vulnerabilities of wireless networks, which are a key element of the infrastructure of smart cities. This paper proposes a comprehensive approach to penetration testing aimed at identifying vulnerabilities in the wireless networks of smart cities. This approach includes various stages, starting with collecting information about the target system and ending with a detailed report on the identified vulnerabilities. The research results can contribute to enhancing cybersecurity in smart cities in Kazakhstan and the development of effective strategies for protection against cyberattacks.

Keywords: penetration test, smart city, cybersecurity, IoT, vulnerability, data security, information security, Kazakhstan.

DOI: https://doi.org/10.32523/bulmathenu.2024/4.1

2000 Mathematics Subject Classification: 94-10; 94A05

1. Introduction

In today's digital world, smart cities are a key factor in urban development, which are the integration of information and communication technologies that contribute to the improvement of the

[1]This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR24992852 "Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens' quality of life improvement")

efficiency of services, infrastructure and the quality of life of citizens in general. According to the report of the analytical agency Research and Markets, the global smart city market is projected to grow with an annual growth rate (CAGR) of 24.81?%, reaching US$345.8 billion by 2028 [1]. The market growth rate is influenced by progressive technologies in the field of the Internet, artificial intelligence and big data. It is important to understand that with growth, the risk of cyber attacks will also increase, which will target the main infrastructure of developing cities. Major trends include integration of smart grids, power grids, intelligent systems, and energy efficiency [2]. The Reference Standard of Smart Cities of the Republic of Kazakhstan was approved in 2019 in order to standardize approaches to their creation. The priority spheres of life of a smart city are security, transportation, housing and utilities, education, healthcare, and city management. Figure 1 shows the ecosystem of a smart city.

Figure 1 – Smart city Applications.

According to the benchmark standard of "smart" cities of the Republic of Kazakhstan, Smart city is defined as an innovative city that uses information and communication technologies and other modern tools to improve the quality of life of its residents, optimize activities and improve services. This model of urban development is also aimed at strengthening the competitiveness of cities, while ensuring the satisfaction of the needs of both present and future generations in various aspects: economic, social, environmental and cultural [3]. The most important element of the smart city strategy is the integration of digital initiatives - projects that are not only implemented within the general concept of Smart city, but also aimed at improving the level of comfort and safety of citizens' life. These initiatives can cover a variety of areas, including smart lighting, traffic management, environmental monitoring systems, and other technologies that contribute to a more comfortable and safer urban environment. Successful examples of such projects include the introduction of smart grids to manage resources such as water and electricity, which allows for more efficient use of resources and reduces the negative impact on the environment. Figure 2 shows the internal ranking of the Republic of Kazakhstan on smart cities based on data for 2020 [3].

The presented rating reflects the current state and dynamics of urban development in the context of Smart city concept implementation, and also reveals the strengths and weaknesses of each region. Analysis of the collected data will allow not only to evaluate the achieved results, but also to

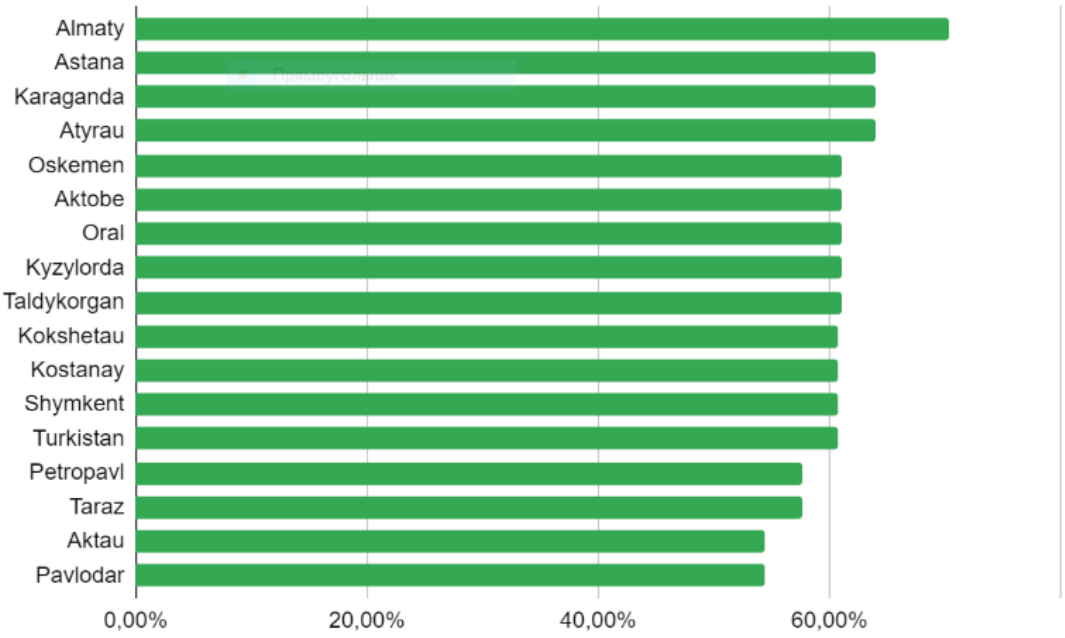


Figure 2 – Internal rating of the Republic of Kazakhstan for "smart" cities for 2020 [3].

formulate recommendations for further improvement of the urban infrastructure and enhancement of the quality of life of citizens.

According to the E-Government Survey 2024 report, Kazakhstan ranks 24th out of 193 in the UN Global E-Government Development Index (EGDI), and first among landlocked developing countries [4]. Figure 3 shows the e-government development index of Kazakhstan in comparison with other Asian countries. This index serves as an important indicator of the level of digitization of public services and the effectiveness of the use of information and communication technologies in governance. The index consists of several main components, including the availability and quality of electronic services, the level of citizen participation in the e-government process, and the degree to which government agencies are prepared and equipped with the necessary resources to provide digital services [4].

As can be seen from the figure, Kazakhstan demonstrates positive dynamics in the development of e-government, which is confirmed by its high scores on various indicators. This is the result of a targeted government policy aimed at introducing modern technologies in the sphere of public administration and improving the quality of services for citizens. Thus, the analysis of the index of e-government development not only reflects the current state of digitalization in Kazakhstan, but also provides useful data for developing strategies for further development in this area, which will ultimately lead to an improvement in the quality of life of citizens and strengthen confidence in public institutions.

Cybersecurity in smart cities has become a major issue. Wireless networks, which serve as the backbone of city services, are particularly vulnerable to a variety of cyber threats, including man-in-the-middle (MITM) attacks, data leaks, and distributed denial-of-service (DDoS) attacks. With the increasing use of Internet of Things (IoT) devices and interconnected systems in smart cities, the complexity and number of potential security vulnerabilities are increasing, making the development of robust methods to protect these infrastructures extremely urgent.

