***“Fox hunting”***

***O.A. Vasiliev,***

***Director***

***Radioservice Co.***

***rsjet@mail.ru***

This article describes modern tendencies in development of digital communication jamming systems, global navigation systems, and UAV’s (drone) control lines used for design of universal multipurpose digital jammers. The article also provides examples of new systems of this type produced in Russia and abroad.

***Keys word***: digital wideband jammer, DDS technology, unmanned aerial vehicle – UAV.

Have you ever been interested in radiosport (radio broadcasting)? For example “fox hunting”? People of the older generation remember how cross or orientation with direction finder was very popular in USSR, even a film with the same title (“Fox hunting”) was shown in cinemas. It’s easy to find in *Wikipedia* that this kind of sport is still alive in Russia and we have the Federation of Radiosport, which promotes it and organizes many competitions. They are real enthusiasts, all honour to them! But I feel sorry for these guys because the technical side of this sport is absolutely out of date: receiver-direction finder is too primitive and it’s possible to run the cross with smartphones with GPS.

There are a lot of modern technical kinds of sport, including those connected with radio. For example, races of drones. But in Russia I have never heard about it, where is DOSAAF (Volunteer Society for Cooperation with the Army, Aviation, and Navy in Russia)? But I know that we have enthusiasts, who design drones and even participate in different exhibitions, competitions and win top places. That’s why our modest company decided to join the trendy progress. It’s very difficult to compete with Elon Musk’s *Space-X* and with *DJI* company (the main leader in drones’ manufacturing) but we could create something for protection or jamming of drones that are not used in a proper way – it’s our company’s profile.

First of all, we would like to describe the world of drones and list shortly the threats (also the informational ones) presented by unauthorized drones.

***UAV radio channels for control and information transmission***

Most of all, we will be interested in commercial drones. There are two sides of using drones. On the one hand, they can be used for monitoring situation on the ground, ensuring security of events, photo and video shooting, control of oil and gas pipelines, etc. On the other hand, drones can be used in terrorist and other illegal purposes: transportation and delivery of forbidden cargos (for example, drugs and explosives), unauthorized shooting of objects, exploring of closed territories, etc.

Most of drones can be categorized as robots as they can fly offline using GPS or GLONASS, rarely Galileo and BeJue for orientation. According to the law in most countries, drones must remain in the field of vision of their operators with possibility to control them manually using a remote control. Also there should be a radio link for fast information transmission between drone and a pilot. It can be video, telemetry, sound etc. transmitted in real-time mode. Nowadays most drones use unlicensed bands such as 433 MHz, 868 MHz, 2.4 GHz and 5.8 GHz.

We would like to specify communication links, technologies and signal types used for drones. In most cases, 2.4–2.483 MHz band is used for remote control and FHSS and DSSS technologies are used for high noise immunity in radio link. Every single manufacturer uses its own protocols for control channels, that’s why they are not compatible with UAVs of different manufacturers. For video transmitting 5.6–5.8 GHz band and OFDM technology are mainly used. This kind of modulation has very high bit rate but worse noise immunity (in comparison with wideband signals). Sometimes video is transmitted via Wi-Fi. For the telemetry transmission different types of channels and protocols, which use unlicensed bands, can be used, for example a separate channel in Wi-Fi 2.4 GHz, sometimes – built into a video image transmitted to the display in the same video channel, sometimes – through Zigbee on 868 MHz. frequency.

It should be mentioned that using a common frequency band leads to interference of Wi-Fi signal and drones’ control channels. This results in information loss, communication failure and drone control loss. The question of mutual influence of communication systems is under control of ETSI (European Telecommunications Standard Institute) standard. However, unlike *DJI*, many manufacturers don’t follow this standard. Now, when we know frequency ranges and types of signals, we can understand what and how must be jammed to interfere with drone flight and in what bands control signals and information received can be found. It should be taken into consideration that unlicensed frequency ranges are also the most dangerous for RIED, that’s why tasks of jamming of drone’s control radio channels, and of protection from radio fuses are similar in some way.

Now we will continue with description of jamming technologies and choice of the optimal strategy.

***Jamming technologies and signals blocking***

What kind of interference is the most “malicious” for this type of signals? Or, in other words, what kind of signals is the most interference-free? This question has been raised for a long time but it still doesn’t have any accurate answer. The main postulates are the following:

* The interference spectrum must be in the range of the jammed signal;
* If the structure of the signal is known but there is no accurate copy of signal transmitted in this particular moment, then the signal at the receiver’s input can be jammed only energetically (the structure of the jammed signal has no defining value).

