http://www.moderntechno.de/index.php/meit/article/view/meit26-01-052
DOI: 10.30890/2567-5273.2023-26-01-052

UDC 623.746

ANALYSIS OF ANTI-DRONE SYSTEMS

Prytula M.O.
c.t.s., as.prof.
ORCID: 0000-0003-1577-5215
Khloba A.A.
student of the 1st year of the master's degree
Shurkhal M.Y.
student of the 1st year of the master's degree
Vinnytsia National Technical University, Vinnytsia, Khmelnytsky highway 95, 21021

Abstract. *The use of drones for military and commercial purposes has grown dramatically over the past two decades, and their missions range from surveillance and reconnaissance to combat support. Technological progress has led to increased capabilities and reliability of drones, and the availability of drones has also increased dramatically.*

The methods of combating drones are analyzed. In particular, the main focus is on radio frequency methods and hand drone jammers. Existing hand drone jammers manufactured in different countries are also considered.

Key words: *drones, drone jammers, spoofing, radio frequency warfare.*

Introduction.

Over the past years, the scope of drones (or UAVs - unmanned aerial vehicles) has expanded significantly. Very often, drones appear at airports, at security facilities (detention points, military factories), and are also used to track people. A lot of people have appreciated the advantages of aerial reconnaissance and use it actively without hesitation [1].

All drone manufacturers are constantly improving them. The drone allows users to collect information about the object of interest to us almost imperceptibly from the air. An object can be a person, a group of people, an enterprise or some territory. Commercial drones are becoming more and more autonomous by moving from purely remote-controlled devices using Wi-Fi bands (2.4-5 GHz) to portable and autonomous aircraft with obstacle detection, palm launch, gesture control and capabilities tracking. Unfortunately, these new features can easily be used to commit several types of crimes, ranging from violating privacy, for example through aerial photography, undermining critical infrastructure, military bases and warehouses, or even places of mass gathering of people [2].

Understanding the above problems, in recent decades the world community has taken a number of countermeasures to prevent drones from entering restricted areas. The issue of drones being misused is a global priority. The more expensive the device, the more difficult it is to resist it, which makes the difficult task of fighting drones an unequal battle, because without special equipment, the average person has nothing to oppose the drone [1].

Thus, there is a need to develop consistent standards and rules that, on the one hand, will provide space for the development of UAV technologies and their widespread use in the economy, and on the other hand, ensure the safety of citizens and infrastructure that is of key importance for the security of the state.

Manufacturers of anti-UAV systems are constantly looking for the most effective tools to solve this problem. The main objective of this publication is to analyze existing anti-drone systems.

Analysis of anti-drone methods.

Since different objects are not equally located on the territory, don't have the same infrastructure, therefore different approaches are used to ensure that the protection is maximum, it depends on the size, security policy and other factors of the object. At the moment, there is no such system that can provide 100% anti-drone protection.

There are three types of protection:

1. Preventive: restriction of use by making amendments to the legislation; warning boards in front of the territory; no-fly entered into software (geolocation data).

2. Observation and detection: radar, acoustic, optical, radio-frequency, multi-sensors and systems that are located on the object's territory.

3. Neutralization: control interception (spoofing) and radio suppression of drones, physical interception (by other drones using a net), physical destruction (lasers, weapons) [2-3].

One of the methods of neutralizing a drone is jamming. This method allows you to save the drone and get valuable information from it. A jammer can broadcast a strong jamming signal to prevent the drone's receiver from properly receiving and receiving messages from the radio frequency spectrum emitted by the source (drone user). Jamming is particularly useful for combating drones because it allows you to disrupt both the remote control and the drone's Global Positioning System (GPS). When the positioning and navigation functions are blocked, the drone goes into a safe mode - landing or returning to the original position. Today, GPS jamming is considered one of the best methods for protecting specific targets, territories, infrastructure and preventing unauthorized drone flights [4].

This technology is relatively cheap, easy to operate and can have a significant positive effect - temporarily disabling all nearby drones. These advantages are also accompanied by some significant disadvantages.

RF noise can interfere with nearby communications systems, making this jamming technology problematic in many sensitive environments, including the ability to disable authorized drones. Since the jamming effect depends on the strength of the RF noise, its resulting effect depends on the relative strength of the signals that the drone receives from the remote control and the jammer, which depends on the transmission power and the distance to the object. The jammer works only if its signal is dominant. That is, the silencer will work only when the drone is far enough from the remote control and close enough to the silencer. Also, if the drone activates the "return to home" function, its pilot will be able to resume control as soon as the drone gets close enough to the remote control. Of course, if the jammer stops transmitting, the pilot can immediately resume control.

Some types of jammers have certain strengths and weaknesses. Directional jammers provide a longer range than other types of jamming and cause less interference in the immediate vicinity. But this requires continuous transmission of

the interference signal. Directional jammers cannot effectively counter swarms of drones, which typically approach from multiple directions. A narrow beam can also become ineffective if the drone begins to turn "home" and the pilot is able to regain control and fly in a different direction or avoid the effective angle of the directional jammer.