While the introduction of new technologies can improve service delivery and government efficiency, it can also expose local communities to cyber attacks from a variety of malicious actors.A major challenge for smart cities is cybersecurity. Cyberattacks on cities can cause significant damage, including disabling or compromising vital services such as electricity or water. For example, the municipal water authority of Aliquippa, Pennsylvania, USA was susceptible to a cyberattack in

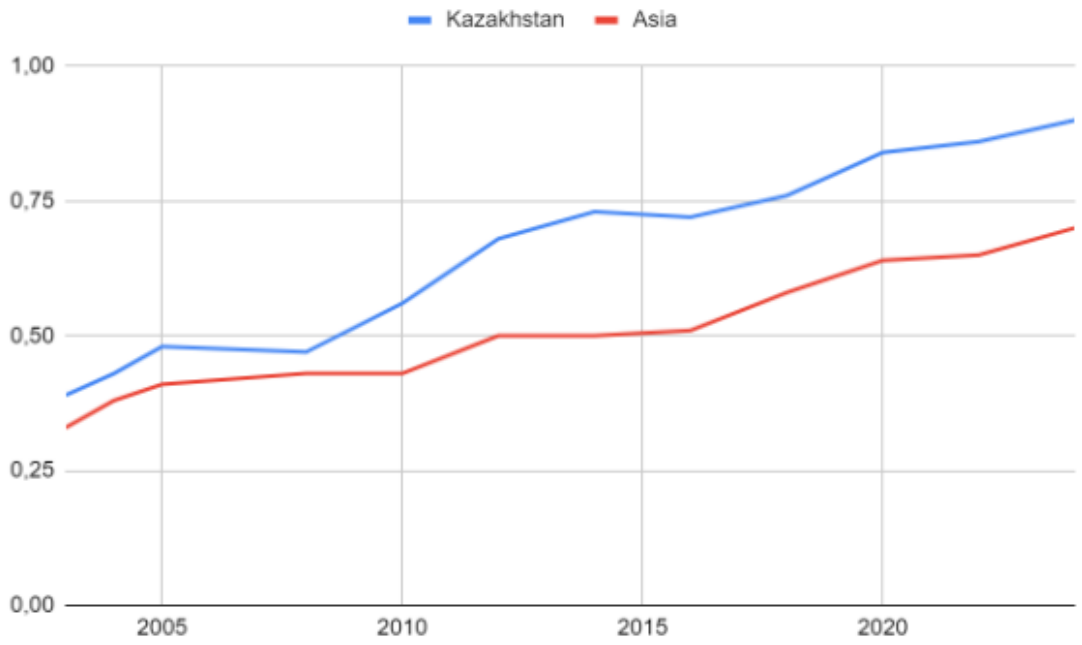


Figure 3 – Kazakhstan and Asia e-Government Development Index [4]

2023. As a result, the water pressure control system was compromised [5]. The transportation system of Olsztyn, Poland was paralyzed by a cyberattack in 2023. The attack affected almost a hundred intersections in the city center, disrupting the operation of traffic lights and other important elements of the transportation system [6]. Also in China, a facial recognition database leak affecting the surveillance system in Chinese smart cities was discovered in 2019 [7]. And this is only a small part of the cases with cyberattacks on smart cities. The software development company Stormshield provides an overview of cyberattacks on smart cities [8]. Given the potential risks associated with the development of smart cities, ensuring the safety of the population and infrastructure becomes a top priority for their sustainable development.

Despite the growing awareness of cybersecurity issues in smart cities, few studies focus on specific penetration testing methodologies that take into account the unique vulnerabilities of wireless networks in this context. This paper aims to fill that gap by proposing a comprehensive penetration testing methodology specifically designed for wireless networks in Kazakhstan's smart cities. The methodology offers a systematic approach to identifying and mitigating security risks, thereby enhancing the resilience of urban infrastructure to cyber threats.

The main objective of the paper is to investigate wireless network penetration testing techniques in the context of digital city ecosystems. In order to achieve the objective, it is necessary to accomplish the tasks:

- To review the scientific literature and practical research in this area;
- To propose a methodology for comprehensive wireless network penetration testing.

The paper has been organized as follows: The second section will present an overview of previous works. The third section will present the vulnerability analysis of wireless networks, the comprehensive testing methodology will be presented in the fourth section. Future research directions are presented in the fifth section. Finally, the paper concludes in Section six, where the results of the conducted research are summarized.

2. Related work

The field of cybersecurity in smart cities is attracting more and more researchers every year, with various strategies being actively studied to reduce the risks associated with cyber threats. Key areas of research include the integration of modern machine learning algorithms and intrusion detection

systems to protect urban infrastructure. Mehdi et al. has presented the results of the analysis of smart city security issues aimed at tracking intrusion attempts and cyber attacks, where the research was conducted on the CICIDS2017 dataset. The obtained results highlight the ongoing need to monitor malicious activity and implement effective controls to prevent security incidents. However, in their study, they do not consider the role of penetration testing in identifying vulnerabilities of wireless networks [9]. Similarly, Amaizu et al. also studied machine learning methods for detecting cyberattacks in smart cities, demonstrating high performance of their models on various infrastructures. The work provides valuable insights into approaches to urban security, but does not focus on wireless network vulnerabilities, which is a critical aspect for smart city ecosystems [10].

During the literature review and analysis, studies that consider penetration testing methodologies were examined. For example, F. Almeida discussed the importance of penetration testing in identifying vulnerabilities in smart city infrastructure in his paper. Almeida presented the results of the analysis of 62 European research projects and as a result, presents multiple dimensions of cybersecurity risks, proposed mitigation strategies, contributing to a complete understanding of the smart city security landscape [11]. Andino et al. presented an intrusion detection system (IDS) using recurrent neural networks (RNN)-based AI and optimization methods, which contributed to the discussion of smart security solutions. In their paper, they presented the process of analyzing data obtained from smart meters and sensors, thereby highlighting the high potential of deep learning models to improve intrusion detection [12]. Similarly, Alaa et al. focused on ensemble IDS, emphasizing the performance and efficiency of cloud-based solutions. Their study used machine learning models to help improve IoT security in smart cities, but it is important to note that they do not consider penetration testing methodologies [13].

To improve the security of smart city wireless networks, Siriginedi et al. proposed a generative adversarial network (GAN) approach, while Muhammad et al. presented the results of a comparative analysis on AI-based intrusion detection systems, focusing on the diversity of datasets and deep learning algorithms applicable to smart cities. The obtained results substantiate the need for robust cybersecurity measures adapted to the unique challenges of the urban environment [15]. Also, the digital city ecosystem can be negatively affected by various attacks on smart home IoT devices. For example, Rohit et al. investigated automated penetration testing frameworks specifically for smart home IoT devices. In their study, they note the interrelatedness of home and city security measures, emphasizing the need for comprehensive assessment frameworks [16]. Kyungon et al. identified the need for vulnerability assessment, including penetration testing, to effectively secure IoT devices which were obtained from the analysis of 154 sources on cybersecurity and cyber forensics for smart cities [17]. Finally, Naila et al. in their study highlight the importance of preventing system infection rather than searching for already known malware [18].

Cybersecurity challenges in smart cities are driven by multiple factors, including the widespread adoption of IoT devices with varying levels of security and the interconnectedness of systems. Research shows that smart device touch interfaces can be a potential point of vulnerability in cyber-physical security systems. This is due to the possibility of using the sensor channel to infect devices with malware, which can further compromise data privacy [20].

To summarize, the research publications highlight a versatile approach to improving cybersecurity in smart cities, combining penetration testing, machine learning, and innovative detection systems to address the changing threat scenario. This study provides a foundation for further research aimed at developing more sustainable and safe urban infrastructures.

