# Informational Technology for the Improvement of Flight Zone Security

Olena Kozhokhina[1] [0000-0002-3404-5704], Olga Shcherbyna[1] [0000-0001-6857-2505],
Oleksii Chuzha [1] [0000-0002-4625-2938], Serhii Yehorov [1] [0000-0001-6976-2394],
Maksim Iavich [2] [0000-0002-3109-7971], Nikolay Churkin[3][0000-0002-3056-657X ]

[1]National Aviation University, Kyiv, Ukraine
[2]Scientific Cyber Security Association, Tbilisi, Georgia
[3]JSC ‘Aeropribor Voskhod’, Moscow, Russian Federation

kozhokhina@gmail.com

**Abstract.** Unmanned Aircraft Systems are a new component of the aviation system and based on cutting-edge developments in aerospace technologies. Research has shown that the number of incidents involving unmanned aircraft systems operations in flight zones of airports increased rapidly. This paper aims to secure flight zone from unauthorized unmanned aircraft systems operations. Based on a review of the literature and incident statistics, the highest collision risks flight stages were highlighted. The results indicate that they are approach, descent and climb stages. On this basis, it is recommended to detect and track unauthorized unmanned aircraft systems use the acoustic sensor, radar, electro-optical sensors, infrared sensors and radiofrequency. Further research is needed to research GNSS antennas and its patterns to interrupt or change the received signal and, accordingly, lose the spatial orientation of the unmanned aircraft systems and shifted it from the flight zone to secure it.

**Keywords:** unmanned aircraft systems, aviation safety and security, flight zone, incidents, antennas for navigation system

## 1 Introduction

The principal purpose of international civil aviation is to ensure safety, security and regularity of aircraft operations. Unmanned Aircraft Systems (UAS) are a new component of the aviation system, and it is the fastest-growing segment. UAS based on cutting-edge developments in aerospace technologies and the safe and efficient integration of UAS into the non-segregated airspace is a long-term activity. It requires resolving key challenges to enable evolving technology. Several of these challenges are related to UAS operations in the airport environment [1].

The development of UAS is strictly linked with all stages of development of aviation in general. Currently information technology has changed the concept of UAS and expanded the scope of its application. That is why the number of UAS is overgrowing. According to the Federal Aviation Administration (FAA) forecast, the number of small UAS registered in the United States alone increased from 1.1 million units in 2017 to 2.4 million in 2022. The use of UAS essential for complex and dangerous missions, such as reconnaissance, monitoring, communications and others [2].

Reasoning from these facts, it is understandable that the number of UAS operations currently has far exceeded all estimates. Reports show that in recent years, because of incidents and accidents, a record number of UAS were damaged or lost. According to the analysis of incidents in UK Airspace [3], this number has increased twenty times over the past four years and more than thirty times over the past eight years (Fig. 1).

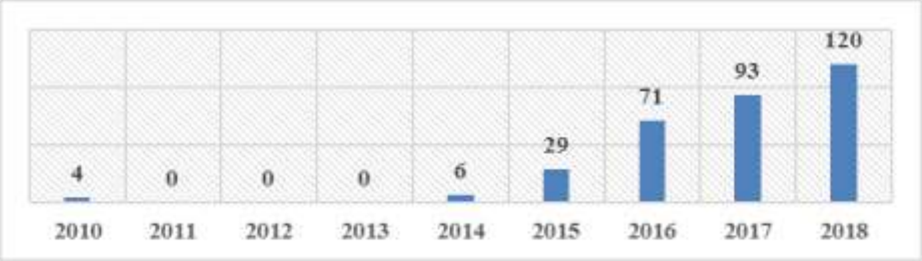


**Fig. 1.** Accidents involving UAS in UK Airspace

## 2 Problem statement

The use of UAS is expanding rapidly as well as accidents and incidents involving UAS and key aviation stakeholders such as airports, and aviation authorities are considering that many risks are migrated. From the analysis of the events with UAS, airborne conflict (defined as a potential collision between a UAS and an aircraft in the air) is the most common type of occurrence and closely associated with this type of occurrence were a number of occurrences classified as an Airprox (Air Proximity). Unauthorized UAS operations on or near airports have great potential to disrupt aircraft operations (Fig.2). The threat of UAS intrusions introduces substantial risk and highlights the need for solutions that can safeguard airports from rogue UAS. Recent UAS incidents at airports raise concerns of gaps in safety and security and underscore the need for airports to have clear policies to manage these incidents [4].