Omni-directional jammers can deter drones from all directions and thus better deal with drone swarms. They offer a shorter range in a larger area than directional silencers. The side effect of authorized and safe drones, as well as other nearby communication systems, also increases.

Hand jammers are mobile and easy to use. The operator simply pulls out the device and points it. Disadvantages: Since this method is manual, the user must carry a portable jammer, power batteries (in a backpack) and be alert (optics are also required).

If the operator is unable to immediately activate the portable jammer or is not paying attention, the chance to neutralize the drone may be lost. Also, manual silencers operate at a low power level in order not to endanger the health of the operator, which also limits the range of the device.

This type of jammer is effective in scenarios where a specific sensitive point needs to be protected and the threat is close and within sight. This is practically useless in cases where it is necessary to protect a perimeter or border, that is, a large area, since the drone can simply fly high enough to be out of range of the manual jammer [5].

Drone developers use several frequency bands for radio control of copters. Depending on the frequency range in which the radio control of the drone will be carried out, the cost, class and tasks that it must perform are affected. Commonly used radio frequency bands are Wi-Fi 2.4-2.5 GHz, GPS L1 / Glonass L1 - 1.57-1.62 GHz, GPS L2-L5 - 1.17-1.280 GHz, 5.8G - 5, 5-6.1 GHz, 5.2G - 4.9-5.5 GHz, RC433 - 4.33 GHz, 3G - 2.11-2.17 GHz. The drone does not work at all of the above frequencies, it all depends on the model and factory settings, in some models you can change the communication channel [6].

Many of the latest drones operate on 5G cellular networks rather than traditional remote control frequencies, allowing for greater range and improved smartphone integration. This is expected to become the norm, creating problems for all types of jammer drones.

Drone spoofers look, feel, and work just like other portable drone "guns," except they don't actually block drones. As jammers broadcast noise to make radio signals unintelligible, spoofers intercept radio signals to take control of drones, forcing them to stop. This is done by transmitting compatible signals with sufficient strength to replace the source [7].

One of the main jammer's problems is that they are inaccurate. They often jam other electronic devices such as radios and navigation systems.

Analysis of existing hand jammers.

Based on the results of the analysis of existing hand jammers, some jammers can be marked. We can cite the UAV Scrambler 300 model manufactured by Iding Design (Figure. 1, a), which uses a design of three antennas (Figure. 1, b), which can

create directional interference at operating frequencies including 2,4 GHz, 5,8 GHz and GPS L1/L2, which allows you to suppress the signals of various types of drones [8].

(a) (b)

Figure 1 - Appearance of the UAV Scrambler 300 model (a) and body components (b).

The frequency selector button can control three different frequencies to achieve separate or simultaneous interference, equipped with a built-in 3000mAh battery that provides up to 1 hour of continuous operation. It has a compact size and is easily installed on a stand or tripod. [8].

Another of the analyzed models is the UAV-D04JAI. Designation and detailed description of parts of the UAV-D04JAI model is shown in Figure. 2 and in Table 1 [9]. Operating frequencies: GPS, GLONASS, Galileo, BeiDouB1, 2.4 GHz 5.8 GHz. The power at different frequencies is different, as is the width of the main lobe of the antenna, for example, at a frequency of 2.4 GHz, the transmission power will be 50.05 dBm, with a beam width of 29 degrees horizontally and 25 vertically [9]. This also applies to all other models of hand jammers on the market.

Table 1 - Components of the UAV-D04JAI

№	Part name	Function
1	Power adapter interface	Connecting the adapter
2	Main unit	Control center
3	Battery	Powering the device
4	Antenna	Signal transmission
5	RF switch	Turns transmission off/on
6	Stock	Auxiliary element
7	Indicator of radio frequency, power status	Determination of the current state
	Power button	Off/On
	Mode switch button	D - Home flight mode L - Forced landing
	Power setting button	Power change
8	Telescopic sight	Observation of the target

There are many models of different manufacturers with different design features, power, frequencies and number of functions. A number of modern manual

jammers are presented on Figure 3. They are used in armies around the world, including the Ukrainian. Among them are Lithuanian EDM4S, Australian DroneGun Tactical, Ukrainian KVSG-6 and Antidrone-M, RG-7 [10-12]. It should be noted that the battery life is 1-2 hours.

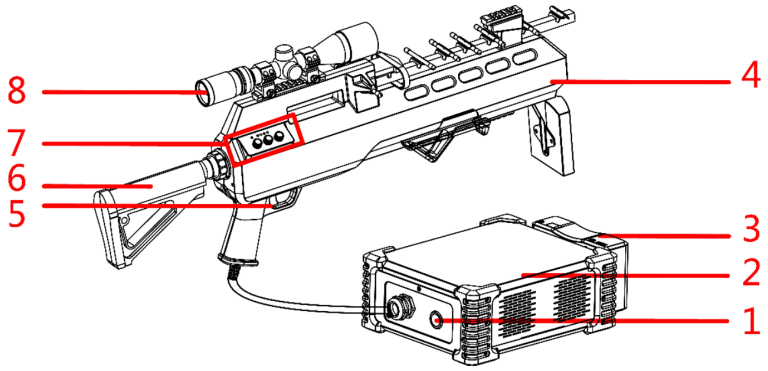

Figure 2 - Design features of the UAV-D04JAI model.