3. Common attacks in Smart City ecosystems

In the process of studying various published works in the research area, the most common types of attacks in the digital ecosystem of the city were identified. The attack scenarios range from cyber threats to physical interventions that impact the security and operation of urban systems. One critical example of such cyber attacks is the MITM attack, in which an attacker disrupts, interrupts, or spoofs communications between two systems [21]. The MITM attack process involves an attacker intercepting and potentially modifying communications between two systems during transmission

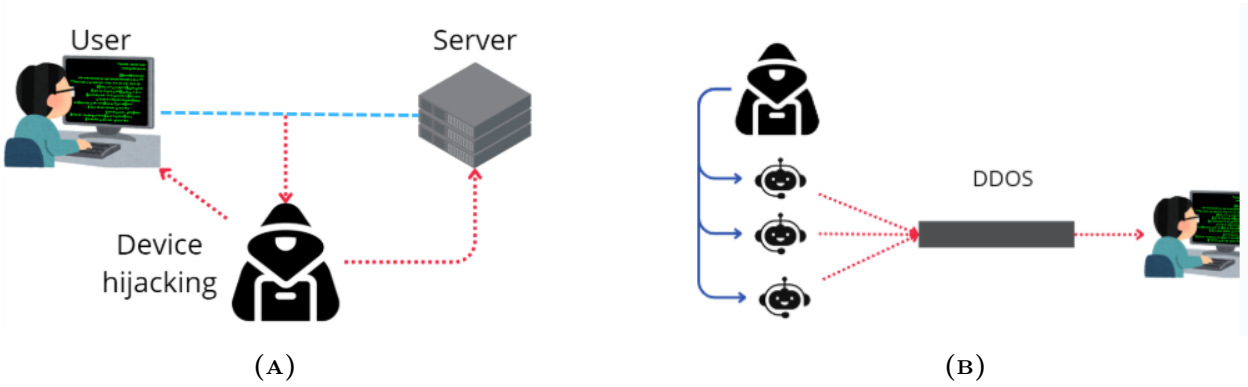
without the knowledge of the parties involved. In a digital city ecosystem, an attacker could target smart city utility management systems, such as a smart valve in a wastewater management system, resulting in serious disruptions such as a biohazard leak. Figure 4a shows a typical MITM attack flow, demonstrating how an attacker captures and manipulates traffic between two communicating devices. It is also important to note the possibility of theft of sensitive and personal data generated by unprotected smart city infrastructure. With the proliferation of IoT devices in smart cities, large amounts of personal data are generated and stored. Insecure smart city infrastructure makes it easy for cybercriminals to steal personal data, which can then be exploited for identity theft or fraudulent transactions [22]. The flow of a data theft scenario is depicted in Figure 4b, showing how attackers' access and misuse sensitive information.

(A) (B)

Figure 4 – Diagram of a MITM attack and Data/identity theft

Figure 5a shows a device hijacking scenario where an attacker seizes and actually takes control of a device [23]. These attacks can be difficult to detect because in many cases the attacker does not change the basic functionality of the device. In the context of a smart city, a cybercriminal could use captured smart meters to launch extortion attacks on energy management systems (EMS) or surreptitiously siphon energy from a municipality. Device hijacking involves cybercriminals gaining unauthorized control over smart devices. In the context of smart cities, this can include taking over devices such as smart meters to launch extortion attacks on energy management systems (EMS) or siphoning electricity from the grid. Figure 5a demonstrates how an attacker can take control of a device, often without changing its basic functionality, making it harder to detect the intrusion. Figure 5b depicts a typical DDoS attack scenario, emphasizing how multiple compromised devices can disrupt essential urban services. A DDoS attack floods a target system with an overwhelming amount of traffic, rendering the service unavailable to legitimate users. In smart cities, this could involve compromising a network of IoT devices, such as parking meters or traffic management systems, to form a botnet. This botnet would then launch simultaneous service requests, crippling the targeted infrastructure [24]. This is usually accomplished by flooding the target with redundant requests to prevent legitimate requests from being fulfilled. In the case of a distributed denial of service (DDoS attack), the incoming traffic overwhelming the target comes from multiple sources, making it difficult to stop the cyber attack by simply blocking a single source. In smart cities, multiple devices such as parking meters can be compromised and forced to join a botnet programmed to suppress the system by simultaneously requesting service.

Thus, the vulnerabilities discussed emphasize the need to develop comprehensive security measures to protect smart city infrastructure from a variety of cyber threats. The attacks described above highlight the importance of developing robust security measures for smart city infrastructures. As these cities grow increasingly interconnected, the vulnerabilities exposed by such cyberattacks pose significant risks to public safety, urban services, and citizen privacy.



(A) (B)

Figure 5 – Diagram of Device hijacking attack and DDoS

4. Methodology of Vulnerability detection

To effectively reduce the likelihood of a cyberattack, it is essential to localize and address weaknesses within the networks and systems that constitute smart cities. However, the complex architecture of smart cities, with their numerous interconnected devices, presents unique challenges. Our proposed penetration testing methodology provides a systematic approach to identifying vulnerabilities in wireless networks within smart city environments. The use of penetration testing is one method that can be used in the vulnerability localization process [25]. Simulating a cyber attack to find vulnerabilities in system defenses is an integral part of the penetration testing process. This approach can help discover weaknesses in smart city infrastructure, which can then be used to inform the development of security solutions to address these vulnerabilities [26].

The use of vulnerability scanners that can automatically find flaws in system software and hardware is another strategy that can be implemented [27]. Using these technologies, smart cities will be able to quickly detect weaknesses and fix them, preventing hackers from taking advantage of these weaknesses. In addition, smart cities should conduct regular security assessments to localize any potential vulnerabilities within their information technology infrastructure [28]. Such audits should be conducted by independent security experts to ensure that they are comprehensive and objective.

In modern information technology and cybersecurity management, various framework models and methodologies are widely used. One of the best known is ITIL (Information Technology Infrastructure Library), which offers practices for managing IT services, improving service quality and user satisfaction [29]. In parallel to ITIL, COBIT (Control Objectives for Information and Related Technologies) provides a structured approach to IT resource management, ensuring control and compliance with organizational goals [30].

In the context of cybersecurity, an important resource is NIST (National Institute of Standards and Technology), which develops standards and guidelines to help improve the security of information systems [31]. In particular, CPG13 (Commonly Accepted Security Practices for Software Development) emphasizes best security practices in software development, allowing the integration of security measures at all stages of the product lifecycle [32]. In addition, the MITRE organization plays a key role in cyber threat analysis by offering tools such as the ATTACK database, which helps security professionals better understand and respond to potential attacks [33]. The STIX (Structured Threat Information Expression) format is used to share cyber threat information, which facilitates communication between organizations and improves collective security [34]. Thus, the use of these models and techniques in information technology and cybersecurity management allows organizations to respond to threats more effectively and protect their resources.

Based on the results of the study of existing testing methods, a methodology based on a standard for performing penetration testing was developed. Figure 6 shows a diagram of the methodology of comprehensive testing for identifying vulnerabilities in the wireless network in the smart city ecosystem, which consists of six stages that are performed one after another: Pre-Engagement Interactions, Reconnaissance, Vulnerability Identification, Exploitation, Post Exploitation, Reporting.

