DOI 10.53364/24138614_2022_25_2_24
UDC 528.71:004.512.4

Zhanzak G.S., Master's student
Scientific supervisor: **Koshekov K.T.**
Academy of Civil Aviation, Almaty

[1]*E-mail: gaziz1094@gmail.com*
[2]*E-mail: kkoshekov@mail.ru*

CYBERSECURITY OF UNMANNED AERIAL VEHICLES

КИБЕРБЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫНЫҢ КИБЕРҚАУІПСІЗДІГІ

Abstract: The threat of cyberattacks today is one of the main problems in the activities of modern aviation. This article will consider common methods of hacking unmanned aerial vehicles as well as regulatory legal acts on the cyber protection of UAVs.
Keywords: UAV, cyber threat, GPS-spoofing, malware, traffic interception.

Аннотация: Угрозы кибератак на сегодняшний день является одним из основных проблем в деятельности современной авиации. В данной статье будет рассмотрено распространенные методы взлома беспилотных летательных аппаратов а так нормативно правовые акты по кибер-защите БПЛА.
Ключевые слова: БПЛА, киберугроза, GPS-spoofing, вредоносное ПО, перехват траффика.

Аннотация. Бүгінгі күні кибершабуылдардың қаупі қазіргі авиация қызметіндегі негізгі проблемалардың бірі болып табылады. Бұл мақалада ұшқышсыз ұшу аппараттарын бұзудың кең таралған әдістері, сондай-ақ ҰҰА-тарын кибер-қорғау жөніндегі нормативтік құқықтық актілер қарастырылатын болады.
Түйін сөздер: ҰҰА, киберқауіптер, GPS-spoofing, зиянды БҚ, траффикті ұстап алу.

Introduction. The International Civil Aviation Organization (ICAO) defines an unmanned aerial vehicle as described in the Global Operational Concept of Air Traffic Control (Doc 9854) and approved by the 35th Session of the ICAO Assembly: An unmanned aerial vehicle is an unmanned aerial vehicle within the meaning of article 8 of the Convention on International Civil Aviation, which is operated without a pilot commander on board and either remotely and completely controlled from another place (earth, another plane, space), or programmed and completely autonomous.

Nowadays we are seeing a very large demand for unmanned vehicles. Whether it's an unmanned aerial vehicle or a land-based unmanned vehicle. But in this article we will consider unmanned aerial vehicles (UAVs). The range of use of such machines is very wide. In aviation, these drones are used for patrolling zones, reconnaissance from a bird's-eye view, as this gives a great overview, thereby increasing the received information. Can be used to deliver things, etc.

There are also military drones that are equipped with modern additional sensors such as a thermal imager and a night vision device, as well as weapons. Such aircraft attract with their autonomy and also in case of an emergency situation can not pose a danger to the pilot. In modern

wars, it is often unmanned aircraft that has begun to be used. As the facts show, unmanned aircraft has more positive results.

Like commercial aviation, unmanned aircraft is a target for intruders. Since there is no living person on board the UAV, the only way to harm the UAV is only through cyber attacks. The targets for intruders are different. Sabotage, terrorist attack after capture, interception for the purpose of theft of technological know-how of the UAV.

Real examples of UAV hacking:

• In 2009, in Iraq, Iraqi hackers hacked a Predator military UAV. For interception, unprotected communication channels with UAVs and special software that is freely available were used. Reason: After it was found out about the vulnerability of the data transmission channel from the UAV to the ground control center.

• In 2011, in Iran, Persian specialists intercepted GPS spoofing, imitation and substitution of GPS signals. It was reported about the successful interception of an American UAV of the RQ-170 Sentinel type due to the use of special electronics, which drowned out the signal of the GPS satellites and replaced it with its own. As a result, after completing tasks in offline mode, I started returning home. And since the location data was replaced, the drone landed at an Iranian airfield.

• 2012, Moscow, Vulnerability of the mobile offer. Introduction of malware.

List the main technical capabilities of the violator:

• influence on the electrical parameters of the signal in the data bus;

• creating overloads;

• sending destructive packets (data of the wrong format, which may cause the device to malfunction as part of the avionics);

• unauthorized use of undocumented device capabilities, prohibited commands (falsification of sender device addresses);

• substitution of navigation data;

• substitution of control information;

• violation of the integrity of the system.

The drones are controlled remotely. Their operators can be thousands of kilometers away in ground control points. The UAV is controlled via satellite or other wireless command and data transmission channel. In this regard, the following types of hacking of unmanned aerial vehicles are most often used.

1. Interference, introduction of malware

By broadcasting on the frequencies used by the drone, communication with its operator may be cut off. By silencing or intercepting the communication channel, you can interfere with the management of the UAV, including by introducing a malicious program. The communication channel can be encrypted, but often it is not.

2. Traffic interception

A more complex method is to use a satellite dish, a TV tuner and a skygrabber-type program to intercept the drone's frequencies. Both commands and data sent from the control point to the drone and going in the opposite direction can be intercepted.

3. Simulation and substitution of GPS signals

Portable GPS transmitters can send false signals and disrupt the drone's navigation system. This can be used to guide the drone along the trajectory on which it will crash, or even to intercept and land it.

Such GPS spoofing or an attack on GPS tries to deceive the GPS receiver of the UAV by broadcasting a signal more powerful than that received from GPS satellites in order to be similar to a number of normal GPS signals. These simulated signals are modified in such a way as to force the recipient to incorrectly determine their location, considering it to be what the attacker will send.

Conclusion. The main directions of countering cyber threats of avionics UAVs

In order to prevent incidents, it is necessary to carry out a complex of works, including:

• analysis and testing of information and control components of avionics in order to identify vulnerabilities and then classify them according to the degree of possible threats;

• development of a secure, trusted infocommunication infrastructure for specialized management systems;

• development of methods for finding vulnerabilities in the software of information management systems and avionics nodes;

• creation of a certification system and standard stands for special functional and load testing of software;

• improvement of the regulatory framework for information security in information management systems;

• development of means, individual for each UAV model, using blocking patterns to protect against attacks via the data bus and installing a hidden hardware bookmark on the bus, or reprogramming the standard control unit.

These and other measures will reduce the risk of cyber threats, increase the level of UAV flight safety and the effectiveness of the tasks assigned to them.

In the law "On approval of the rules of operation of unmanned aerial vehicles in the airspace of the Republic of Kazakhstan" there is no data on the protection of UAVs from cyber threats. Therefore, it is recommended to develop and implement laws on methods of certification, verification, analysis of countering cyber-attacks of all UAVs flying over the territory of the Republic of Kazakhstan.

References

1. The Law "On approval of the rules of operation of unmanned aerial vehicles in the Airspace of the Republic of Kazakhstan". –Order of the Acting Minister of Industry and Infrastructure Development of the Republic of Kazakhstan dated December 31, 2020 No. 706. Registered with the Ministry of Justice of the Republic of Kazakhstan on January 5, 2021 No. 22031) -2021

2. The Law "On the Use of the Airspace of the Republic of Kazakhstan and Aviation Activities" – the Law of the Republic of Kazakhstan dated 10.05.2017 No. 64-VI (entered into force after ten calendar days after the date of its first official publication) -2017

3. Global Operational Concept of Air Traffic Control [Electronic Resource] : (Doc 9854) – First edition. Twothousand five.

4. Current issues of ensuring cybersecurity of unmanned aerial vehicles [Electronic resource]/-URL://http://militaryreview.ru/aktualnye-voprosy-obespecheniya-kiberbezopasnosti-bespilotnyx-letatelnyx-apparatov.html? (accessed 18.04.2022).