PROTECTING AIRPORT SYSTEMS FROM CYBER INCIDENTS

B.A.Allaberganov
Chief specialist of the Digital Development Department of the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan
D.Sh.Abdullayev
Master's degree, Faculty of Cyber-Security,Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Abstract. *Airports are one of the institutions that can pose a threat to cyber attacks. Aviation is a rapidly developing and growing industry in the world. It plays an important role in increasing the socio-economic welfare of countries. Countries that closely follow the aviation industry are investing in developing their aviation industries. The development of airports and their transformation into smart airports, the use of the internet of things (IoT) in almost every part of the airport, has led to an increase in the gaps that make it easier for hackers to hack airports and access passenger information. In this study, first of all, cyber incidents in smart airports will be discussed. Then, the most vulnerable vulnerabilities of the systems in airports against hacking were determined by examining the studies and cyber security incidents in previous years. As a result of this research, the most common cyber attacks in smart airports were determined. In addition, the most commonly used intrusion prevention methods to protect smart airports against cyber attacks are discussed.*

Keywords. *Internet of Things (IoT), Smart Airport, Cyber Security*

Introduction. With the recent developments in science and the entry of technology into human life, things have become easier for humanity, so it has become easy to control devices from a distance, but this development and technology has created loopholes in the system, which made it easier for hackers and hackers to penetrate the systems of major companies and obtain their information by sending programs that penetrate existing vulnerabilities, extract files from them, or cause system disruptions. Therefore, it has become necessary for companies that deal with technology www.scienceuzbekistan.org Page 147 Proceedings Book TASHKENT 2 st-International Congress on Modern Sciences Tashkent Chemical-Technological Institute December 16-17, 2022 directly to take care of providing security for companies' systems. The method of keeping information away from hackers is called cybersecurity. Computer security or cybersecurity is a branch of technology known as information security, as applied to computers and networks. The goal of computer security includes protecting information and property from theft, corruption, or natural disasters while allowing information and property to remain productive and accessible to its intended users. Computer system security terminology means the collective processes and mechanisms by which sensitive and valuable information and services are protected from dissemination, tampering, or collapse caused by unauthorized activities or untrustworthy personnel, and unplanned events respectivele. In this study will

be discussing the vulnerabilities and cyber-attacks that can be possible in airports. In the end, we will share some advice about how can be avoided or decreased the cyber-attacks on smart airports

Materials. Airports are one of the institutions that are highly vulnerable to attack by hackers, due to the large gaps in them due to their complete dependence on technology. An attack at an airport may be as simple as it can lead to major disasters. A power outage at the airport alone can cause repercussions all over the world. One of the easiest, and arguably, most difficult ways to track security holes can be achieved by sending unauthorized messages over specific radio frequencies. This transmission may spoof air traffic controllers, or simply disrupt communications entirely.

Methods. The operations were carried out by the professional hacker "Chris Robert" electronically on dozens of flights, was arrested by the US authorities in April 2015, after his "tweet" he published explaining the steps of hacking the "United Airlines" plane, which he was traveling on to New York. In the investigations conducted by the FBI, "Chris" admitted the truth of what he had committed, and gave a full explanation of the process of hacking aircraft through "Ethernet"; It is a technology that has been adopted as the basis for the implementation of messaging operations in many local networks.

Results. Explaining the Steps of Hacking the "United Airlines" Plane by Chris Robert, 2015The operations were carried out by the professional hacker "Chris Robert" electronically on dozens of flights, was arrested by the US authorities in April 2015, after his "tweet" he published explaining the steps of hacking the "United Airlines" plane, which he was traveling on to New York. In the investigations conducted by the FBI, "Chris" admitted the truth of what he had committed, and gave a full explanation of the process of hacking aircraft through "Ethernet"; It is a technology that has been adopted as the basis for the implementation of messaging operations in many local networks.

Somali Daaloo Airline Cyber Attak by Al-Shabab, 2016 - with 74 passengers on board, 15 minutes after the plane took off from the capital Mogadishu. It caused a hole in its chassis and killed the bomber.