The methodology consists of six distinct stages, as shown in Figure 7, each designed to comprehensively test and uncover potential vulnerabilities in the system. These stages are executed sequentially to ensure a thorough analysis of the target network.

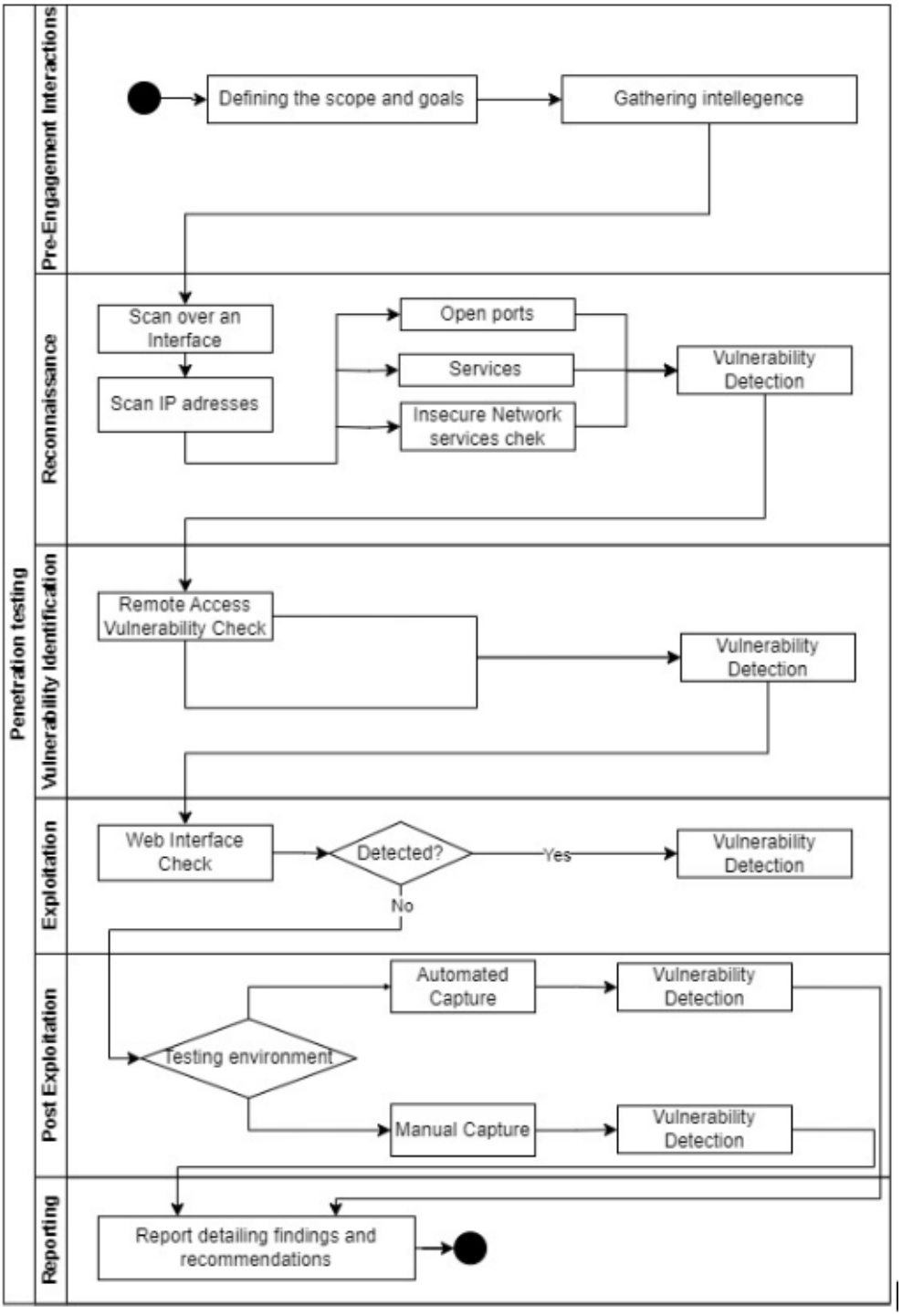


Figure 6 – UML Diagram of the Methodology of Complex testing for Vulnerability Detection

The stages of the proposed methodology represent subprocesses aimed at identifying vulnerabilities in the system. First of all, stage defines the scope, purpose, and boundaries of the testing process and identifies key elements such as network configurations, system endpoints, and sensitive assets. Next, the interactions between the tester and the client (e.g. city authorities or network administrator)

are established. The current stage promotes a deep understanding of the infrastructure and systems that are planned to be tested and is essential to ensure the focus and effectiveness of the penetration test.The next step in the methodology involves collecting information about the target system. This information includes identifying network components, devices, and potential entry points for an attacker. Tools such as Nmap and Wireshark are employed to scan the network for open ports, active devices, and services running on the network. The goal is to create a detailed map of the system's architecture and discover any unprotected or misconfigured components that could be exploited. Function pseudo-code for determining open ports shown in Figure 7.

```
def port_scan(ip, port_range):
    open_ports = []
    for port in range(port_range[0], port_range[1] + 1):
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
            result = sock.connect_ex((ip, port))
            if result == 0:
                open_ports.append(port)
    return open_ports
```

Figure 7 – Part of pseudo-code for determining open ports

If the goal of the previous two stages was to collect information, afterwards the next stage focuses on identifying potential vulnerabilities in the target system. Identifying potential vulnerabilities includes assessing the security status of network services in the form of checking for unpatched software, testing weak encryption protocols, and identifying insecure remote access mechanisms. Thus, ARP analysis is used to detect potential vulnerabilities of man-in-the-middle (MITM) attacks, the pseudocode for which is given below. If the system contains web applications, at this stage they are also checked for common vulnerabilities such as SQL injection and cross-site scripting (Figure 9).

```
def arp_sniff(interface):
    def arp_display(packet):
        if packet[ARP].op == 1:  # ARP request
            print(f"ARP Request: {packet[ARP].psrc} is asking about {packet[ARP].pdst}")
        elif packet[ARP].op == 2:  # ARP response
            print(f"ARP Response: {packet[ARP].psrc} has address {packet[ARP].pdst}")

    sniff(iface=interface, prn=arp_display, filter="arp", store=0)
```

Figure 8 – Part of pseudo-code for detect potential vulnerabilities

Then, once potential vulnerabilities have been identified, the next step is to attempt to exploit these vulnerabilities to gain unauthorized access or control. The attempts mimic real-world cyber-attacks where attackers exploit weaknesses in network security. The outcome of these attempts, in the form of success or failure, provides critical information about the severity of the vulnerabilities and the potential risks to the smart city infrastructure. If successful in the previous stage, further compromise of the system occurs and further information gathering continues. If successful in exploitation, the tester moves on to the post-exploitation stage, where the focus is on gaining deeper

access to the system and gathering additional information that can further compromise the network. This may include accessing sensitive data, installing backdoors, or manipulating network settings to maintain long-term access. The actions taken after exploitation are essential to understanding the potential damage that an attacker can cause after breaching the system. After all stages, a penetration testing report is generated, which is the final stage of the proposed methodology. The report provides an extensive list of vulnerabilities identified, the methods used to exploit them, and the potential impact on the smart city wireless network.