Unauthorized UAS operations on or near airports have great potential to disrupt aircraft operations (Fig.3). The threat of UAS intrusions introduces substantial risk and highlights the need for solutions that can safeguard airports from rogue UAS. Recent UAS incidents at airports raise concerns of gaps in safety and security and underscore the need for airports to have clear policies to manage these incidents [14].

Airport security is no longer limited to the perimeter of the airport; measures must be taken to protect beyond the perimeter for departing and approaching aircraft. These recent incursions around airports demonstrate that more needs to be done and at a faster pace than the regulatory process allows.

Many of reports specified the phase of flight when the UAS was encountered. As expected, most incidents were reported during approach, descent, takeoff and climb [5].

To determine the degree of damage to civilian aircraft in a collision with UAS and, accordingly, their impact on flight safety, some organizations conducted laboratory tests and simulated collisions of UAS with aircraft in the air with an assessment of the consequences of a collision.

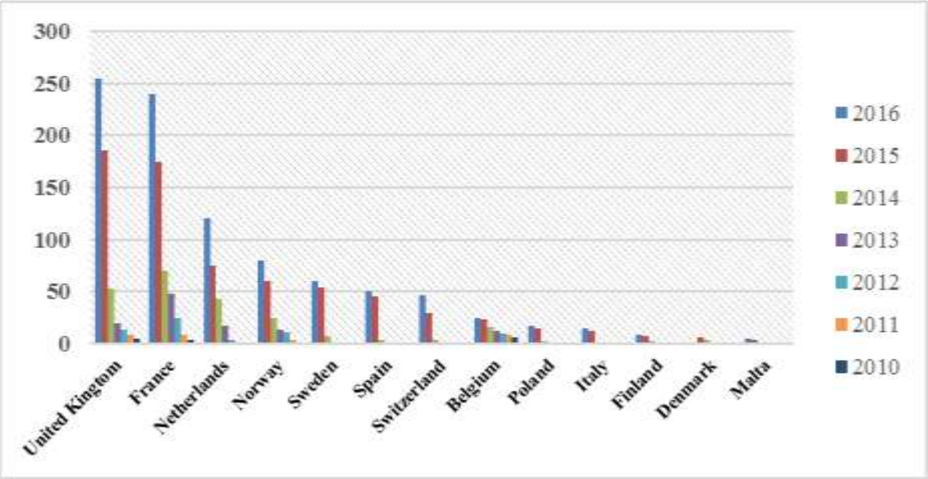


**Fig. 2.** UAS Airborne Conflict occurrences per state

An analysis of these studies identified several risk factors that may cause loss of control in flight:

1. The greatest threat is the ingestion of UAS into the engine, which can lead to disruption of its operation and possible failure in flight. The greatest danger is engine failure on take-off since flight altitude and speed are small.

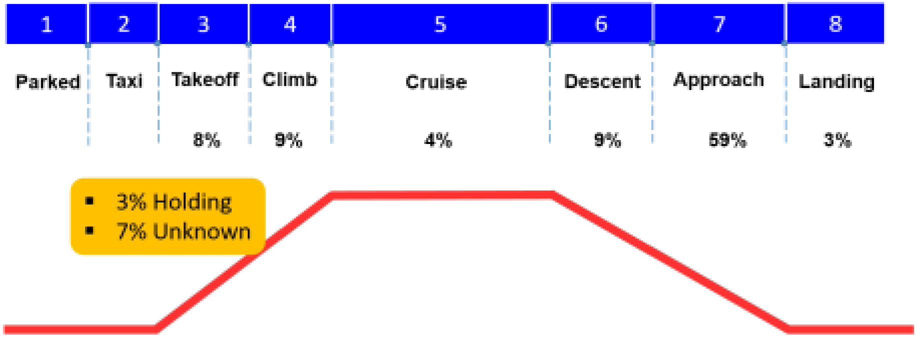


**Fig. 3.** UAS incidents distribution due to the phase of flight

2. The next threat is damage associated with the collision of a UAS with the fuselage, wing, tail of aircraft or the rotors and control screws of helicopters. These damages can lead to a violation of the aircraft tightness, damage to the wing mechaniza-