Figure 3 - Model RG-7 (Ukraine) (a), NightFighter (Britain) (b), DroneGun Tactical (America) (c), EDM4S (Lithuania) (d), KVSG-6 (Ukraine) (f), ANTIDRONE-M (Ukraine) (e).

ANTIDRONE-M jams signals on the following frequency ranges: 2.4G WiFi 2400-2500 MHz - 40W; GPS L2 1227 MHz - 15W; 868-912 MHz (860-920 MHz) - 25W; 433-434 MHz - 20W; GPS L1 + Glonass 1575-1620 MHz - 40W; 5.8G 5.5-5.9 MHz - 2W [10-12].

KBSG-6 allows you to block a similar set of frequencies: video transmission 2.4G WiFi 2400-2500 MHz - 20 W, navigation signals GPS L2 1227 MHz - 10 W and GPS L1 + Glonass 1575 -1620 MHz - 20 W; radio control signals 868-912 MHz (860-920 MHz) - 10 W and 433-434 MHz - 10 W; And 5.8G 5.7-5.9 GHz frequencies - 10 W [10-12].

Therefore, there are a large number of models of hand jammers on the market. We can not say that one or another model is the best. It depends on many factors, so the choice is up to the user.

Summary and conclusions.

In this article, various methods of jamming drones were analyzed. As a result of the analysis, the advantages and disadvantages of all three methods were determined: omni-directional jammers, directional jammers, hand jammers. Hand jammers from manufacturers of different countries that are currently on the market were also analyzed.

Summarizing, we can say that technologies for countering military and civilian quadcopters are rapidly developing, especially radio jamming. They allow you to delay, divert, destroy or intercept control of the drone. At the same time, developers are improving the drones themselves. Either completely autonomous drones are being created, which use inertial navigation, or complex hardware and software means of signal transmission/reception from/to the operator are used. Thus, anti-drone systems need to be improved every day, and kinetic means of countering drones should not be neglected.

References:

1. Pietro Tedeschi, Gabriele Oligeri, Roberto Di Pietro. Designing and implementing future aerial communication networks, IEEE Access., vol. 8, pp. 5049-5064, December 2019. DOI: 10.1109/ACCESS.2019.2963105

2. Drone detection systems and anti-drone systems at: https://www.bezpeka-shop.com/blog/obzor/sistemy-obnaruzheniya-dronov-i-protivodronnye-sistemy/ (accessed 30.03.2023). (in Ukrainian)

3. Matthieu J. Guitton. Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms. Scandinavian Journal of Military Studies, vol. 4, pp. 26-36, January 2021.

4. 10 Counter-Drone Technologies To Detect And Stop Drones Today at: https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today (accessed 30.03.2023).

5. Evaluating and Comparing Counter-Drone (C-UAS) Mitigation Technologies URL: https://d-fendsolutions.com/cuas-mitigation (accessed 06.04.2023).

6. Features and blocked frequencies of drone jammers at: https://kvertus.com.ua/info/articles/funktsii-i-blokiruemye-chastoty-glushilok-dronov/ (accessed 06.04.2023). (in Ukrainian)

7. Drone Interceptors vs. Drone Jammers & Spoofers at: https://fortemtech.com/blog/discussions/2023/01/24/drone-interceptors-versus-jammers.html (accessed 30.03.2023).

8. UAV Scrambler 300 at: http://www.idingcn.cn/casesingle/41 (accessed 01.04.2023).

9. UAV-D04JAI anti-UAV complex at: https://hikvision.ru/product/uav_d04jai (accessed 02.04.2023). (in Ukrainian)

10. The Ukrainian military received Ukrainian anti-drone guns KVS ANTIDRON G-6 at: https://mil.in.ua/uk/news/ukrayinskym-vijskovym-peredaly-antydronovi-rushnytsi-kvs-antidron-g-6-vitchyznyanogo-vyrobnytstva/ (accessed 03.04.2023). (in Ukrainian)

11. Thanks to the armed forces, the dronegun tactical rifle became famous all over the world at: https://sundries.com.ua/zavdiaky-zsu-rushnytsia-dronegun-tactical-proslavylasia-na-ves-svit/ (accessed 06.04.2023). (in Ukrainian)

12. Ukrainians have created new RG-7 anti-drone guns at: https://focus.ua/uk/digital/556652-ukrajinci-stvorili-novi-antidronovi-rushnici-rg-7-yak-voni-ryatuyut-zhittya-foto (accessed 06.04.2023). (in Ukrainian)

Article sent: 19.04.2024