The proposed methodology will help various organizations involved in the digitalization of the city ecosystem to identify and eliminate vulnerabilities, improving the security of their systems before they can be exploited by attackers. Figure 10 provides a visualization of the Smart City model, presented in the form of interrelated methods, approaches, and various frameworks that contribute to improving security in general. All the elements presented in the figure are related to ensuring the safety and effective functioning of smart cities.

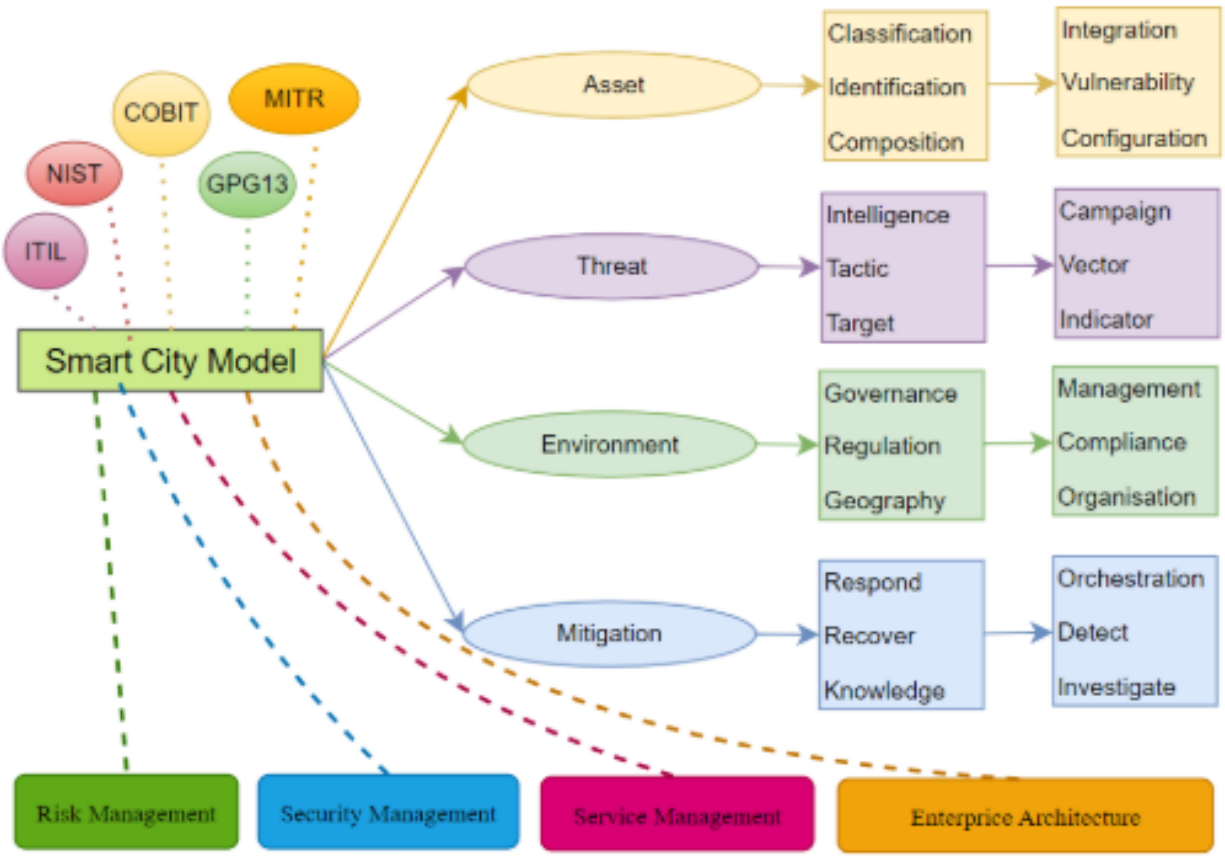


Figure 9 – Smart City Model

This diagram is a useful tool for understanding the interrelationships between different aspects of information security in the context of smart cities. It can be used to develop security strategies, evaluate existing systems and improve risk management processes.

5. Discussion

Research publications in the direction of security in smart cities were reviewed. Figure 6 shows a three-field diagram with Source in the center, country and keywords on the left and right sides respectively. The diagram shows the links of countries with sources and keywords. The height of the rectangles is proportional to the frequency of occurrence of a particular country, source or keyword in the network. The width of the lines between the nodes is proportional to the number of links.

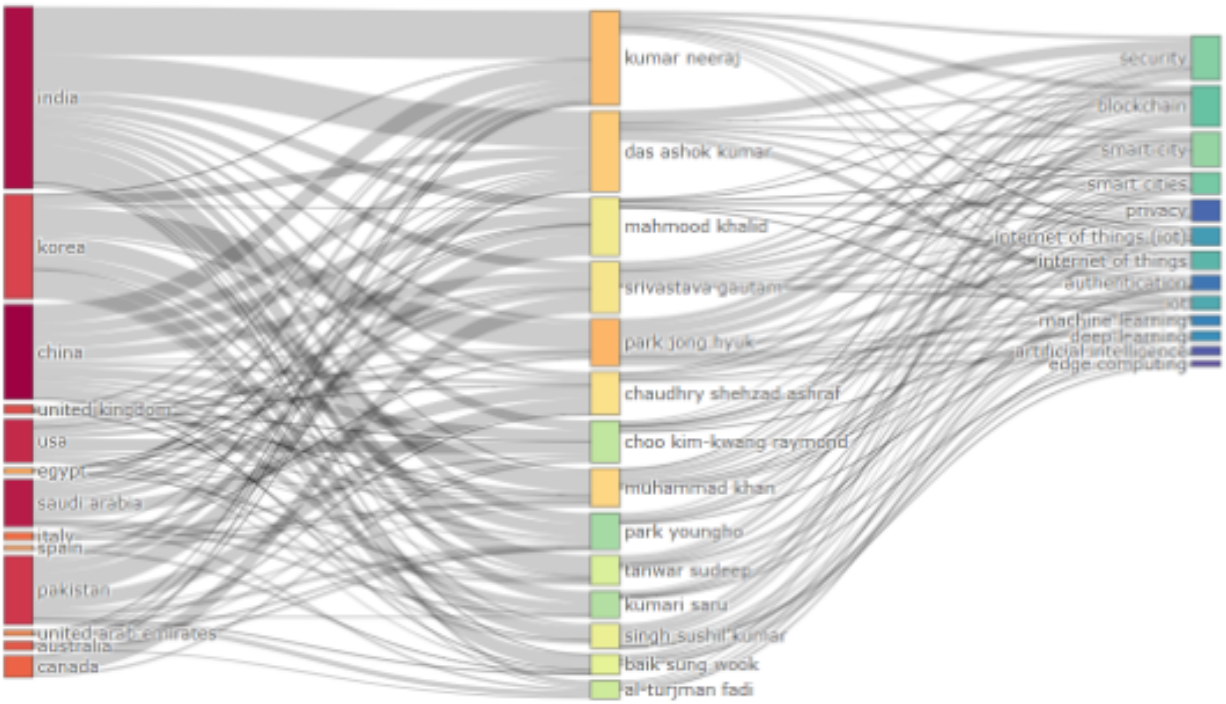


Figure 10 – Smart City Model

Overall, the visualization shows how certain countries and authors are driving the research agenda in smart cities and related technologies. It also underscores the global nature of this research, with significant contributions from both developed and developing countries. The focus on key areas such as security, blockchain, IoT, and machine learning suggests that these technologies will continue to be central to the development of future smart city systems.