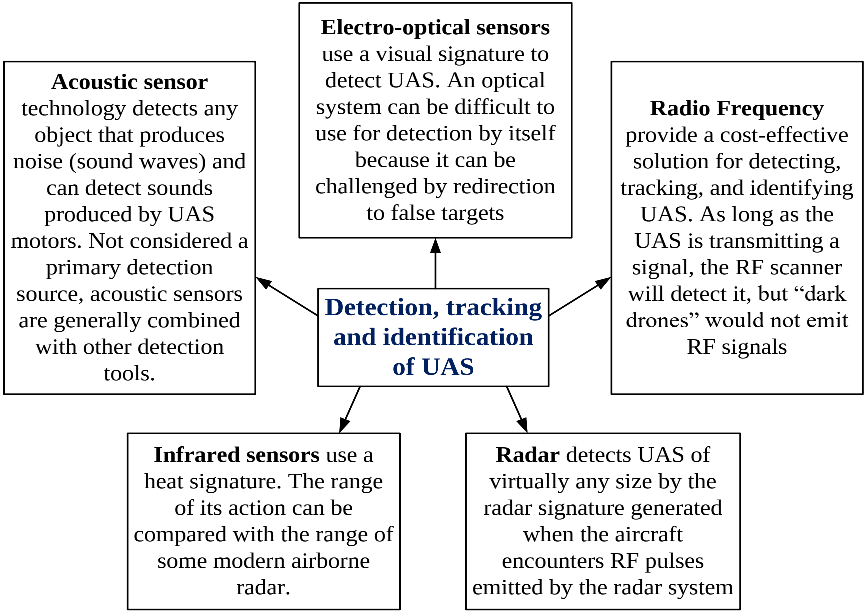
tion elements and anti-icing systems, as well as possible damage to control surfaces or their mechanisms. These facts mentioned above do decrease aircraft manoeuvrability and could lead to a full loss of control in flight.

3. Damage to the windscreen. This factor can lead to loss of aircrew orientation in flight, loss of aircraft tightness, and do decrease the view area in the cockpit [13].

## 3 Detection, Tracking and Identification (DTI)

Firstly, to secure flight zones from unauthorized unmanned aircraft systems operations, these systems must be detected quickly and accurately.

There are several technologies used for detection, tracking and identification of UAS such as acoustic sensor, radar, electro-optical sensors, infrared sensors and radio frequency (Fig. 4).



**Detection, tracking and identification of UAS**

**Electro-optical sensors** use a visual signature to detect UAS. An optical system can be difficult to use for detection by itself because it can be challenged by redirection to false targets

**Acoustic sensor** technology detects any object that produces noise (sound waves) and can detect sounds produced by UAS motors. Not considered a primary detection source, acoustic sensors are generally combined with other detection tools.

**Radio Frequency** provide a cost-effective solution for detecting, tracking, and identifying UAS. As long as the UAS is transmitting a signal, the RF scanner will detect it, but “dark drones” would not emit RF signals

**Infrared sensors** use a heat signature. The range of its action can be compared with the range of some modern airborne radar.

**Radar** detects UAS of virtually any size by the radar signature generated when the aircraft encounters RF pulses emitted by the radar system

**Fig. 4.** Technologies used for detection, tracking and identification of UAS

## 4 Interdiction of UAS

Air Traffic Control (ATC) were aware of the UAS by DTI or had been previously informed by the flight crew. Depending on the airport and region of the UAS activity, ATC undertook different actions to counteract the UAS activity. These activities included closing the airport, aircraft holding, go-arounds and diversions. (Fig. 5).

However, other anti-UAS measures may be deployed.

### 4.1 Jammers – RF or GNSS

Jammers, also called signal blockers, are devices that block communication signals. Technology can disrupt both RF and GNSS links. Once the RF or GPS link is jammed, the UAS can be forced to land immediately or return to its home location. Some serious concern with jammers is the unintended consequence of interfering with legitimate communications approximately the UAS [1].

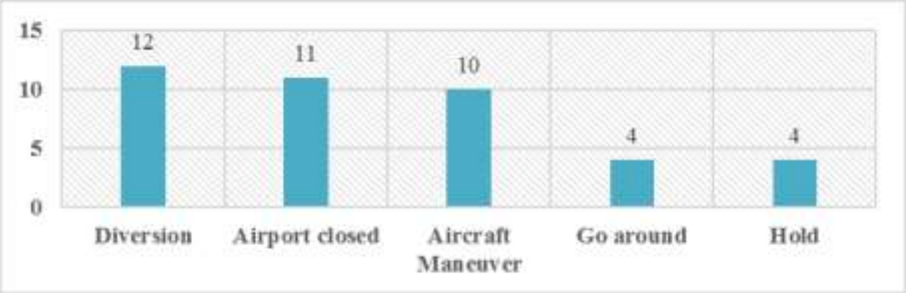


**Fig. 5.** Airport and flight crew actions following UAS activity. Source: STEADES Database

### 4.2 Protocol Manipulation (aka Spoofing or Hacking)

The emitted signal instructions are designed to confuse the UAS so that it operates as though the manipulated instruction is the legitimate signal. Protocol manipulation employs algorithms, often enhanced with artificial intelligence, to take control of the UAS with a new, 'smarter' communications link that removes the UAS from the threat environment (Fig. 6).