Six Saudi Facilities cyber Attack, 2016 www.scienceuzbekistan.org Page 149 Proceedings Book TASHKENT 2 st-International Congress on Modern Sciences Tashkent Chemical-Technological Institute December 16-17, 2022 In November 2016, six Saudi facilities were subjected to hacker attacks, led by the General Authority of Civil Aviation, which regulates Saudi air traffic. The cyberattacks targeted the disruption of servers and devices in these facilities to affect the services provided and attemptedto seize the data of computer systems and implant malicious software.

Cathay Pacific Airways 9.4M Breached Records, 2018 This incident is probably the most serious data breach in airline history to date. The attack affected 9.4 million Cathay Pacific passengers. In March 2018, the IT team detected suspicious an ongoing IT operation had revealed unauthorized access to systems. According to the Informa connected to the internet, and malware was installed to access the data. The regulator also added files that were not password protected, unpatched Internet-facing servers, use of operating systems that were no longer supported by the developer, and inadequate antivirus protection. Later,

Cathay Pacific said it knew the suspicious activity in March was a full-scale attack on its 2018 but continued after that. The stolen data included passport details, birth dates, frequent flier numbers, phone numbers, and credit card information. In September 2018, Cathay Pacific began rolling out multi-factor authentication (MFA) across all users, to counter the sophistication and increase in cyberattacks in the aviation industry. The seriousness of this cyberattack can be explained by its very nature: the number of people affected, the enormous amount of investigative work it required, and the lengthy process of identifying the stolen data.

British Airways 400K Breached Records, 2018 British Airways admitted that the personal data of 429,612 customers and staff was stolen from its site over 15 days from August 21st to September 5th, 2018. This included names, addresses, payment card numbers, and CVV numbers of 244,000 BA customers. At first glance, the infection method was nothing new as it was simply a hacked version of the Modernizr JavaScript library, infected with a malicious code called Magecart. This method is typical in cyberattacks involving banking data. On closer inspection, it turns out this may not be a classicattack. processing a significant amount of personal data without adequate security measures in place to protect the personal and financial details of more than 400,000 of its customers.

Conclusion. This article aims to study the security vulnerabilities in smart airports, where the security vulnerabilities in and from airports have been identified Automated Check-In, E-Gates, Luggage Tracking and Handling, Physical Airport Security, Janitorial Optimization, Runway Structural Integrity Monitoring, Smart Lighting, Airport Asset Tracking, Air Quality, and Environmental Conditions Tracking, Thermal Cameras at Smart Airports provide a detailed explanation of the electronic attacks facing smart airports, and clarify the protocols of electronic devices connected to the Internet of Things, which is a vector between security vulnerabilities. Cyber-attacks, and finally have to take a set of measures to be taken into consideration to avoid or reduce cyber-attacks on smart airports. The researcher can always find and introduce new topics in the field. For example, a researcher can submit a questionnaire to smart airports, conduct statistics about electronic devices used in airports, analyze the device and see if it constitutes a security gap or not. Thus, it has discovered a new vulnerability that must be taken into account. The researcher can also provide a detailed explanation of the SCADA system, study its weaknesses, and strive to develop and strengthen them. The more powerful the SCADA system, the less vulnerable it is to cyberattack. In the end, the cyberattacks that occur at electronic airports in light of the Corona pandemic were reached, as the US Federal Aviation Administration (FAA) issued a report on the situation highlighting that aviation employees tters related to COVIDemails can be difficult to detect due to the efforts of cybercriminals to ensure that they appear legitimate. This is also a security vulnerability in smart airports that can be addressed in the future.

REFERENCES:

1. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8.Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian.
2. Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4.
3. Gopalakrishnan, K.; Govindarasu, M.; Jacobson, D.W.; Phares, B.M. Cyber security for airports. Int. J. Traffic Transp. Eng. 2013, 3, 365 376.
4. Optim, https://en.optim.cloud/industries/airport/, accessed 19.11.2022.
5. Ain, https://www.google.com/amp/s/al-ain.com/amp/article/terrorism-cyber-security,accessed 29.11.2022.