The study and analysis of scientific advances towards security identified open questions that could be the basis for future research efforts, such as:

- Research could focus on creating systems that automatically adapt to new threats and attacks in real time using machine learning and artificial intelligence;
- There is a need to explore how new technologies such as 5G, blockchain, and quantum computing could change approaches to security in smart cities;
- Explore methods to make smart cities more resilient to cyber threats, including creating incident response and attack recovery plans;
- Exploring effective methods to increase user awareness and educate employees on cybersecurity in the context of smart cities;
- Integrate knowledge from different fields, such as social sciences and psychology, to better understand user behavior and responses to cyber threats.

The listed future research directions can significantly contribute to strengthening the security and resilience of smart city ecosystems, which is critical to protect citizens and infrastructure in the face of persistent cyber threats. As the global demand for smarter, more secure cities grows, the findings from this visualization highlight both the progress being made and the areas where further research and collaboration are needed to ensure that smart city technologies can be implemented safely and efficiently across diverse urban environments.

6. Conclusion

Smart cities represent an attractive target for cybercriminals due to the large number of connected devices, extensive networks and the storage of significant amounts of data. To ensure the security of smart cities, comprehensive measures must be taken, including regular software updates, staff

training, the use of multi-factor authentication, network segmentation and the implementation of intrusion detection and prevention systems.

This paper analyzes research publications on the direction of security in the smart city ecosystem. Cybersecurity challenges have been identified and cases of perfect attacks on smart cities have been reviewed. After a thorough review and analysis, and considering the scope of the study, a comprehensive testing methodology was developed to identify vulnerabilities in the wireless network. A visualization of the smart city model was also presented and directions for future research in the context of security in the smart city ecosystem were given.

The study presents a novel penetration testing methodology tailored for wireless networks in smart cities, particularly within the context of Kazakhstan. Our findings indicate that smart cities are increasingly vulnerable to various forms of cyberattacks, particularly in their wireless networks. The proposed methodology addresses this vulnerability by providing a structured, multi-phase approach that enhances the identification and mitigation of potential security breaches.

In conclusion, this study contributes significantly to the field of smart city cybersecurity by providing a tailored penetration testing methodology that addresses the unique challenges of securing wireless networks in urban environments. The methodology not only enhances the security posture of smart city infrastructures in Kazakhstan but also offers valuable insights for other regions facing similar challenges.

Authors' contribution

Zhukabayeva T.K. - Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, software, supervision, validation, visualization, Writing - original draft, Writing - review and editing.

Adamova A.D. - Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Resources, software, validation, visualization, Writing - original draft, Writing - review and editing.

Karabayeva N.Y. - Investigation, Methodology, Resources, software, visualization.

Desnitsky V.A. - Conceptualization, Data curation, Resources, Formal analysis, Methodology, Resources, validation, visualization.

Glazyrina N.S. - Data curation, Formal analysis, Resources, validation, visualization.

References

1 Global Smart City Report 2024 by Research and Markets [Electronic resource]. -URL: https://www. globenewswire.com/en/search/organization/Research%2520and%2520Markets (Accessed: 19.11.2024).
2 Kim, J. (2022). Smart city trends: A focus on 5 countries and 15 companies. Cities, 123, 103551.
3 Public services and online information [Electronic resource]. -URL: https://egov.kz/cms/kk (Accessed: 18.11.2024).
4 UN E-Government Survey 2024 [Electronic resource]. -URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024 (Accessed: 18.11.2024).
5 CNN US [Electronic resource]. -URL: https://edition.cnn.com/2023/11/28/us/pennsylvania-water-cyberattack/index.html (Accessed: 18.11.2024).
6 LeMagIT [Electronic resource]. -URL: https://www.lemagit.fr/actualites/366543032/Olsztyn-Pologne-premiere-Smart-City-touchee-par-une-cyberattaque (Accessed: 20.11.2024).
7 The TechCrunch news [Electronic resource]. -URL: https://techcrunch.com (Accessed: 19.11.2024).
8 Overview of cyberattacks on connected cities [Electronic resource]. -URL: https://www.stormshield.com/news/overview-of-cyberattacks-on-connected-cities (Accessed: 20.11.2024).
9 Houichi M., Jaidi F., Bouhoula A. Analysis of Smart Cities Security: Challenges and Advancements //2022 15th International Conference on Security of Information and Networks (SIN). – IEEE, 2022. – P. 01-05. doi: 10.1109/SIN56466.2022.9970494
10 Adamova A., Zhukabayeva T. Development of a methodology for data normalization and aggregation to enhance security levels in internet of things interactions// Scientific Journal of Astana IT University. -2024. -Vol. 19. -P. 16–27. doi: https://doi.org/10.37943/19UQOC7381
11 Amaizu G.C., Lee J.M., Kim D.S. Machine Learning Based Security for Smart Cities //2022 27th Asia Pacific Conference on Communications (APCC). – IEEE, 2022. – P. 572-573. doi: 10.3390/fi1509028
12 Maseleno A. et al. An Intelligent Intrusion Detection for Smart Cities Application Based on Random Optimization with Recurrent Network // Artificial Intelligence Applications for Smart Societies: Recent Advances. – Cham: Springer International Publishing, 2021. – P. 119-133. -URL: https://doi.org/10.1007/978-3-030-63068-3-8.