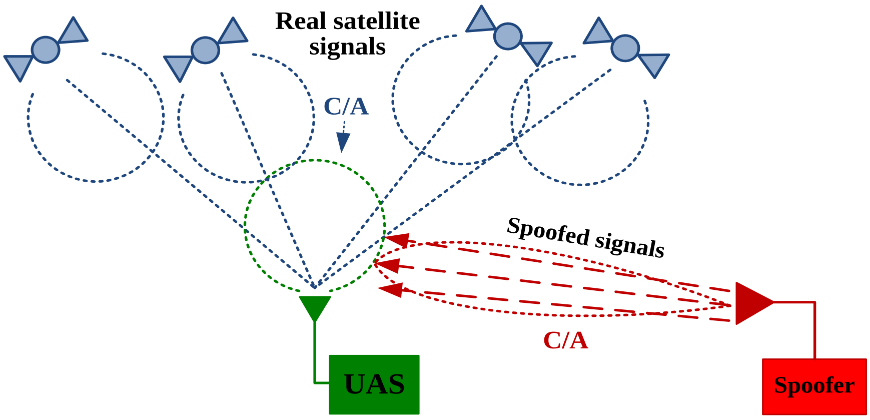


**Fig. 6.** Spoofing of UAS

### 4.3 Kinetic Interdiction and Geofencing

Many types of kinetic options are being tested and, in limited cases, deployed on the battlefield or in high-level special events. In many instances outside of the battlefield, however, kinetic techniques may not be a viable option for use in crowded areas due to the risk of a UAS vehicle crashing or triggering the deployment of a payload (see Fig. 7) [1].

Risk-based solutions such as manufacturer-installed geofencing technology are essential advancements in mitigation and should become the industry standard, rather than the exception [1].

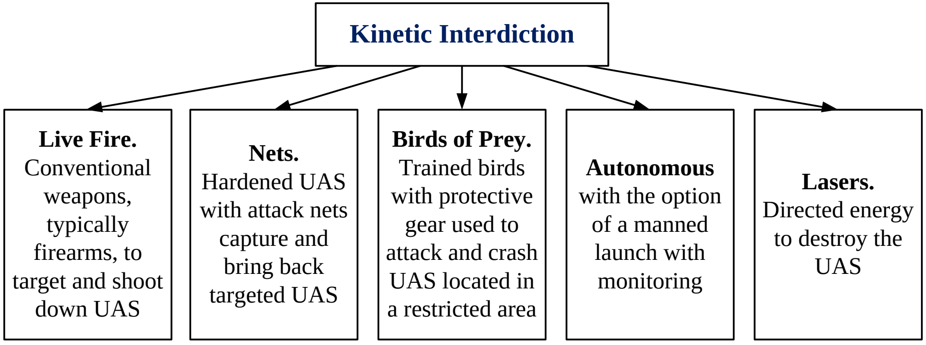

Kinetic Interdiction
Live Fire. Conventional weapons, typically firearms, to target and shoot down UAS
Nets. Hardened UAS with attack nets capture and bring back targeted UAS
Birds of Prey. Trained birds with protective gear used to attack and crash UAS located in a restricted area
Autonomous with the option of a manned launch with monitoring
Lasers. Directed energy to destroy the UAS

**Fig. 7.** Kinetic interdiction refers to intercepting UAS by physical means

## 5 Antennas on UAS

The jamming or spoofing of GPS signals may harmfully impact aircraft navigation systems as well as air traffic management systems - both of which heavily rely on functional, uninterrupted GPS signals. Nevertheless, this impact can be reduced by studying the radiation pattern of antennas for Global Navigation Satellite System (GNNS) such as Global Positioning System (GPS), Galileo, GLONASS and other.

In this way, also the likelihood of detection, tracking and identification of unauthorized UAS can be increased. All this, as a result, leads to improvement of flight zone security.

### 5.1 Blade Antennas for radio communication

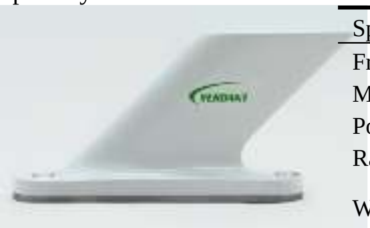
Most of the blade antennas are an adaptation of the monopole radiator, one of the most fundamental types of antennas. Typical monopoles have a quarter wavelength and should be mounted on a conductive plane, resulting in a vertically polarized wave with the maximum gain in the horizontal plane. For electrically small structures, such as UAS, where the vehicle body operates as a reflection plane, the maximum gain is achieved at lower lift angles.