13 Alhowaide A., Alsmadi I., Alsinglawi B. Ensemble-based Cyber Intrusion Detection for Robust Smart City Protection // 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). – IEEE, 2024. – P. 124-129. -URL: https://doi.org/10.1109/dcoss-iot61029.2024.00027.
14 Sirigineedi M. et al. Enhanced Security in Smart City GAN-Based Intrusion Detection Systems in WSNs // In: Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs). – IGI Global, 2024. – P. 162-176.
15 Rakha M. A. et al. A Detailed Comparative Study of AI-Based Intrusion Detection System for Smart Cities //2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE). – IEEE, 2024. – P. 1783-1790. doi: 10.1109/ic3se62002.2024.10593485
16 Akhilesh R. et al. Automated penetration testing framework for smart-home-based IoT devices //Future Internet. – 2022. – Vol. 14. – №. 10. – P. 276. doi: 10.3390/fi14100276
17 Kim K. et al. Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey //Sensors. – 2023. – Vol. 23. – №. 7. – P. 3681. doi: 10.3390/s23073681
18 Al-Taleb N. et al. Cyber threat intelligence for secure smart city //arXiv preprint arXiv:2007.13233. – 2020. doi: 10.48550/arXiv.2007.13233
19 Mijwil M. M. et al. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects //Mesopotamian journal of cybersecurity. – 2022. – Vol. 2022. – C. 1-4.
20 Baig Z.A. et al. Future challenges for smart cities: Cyber-security and digital forensics //Digital Investigation. – 2017. – Vol. 22. – P. 3-13.
21 Li C. et al. Securing SDN infrastructure of IoT–fog networks from MitM attacks //IEEE Internet of Things Journal. – 2017. – Vol. 4. – №. 5. – P. 1156-1164.
22 Hamid B. et al. Cyber security issues and challenges for smart cities: A survey //2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). – IEEE, 2019. – P. 1-7.
23 Toh C. K. Security for smart cities. IET Smart Cities. – 2020. 2(2), -P. 95–104.
24 Chen W. et al. A DDoS attacks traceback scheme for SDN-based smart city //Computers & Electrical Engineering. – 2020. – Vol. 81. – P. 106503.
25 Telo J. Smart city security threats and countermeasures in the context of emerging technologies //International Journal of Intelligent Automation and Computing. – 2023. – Vol. 6. – №. 1. – P. 31-45.
26 Kitchin R., Dodge M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention //Smart cities and innovative Urban technologies. – Routledge, 2020. – P. 47-65.
27 Lupton B. et al. Analysis and prevention of security vulnerabilities in a smart city //2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). – IEEE, 2022. – P. 0702-0708..
28 Cui L. et al. Security and privacy in smart cities: Challenges and opportunities //IEEE access. – 2018. – Vol. 6. – P. 46134-46145.
29 Batmetan J. R. et al. IT Infrastructure Library Framework Approach to the Measurement of e-Government Maturity //International Journal of Information Technology and Education. – 2022. – Vol. 1. – №. 2. – P. 119-128.
30 de Santana E. S. et al. SMM: a maturity model of smart cities based on sustainability indicators of the ISO 37122 //International Journal of Advanced Engineering Research and Science. – 2019. – Vol. 6. – №. 2. – P. 13-20.
31 NIST [Electronic resource]. -URL: https://www.nist.gov/.
32 Cai W. et al. A software vulnerability detection method based on deep learning with complex network analysis and subgraph partition //Information and Software Technology. – 2023. – Vol. 164. – P. 107328.
33 Naik N. et al. Comparing attack models for it systems: Lockheed martin's cyber kill chain, mitre attack framework and diamond model //2022 IEEE International Symposium on Systems Engineering (ISSE). – IEEE, 2022. – P. 1-7.
34 Bromander S. et al. Examining the" Known Truths" in Cyber Threat Intelligence–The Case of STIX //International Conference on Cyber Warfare and Security. – Academic Conferences International Limited, 2020. – P. 493-XII.

Қазақстандағы ақылды қалалардың қауіпсіздігін арттыру мақсатында сымсыз желілерге ену жолдары әдістемесін әзірлеу

Т. К. Жукабаева [1], А. Д. Адамова [2*], Н.Е. Карабаев [3], В.А. Десницкий [4], Н.С. Глазырина [5]

[1,2,3,5] Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаев көш., 2, Астана, 010008, Қазақстан

[4] Ресей ғылым академиясының Санкт-Петербург Федералды зерттеу орталығы, 14-ші жол В.А., № 39, Санкт-Петербург, 199178, Ресей

Аңдатпа. Қазіргі заманғы қалалар ақпараттық технологияларды көбірек енгізіп, "ақылды" болып келеді. Технологиялық даму мен кибершабуылдардың әлеуеті де артып келе жатқанын атап өткен жөн. Бұл жұмыста Қазақстанның ақылды қалаларындағы сымсыз желілердің киберқауіпсіздігінің маңызды мәселесі қарастырылады. Зерттеу сымсыз желілердегі осалдықтарды анықтау және оларды жою үшін жолдарын тестілеудің кешенді әдісін ұсынады. Бұл тәсіл ақылды қаланың экожүйесіндегі қауіпсіздікке ықпал ететін және Қазақстанның қалалық инфрақұрылымды қорғау жөніндегі ортақ күш-жігерін қолдайтын стратегияны қамтиды. Ақылды қала инфрақұрылымының негізгі элементі болып табылатын сымсыз желілердің осалдығына ерекше назар аударылады. Бұл жұмыста ақылды қалалардың сымсыз желілеріндегі осалдықтарды анықтауға бағытталған ену жолдарын тестілеудің кешенді тәсілі ұсынылады. Бұл тәсіл мақсатты жүйе туралы ақпаратты жинаудан бастап анықталған осалдықтар туралы есепке дейінгі әртүрлі кезеңдерді қамтиды. Зерттеу нәтижелері Қазақстанның ақылды қалаларында киберқауіпсіздікті арттыруға және кибершабуылдардан қорғаудың тиімді стратегияларын әзірлеуге ықпалын тигізеді.

Түйін сөздер: ену сынағы, ақылды қала, киберқауіпсіздік, заттар интернеті, осалдылық, деректер қауіпсіздігі, ақпараттық қауіпсіздік, Қазақстан.

Разработка методики тестирования на проникновение в беспроводных сетях для повышения безопасности умного города в Казахстане

Т. К. Жукабаева [1], А. Д. Адамова [2*], Н.Е. Карабаев [3], В.А. Десницкий [4], Н.С. Глазырина [5]

[1,2,3,5] Евразийский национальный университет им. Л. Н. Гумилева, ул. Сатпаева, 2, Астана, 010008, Казахстан

[4] Санкт-Петербургский Федеральный исследовательский центр РАН, 14-я линия В.О., д.39 Санкт-Петербург, 199178, Россия

Аннотация. Современные города все больше внедряют информационные технологии и становятся «умными». Важно отметить, что с развитием технологий увеличивается и потенциал для кибератак. В данной работе рассматривается значимая проблема кибербезопасности беспроводных сетей в умных городах Казахстана. В исследовании предлагается комплексный подход к тестированию на проникновение для выявления и устранения уязвимостей в беспроводных сетях. Этот подход включает стратегию, которая способствует безопасности в экосистеме умного города и поддерживает общие усилия Казахстана по защите городской инфраструктуры. Особое внимание уделяется уязвимостям беспроводных сетей, которые являются ключевым элементом инфраструктуры умных городов. В данной работе предлагается комплексный подход к тестированию на проникновение, направленный на выявление уязвимостей в беспроводных сетях умных городов. Этот подход включает различные этапы, начиная со сбора информации о целевой системе и заканчивая подробным отчетом о выявленных уязвимостях. Результаты исследования могут способствовать повышению кибербезопасности в умных городах Казахстана и разработке эффективных стратегий защиты от кибератак.

Ключевые слова: тест на проникновение, умный город, кибербезопасность, интернет вещей, уязвимость, безопасность данных, информационная безопасность, Казахстан.

References

1 Global Smart City Report 2024 by Research and Markets [Electronic resource]. Available at: https://www. globenewswire.com/en/search/organization/Research%2520and%2520Markets (Accessed: 19.11.2024).

2 Kim J. Smart city trends: A focus on 5 countries and 15 companies. Cities. 2022. Vol. 123, 103551.

3 Public services and online information [Electronic resource]. Available at: https://egov.kz/cms/kk (Accessed: 18.11.2024).