VERDANT JL 50 is an L - band antenna used with the telemetry system of UAS and helicopters (Fig. 8).

The antenna has an excellent omnidirectional pattern over the entire band. The radiating element is encased in a single piece of fiberglass-reinforced epoxy shell. The antenna is designed as lightweight, low profile, low drag stub antennas ideally suited for high-performance, supersonic aircraft.

## 5.2 Antennas used in First Person View

The antennas used in FPV (First Person View) most often operate at 2.4 GHz and 5.8 GHz, respectively for radio and video. Lower radio frequencies for radio control and video transmission, such as 915 MHz, are often used when the long-range flight is a priority.



| Specifications | Value |
|---|---|
| Frequency Range, MHz | 1430-1540 |
| Polarization | Vertical |
| Radiation Pattern | Omnidirectional in azimuth |
| Weight, grams | 55 |
| Height, mm | 44 |

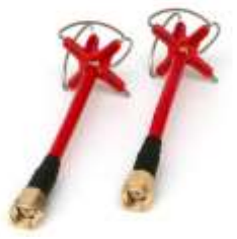
**Fig. 8.** Blade antenna VERDANT JL 50

According to the type of FPV, the antenna pattern can be divided into two categories - directional and omnidirectional. Directional antennas are best suited for receiver-side applications where they can be placed to ensure optimum reception of the signal transmitted by the video transmitter. The transmitter side typically uses an omnidirectional antenna, as its radiation pattern is well adapted to adapt to sudden changes in the altitude and flight direction of the aircraft of UAS.

There is a relatively wide range of antennas for this purpose. Most referred are Pagoda-2 - omnidirectional antenna with circular polarization (Fig. 9) and Leaf Clover AV Transmission RHCP antenna Aomway 5.8GHz FPV with circular polarization (Fig. 10).

| Specifications | Value |
|---|---|
| Frequency Range, GHz | 5,55 – 6,05 |
| Polarization | RHCP or LHCP |
| Radiation Pattern | Omnidirectional in azimuth |
| Axial ratio | < 1.3 (2.28 dB) |
| Gain, dBi | 5 |
| Weight, grams | 9,3 |
| Size, mm | 22 x 54 x 80 |

**Fig. 9.** Antenna Pagoda-2



| Specifications | Value |
|---|---|
| Frequency Range, MHz | 5645-5945 |
| Polarization | RHCP or LHCP |
| Radiation Pattern | Omnidirectional in azimuth |
| Gain, dBi | 3 |
| Weight, grams | 8 |
| Size, mm | 25 x 85 |

**Fig. 10.** Leaf Clover Antenna Aomway 5.8GHz FPV

## 5.3 Antennas for satellite navigation

The passive antenna must function within the required GNSS service range. Frequencies of GNSS systems are shown in Table 1.

**Table 1.** GNSS frequency bands.

| GNSS | Lower L-band | Upper L-band |
|---|---|---|
| GPS | L5: 1164–1189 MHz<br>L2: 1215–1239.6 MHz | L1: 1567–1587 MHz |
| Galileo | E5: 1164–1215<br>E6:1260–1300 MHz | E1: 1559–1591 |
| GLONASS | G3: 1189–1214 MHz<br>G2: 1237–1254 MHz | G1: 1593–1610 MHz |
| BeiDou/Compass | B2: 1179–1203 MHz<br>B3: 1256–1280 | B1: 1553–1569 MHz |

General specifications for passive GNSS antennas are summarized in Table 2. It should be noted that these characteristics may vary greatly depending on the antenna platform and the particular application.

**Table 2.** General technical specifications for a GNSS passive antenna.

| Specification | Value |
|---|---|
| Frequency band, MHz | 1164–1610 |
| Polarization | RHCP |
| Input impedance, Ohm | 50 |
| VSWR (voltage standing wave ratio) | < 2.5 (typical) |
| Gain at 0° (zenith), dBi | min 0 dBi |
| HPBW (half-power beamwidth) | 85° – 100° (typical) |
| Axial ratio (zenith), dB | < 3 |

There are two types of antennas most commonly used in GNSS microstrip rectangular and spiral (quadrifilar) antennas.

Microstrip patch antennas (Fig. 11) easy to integrate and ideal for less demanding applications where extreme performance and battery life can be sacrificed at the expense of device cost. The typical height of GNSS microstrip antennas is 2-5 mm and can be designed on low or high dielectric substrates. Depending on the choice of the substrate, the transverse dimensions range from 15 to 35 mm. One of the most commonly used forms of microstrip antennas is ceramic dielectric with a relative dielectric constant of about 20, and the total size is usually 25 × 25 mm. This particular antenna size and performance is perfect for most navigation applications. The design of microstrip antennas is well described in the literature [6, 7].

One of a commonly used example of GPS microstrip patch antenna GPS is MPA-254 from Maxtena (Fig. 11). This antenna is designed for embedded applications such as GPS handheld units, mobile devices, and tracking devices.

| Specification | Value |
|---|---|
| Frequency band, MHz | 1575.42 ± 20 |
| Polarization | RHCP |
| Beamwidth (3dB) | 100 (both axes) |
| Gain, dBi | 5,5 |
| Size, mm | 25 x 25 x 4 |

**Fig. 11.** Passive GPS microstrip patch antenna GPS MPA-254

Fig. 12-13 presents the results of simulation of a patch antenna for GPS network frequency (L2 1227.6 MHz), which is made from foil FAF-4D foil with the parameters: substrate thickness h = 0.002 m, dielectric constant of substrate $\varepsilon_r$ = 2.5, dissipation factor of a dielectric tg$\delta$ = 0.0007.

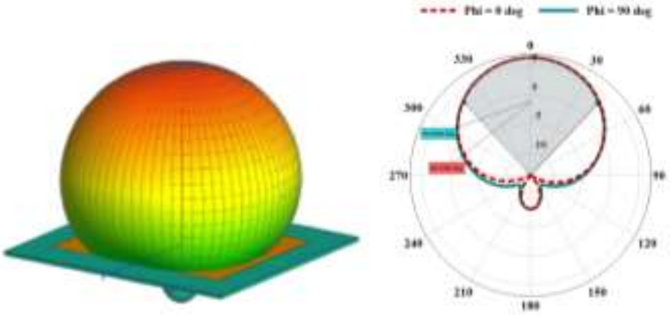


**Fig. 12.** Patch antenna pattern in polar coordinates at the centre frequency and 3D patch antenna pattern

A helical antenna is the main types of antenna for circular polarization due to its good axial ratio in a frequency band and simple construction. However, in the GNSS bands, the wavelengths are too large for the helical antenna to be practical for integration into the user platform. Therefore, a particular form of helical antenna known as quadrifilar helical antenna (QHA) has been used in mobile applications. It has better performance, especially on the broader frequency range [15-19].

Printing spiral shoulders can reduce the size of the antenna on a ceramic substrate with a large dielectric constant. Spirals can also be mounted on flexible thin substrates. Both mentioned types of antennas are shown in Figs. 14 and 15.

Fig.16-18 presents the results of QHA simulation for the Beidou network frequency (BD3 1268 ± 12 MHz). A special radiofrequency substrate with the following parameters was selected as the dielectric substrate material for the antenna shoulders: thickness t = 0.0001 m; dielectric constant $\varepsilon_r = 3.4$; dissipation factor of a dielectric $\mathrm{tg}\delta = 0.002$; the thickness of the copper layer $\Delta = 35$ μm.

For QHA, the shoulders of which are made of wires, there are known methods of calculation [8]. However, for microstrip shoulders, these ratios need adjustment [9,10,11, 12].

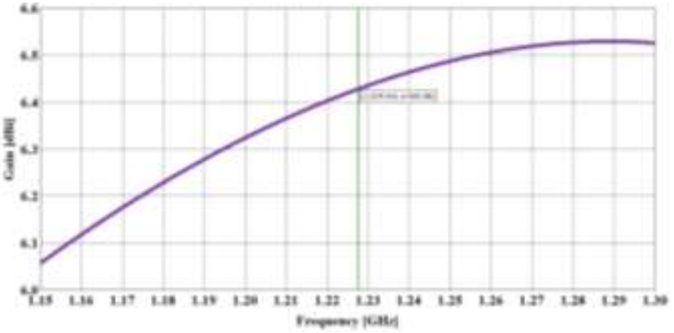
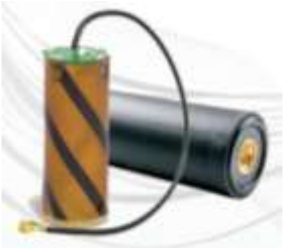
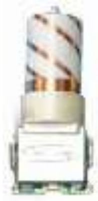