4 UN E-Government Survey 2024 [Electronic resource]. Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024 (Accessed: 18.11.2024).
5 CNN US [Electronic resource]. Available at: https://edition.cnn.com/2023/11/28/us/pennsylvania-water-cyberattack/index.html (Accessed: 18.11.2024).
6 LeMagIT [Electronic resource]. Available at: https://www.lemagit.fr/actualites/366543032/Olsztyn-Pologne-premiere-Smart-City-touchee-par-une-cyberattaque (Accessed: 20.11.2024).
7 The TechCrunch news [Electronic resource]. Available at: https://techcrunch.com (Accessed: 19.11.2024).
8 Overview of cyberattacks on connected cities [Electronic resource]. Available at: https://www.stormshield.com/news/overview-of-cyberattacks-on-connected-cities (Accessed: 20.11.2024).
9 Houichi M., Jaidi F., Bouhoula A. Analysis of Smart Cities Security: Challenges and Advancements, 2022 15th International Conference on Security of Information and Networks (SIN). IEEE, 2022. P. 01-05. doi: 10.1109/SIN56466.2022.9970494
10 Adamova A., Zhukabayeva T. Development of a methodology for data normalization and aggregation to enhance security levels in internet of things interactions, Scientific Journal of Astana IT University. -2024. -Vol. 19. -P. 16–27. doi: https://doi.org/10.37943/19UQOC7381
11 Amaizu G.C., Lee J.M., Kim D.S. Machine Learning Based Security for Smart Cities, 2022 27th Asia Pacific Conference on Communications (APCC). IEEE, 2022. P. 572-573. doi: 10.3390/fi1509028
12 Maseleno A. et al. An Intelligent Intrusion Detection for Smart Cities Application Based on Random Optimization with Recurrent Network // Artificial Intelligence Applications for Smart Societies: Recent Advances. – Cham: Springer International Publishing, 2021. – P. 119-133. -URL: https://doi.org/10.1007/978-3-030-63068-3-8.
13 Alhowaide A., Alsmadi I., Alsinglawi B. Ensemble-based Cyber Intrusion Detection for Robust Smart City Protection // 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). – IEEE, 2024. – P. 124-129. -URL: https://doi.org/10.1109/dcoss-iot61029.2024.00027.
14 Sirigineedi M. et al. Enhanced Security in Smart City GAN-Based Intrusion Detection Systems in WSNs, In: Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs). IGI Global, 2024. P. 162-176.
15 Rakha M.A. et al. A Detailed Comparative Study of AI-Based Intrusion Detection System for Smart Cities //2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE). IEEE, 2024. P. 1783-1790. doi: 10.1109/ic3se62002.2024.10593485
16 Akhilesh R. et al. Automated penetration testing framework for smart-home-based IoT devices, Future Internet. 2022. Vol. 14. №10. P. 276. doi: 10.3390/fi14100276
17 Kim K. et al. Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey, Sensors. 2023. Vol. 23. №7. P. 3681. doi: 10.3390/s23073681
18 Al-Taleb N. et al. Cyber threat intelligence for secure smart city, arXiv preprint arXiv:2007.13233. 2020. doi: 10.48550/arXiv.2007.13233
19 Mijwil M. M. et al. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects, Mesopotamian journal of cybersecurity. 2022. Vol. 2022. P. 1-4.
20 Baig Z.A. et al. Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation. 2017. Vol. 22. P. 3-13.
21 Li C. et al. Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet of Things Journal. 2017. Vol. 4. №5. P. 1156-1164.
22 Hamid B. et al. Cyber security issues and challenges for smart cities: A survey, 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). IEEE, 2019. P. 1-7.
23 Toh C.K. Security for smart cities. IET Smart Cities. 2020. 2 (2). P. 95–104.
24 Chen W. et al. A DDoS attacks traceback scheme for SDN-based smart city, Computers & Electrical Engineering. 2020. Vol. 81. P. 106503.
25 Telo J. Smart city security threats and countermeasures in the context of emerging technologies, International Journal of Intelligent Automation and Computing. 2023. Vol. 6. №1. P. 31-45.
26 Kitchin R., Dodge M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention, Smart cities and innovative Urban technologies. Routledge, 2020. P. 47-65.
27 Lupton B. et al. Analysis and prevention of security vulnerabilities in a smart city, 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022. P. 0702-0708.
28 Cui L. et al. Security and privacy in smart cities: Challenges and opportunities, IEEE access. – 2018. Vol. 6. P. 46134-46145.
29 Batmetan J. R. et al. IT Infrastructure Library Framework Approach to the Measurement of e-Government Maturity, International Journal of Information Technology and Education. 2022. Vol. 1. №2. P. 119-128.
30 de Santana E. S. et al. SMM: a maturity model of smart cities based on sustainability indicators of the ISO 37122 //International Journal of Advanced Engineering Research and Science. 2019. Vol. 6. №2. P. 13-20.
31 NIST [Electronic resource]. Available at: https://www.nist.gov/.
32 Cai W. et al. A software vulnerability detection method based on deep learning with complex network analysis and subgraph partition, Information and Software Technology. 2023. Vol. 164. P. 107328.

33 Naik N. et al. Comparing attack models for it systems: Lockheed martin's cyber kill chain, mitre attack framework and diamond model, 2022 IEEE International Symposium on Systems Engineering (ISSE). IEEE, 2022. P. 1-7.
34 Bromander S. et al. Examining the" Known Truths" in Cyber Threat Intelligence–The Case of STIX, International Conference on Cyber Warfare and Security. – Academic Conferences International Limited, 2020. P. 493-XII.

Авторлар туралы мәлімет:

Жукабаева Тамара Кокеновна - PhD, Профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаев көш., 2, Астана қ., 010008, Қазақстан. zhukabayeva_tk@enu.kz.

Адамова Айгуль Дюсенбиновна - *байланыс үшін автор*, PhD, Жетекші ғылыми маман, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаев көш., 2, Астана қ., 010008, Қазақстан. aigul.dyusenbinovna@gmail.com.

Карабаев Нурдаулет Ерланович - Докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаев көш., 2, Астана қ., 010008, Қазақстан. 020419501012@enu.kz.

Десницкий Василий Алексеевич - техника ғылымдарының кандидаты, доцент, Ресей ғылым академиясының Санкт-Петербург Федералды зерттеу орталығы, 14-ші жол В.А., № 39, Санкт-Петербург, 199178, Ресей. desnitsky@comsec.spb.ru.

Глазырина Наталья Сергеевна - PhD, қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтбаев көш., 2, Астана қ., 010008, Қазақстан. glazyrina_ns_1@enu.kz.

Zhukabayeva Tamara Kokenovna - PhD, Professor, L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan. zhukabayeva_tk@enu.kz.

Adamova Aigul Dyusenbinovna - *corresponding author,* PhD, Leading Researcher, L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan. aigul.dyusenbinovna@gmail.com.

Karabayev Nurdaulet Erlanovich - PhD Student, L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 010008, Kazakhstan. 020419501012@enu.kz.

Desnitsky Vasily Alekseevich - St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14th line V.O., no. 39, St. Petersburg, 199178, Russia. desnitsky@comsec.spb.ru.

Glazyrina Natalya Sergeevna - PhD, Associate Professor, L.N. Gumilyov Eurasian National University, Satpayev str., 2, Astana, 199178, Kazakhstan. glazyrina_ns_1@enu.kz.

Received: 19.11.2024. Revised: 25.11.2024.
Approved: 01.12.2024. Available online: 30.12.2024.