**Fig. 13.** Dependence of the gain of the microstrip antenna in the maximum radiation from the frequency of operation.



| Specification | Value |
|---|---|
| Frequency band, MHz | 1575 (GPS)<br>1602 (GLONASS) |
| Polarization | RHCP |
| Axial ratio, dB | 0,5 |
| Gain, dBi | 1,5 |
| Size, mm | 13,2 x 33 |
| Weight, grams | 3 |

**Fig. 14.** Passive QHA L1 GPS GLONASS M1516HCT-P-UFL



| **Specification** | **Value** |
|---|---|
| **Frequency band, MHz** | 1575 ± 20 |
| **Polarization** | RHCP |
| **Axial ratio, dB** | < 2 |
| **Gain, dBi** | 18 |
| **Size, mm** | 13,3 x 34 |
| **Weight, grams** | 7 |

**Fig. 15.** Active QHA L1 GPS SL1204 Sarantel

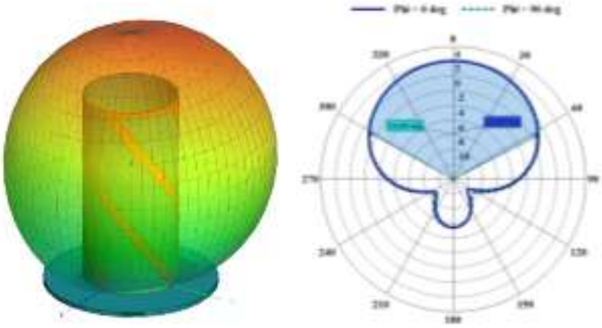


**Fig. 16.** QHA microstrip antenna pattern at the centre frequency

After mathematical modelling and further experimental studies of microstrip QHA (for different frequency ranges), the relationships between the working wavelength and the height and diameter of the microstrip QHA were calculated as diameter~ 0,25 Λ and Height ~ 0,3 λ. Uses two wavelengths, taking into account the effect of the dielectric substrate Λ and without taking into account λ (since the thickness of the dielectric material used to fabricate the QHA spiral arms has a minimal thickness, its influence can be neglected).

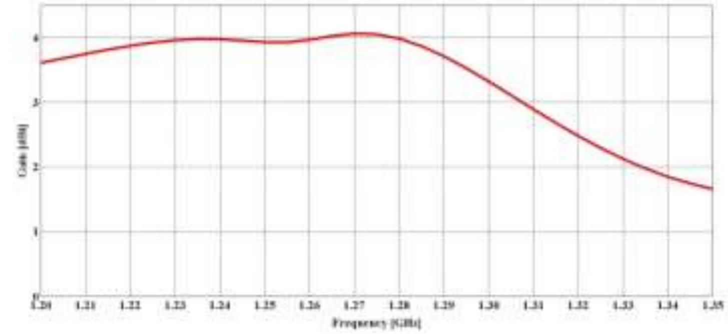


**Fig. 17.** Dependence of the gain of the QHA microstrip antenna in the maximum radiation from the frequency of operation.

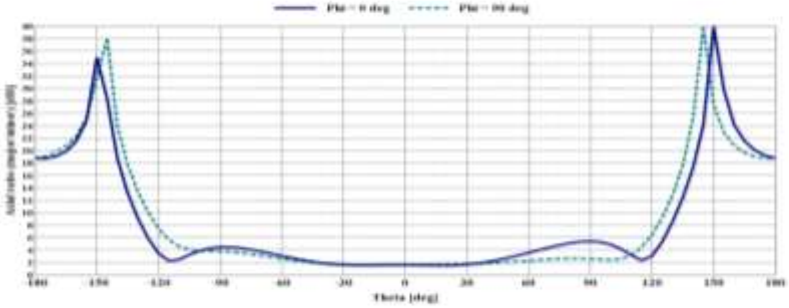


**Fig. 18.** The dependence of the axial ratio of the polarization ellipse on the meridional angle at the centre frequency

## 6 Conclusions

1. The use of UAS is expanding rapidly as well as incidents involving unauthorized UAS in flight zones of airports.
2. An analysis of the appearance of UAS in the area of dangerous proximity of aircraft showed that the highest collision risks arise during the approach, descent and climb stages.
3. Research of the consequences of UAS collisions with aircraft has identified many factors that may cause loss of control of an aircraft in flight. Such as ingestion of UAS into the engine. In addition, the collision of UAS with the fuselage, wing, the tail of aircraft or the rotors and damage of windscreen.
4. An analysis of the technical means of detecting, tracking, and recognizing of UAS showed that for this purpose radar and optical sensors for technical vision most appropriate, and UAS localization and elimination, it is advisable to use radio-frequency means.
5. There are algorithms for calculating the antennas of GNSS positioning systems, which allow generating the characteristics of the radiation patterns of UAS antennas for radio-frequency usage to eliminate unauthorized unmanned aircraft systems operations.
6. Analysis of the antennas of UAS positioning systems showed that for interrupt or change the received signal and, accordingly, lose the spatial orientation of the UAS. It is necessary to use a directional interference signal in the GNNS frequency range in which the UAS operates.
7. For elimination of unauthorized unmanned aircraft systems operations, their detection, identification and tracking are necessary, by radar, electro-optical sensors, infrared sensors and radiofrequency. Combined with a directional antenna considering its pattern for jamming or spoofing the positioning system, which leads to the loss of UAS orientation and its automatic landing.

### References

1. Blue Ribbon Task Force on UAS Mitigation at Airport. Interim Report. – July 2019. – P.32.
2. Arterburn D. Final Report for the FAA UAS Center of Excellence Task A4: UAS Ground Collision Severity Evaluation / 2017. – P. 196.
3. Analysis of Airprox in UK Airspace. Report Number 33. – 2017. – P.62.
4. Annual Safety Review. European Aviation Safety Agency. – 2016. – P.96.
5. Safety Report 2018 (Issued April 2019), 55th Edition, International Air Transport Association. –2019. – P.264.
6. Ilnitsky L., Sibruk L., Shcherbyna O. ‘Antenna Devices’. Kyiv, Ukraine. –2017. – P.200.
7. C.A. Balanis. Antenna Theory Analysis / John Wiley & Sons, Inc., Hoboken, New Jersey, 2005. — 1073 p.
8. Olga Shcherbyna, Oleg Tomai, Olena Kozhokhina, ‘Quadrifilar Helical Antennas with Different Types of Supply Lines’, Proc. of International Conference on Advances in Wireless and Optical Communications, 15-16 Nov. 2018, Riga (Latvia), pp. 167-170.

9. U. Kim, S. Choi and G. Kim, “Wide beamwidth quadrifilar helix antenna with improved axial ratio,” in Proc. of 2016 International Symposium on Antennas and Propagation (ISAP), 24–28 Oct. 2016, Okinawa (Japan), pp. 724–725.
10. M. S. Ghaffarian, S. Khajepour and G. Moradi, “A quadrifilar helix antenna using low cost planar feeding circuit,” in Proc. of 24th Iranian Conference on Electrical Engineering (ICEE), 10–12 May 2016, Shiraz (Iran), pp. 1019–1022.
11. J.-M. F. Gonzalez, P. Padilla, J. F. Valenzuela-Valdes, ‘An Embedded Lightweight Folded Printed Quadrifilar Helix Antenna: UAV telemetry and remote control systems’, ‘IEEE Antennas and Propagation Magazine’, vol. 59, no. 3, pp. 69–76, 27 April 2017.
12. Q.-X. Chu, W. Lin, W.-X. Lin and Z.-K. Pan, “Assembled dual-band broadband quadrifilar helix antennas with compact power divider networks for CNSS application,” IEEE Trans. Antennas Propagat., vol. 61, no. 2, pp. 516–523, February 2013.
13. O. Chuzha, A. Smyk, M. Chuzha. On-board warning system about the proximity of UAVs and other objects on the air. APUAVD 2019, Kyiv, Ukraine, pp 1-4.
14. Manual on RPAS/Doc 10019-AN/507 ICAO. –2015. – P.190.
15. Al-Azzeh J.S., Al Hadidi M., Odarchenko R., Gnatyuk S., Shevchuk Z., Hu Z. Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations, № 10(5), pp. 328-336, 2017.
16. Mazin Al Hadidi, Jamil S. Al-Azzeh, R. Odarchenko, S. Gnatyuk, A. Abakumova, Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions, Contemporary Engineering Sciences, Vol. 9, № 10, pp. 473-485, 2016.
17. Mazin Al Hadidi, J. Samih Al-Azzeh, O. Tkalich, R. Odarchenko, S. Gnatyuk, Yu. Khokhlachova. ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing, International Journal on Communications Antenna and Propagation, Vol. 7, № 1, pp. 48-56, 2017.
18. Odarchenko R., Abakumova A., Polihenko O., Gnatyuk S. Traffic offload improved method for 4G/5G mobile network operator, Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2018), pp. 1051-1054, 2018.
19. M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova. A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.