It's like with channel code access in mobile network WCDMA. It’s known that for blocking of 3G BTS signals (UMTS-WCDMA), the power of the received signal at the subscriber’s receiver input must be exceeded for not less than 26-30 dB – 16-20 dB more than for GSM signals!

Historically, either analog chirp signals, or protection systems based on the principle of reformer (when the received signal was distorted in the receiver and was reemitted in the opposite direction towards the source) were used for jamming. The last way was very popular in the military air force; nearly all aircrafts in USSR had this kind of reformers. Modern analogues perform described operations in digital form and they are compact. But nowadays the leader in this sphere is DDS. Let’s see how a DDS jammer looks like and what the last trends in this technology are.

The jammer is based on a jamming signal conditioner. Usually, these are several DDS-chips controlled by FPGA. It can be programmed for a special task through USB or Ethernet. Today leading manufacturers produce fully digital conditioners based on the newest chips DDS and DAC, which have very high clock rates, for example 12.6 GHz (**DAC**) of AD9173 type of *Analog Devices* company. Such chip allows generating signals with frequency up to 6 GHz.

Apart from a signal conditioner, a wideband amplifier is required for a jammer. Thanks to the latest technologies, now it’s possible to produce power amplifiers with good load matching in a wideband frequency range. The most available amplifiers are produced by *MACOM*, *Minicircuits* and other North Korean companies. On the base of high power output transistors wideband amplifiers with 40-50 dB gain and up to 100 W and higher power are developed. These amplifiers are complete units ready to use, they require a good natural cooling system, or a powerful ventilation system. Any jammer requires such analogue amplifier. Please find in picture 1 a wideband amplifier produced by *Radioservice* company. This amplifier features 38 dB gain and 10 W output power in frequency range 400–3000 MHz or in frequency range 2–6 GHz.



Pic.1 *Radioservice* wideband amplifier

A key moment for design of a jamming system is selection of antennas, especially for a wideband programmed jammers. Most of the wideband antennas have rather low directivity. It’s not bad if you need a wide angle of jamming or large near jamming area. But usage of directional antennas requires significantly lower power of transmitter of jamming signal in drones’ jamming systems. That’s why we see a lot of “Star wars gun” type directional jammers on many security exhibitions. Even *JSC Kalashnikov Concern* showed something similar on the last exhibition in Moscow region.

Nevertheless, if you want this kind of devices to work, you will need special drone detection systems. Here manufactures make everything they can image: detection of radio signals in hemisphere (*Aaronia*), radar (*Blighter*), thermographic cameras, night-vision devices, etc. It’s clear that only a telescopic sight and some other little things can be installed on a “gun”. It’s important to note that a directional antenna will give us a profit in 10-12 dB, which means that if you want to create an interference sufficient for jamming of a drone, you will need an amplifier with less than 10-12 dB power (for example not 100 W, but only 10 or less), and it will be other dimensions, weight, operation time from batteries and etc.

Most of foreign companies, for example *KIRINTEC LTD* (Mercury BLADE5) and *UNIVALGROUP GMBH* (XWJ2), position their systems as universal jammers with power from 10 to 100 W, which can be used for design of a system for solution of certain tasks. Such systems can have 1 or 2 units (man pack – portable variant) or 5-6 and more units (vehicle variant). All of them have special software, but producers keep it secret, and some of them even equip their devices with a special button for instant deleting of system settings.

***RS6000 – universal jammer of digital communication signals, control and global navigation***

The key factor of jammer’s operability and performance is possibility of its reprogramming and distance control, which allows changing configuration, control spectrum and frequency range. As we described above, all modern jamming systems are designed this way. Following these trends, *Radioservice* company developed a multipurpose portable digital wideband jammer RS-6000, which allows changing jamming signal structure, numbers of ranges, spectrum width, type of modulation and other parameters of blocking signal. Software of the jammer allows performing all this remotely, via Wi-Fi or Ethernet.

The jammer can include one, two or more modules. Every module can jam up to 4 frequency bands (channels) with width up to 100 MHz, each of which can be chosen by an operator in frequency range from 400 to 3000 MHz or from 2 to 6 GHz depending on power amplifier used in a certain module with separate output power adjustment in each channel. An operator can create a communication window for his tasks between two jamming frequency ranges. All settings can be saved and downloaded from the file. The system features switchable filters for jamming harmonics and others spurious emissions.

In functioning algorithms time multiplexing of channels is used, which allows significantly saving energy resource of the system. Control of the whole system and jamming process can be carried out even through a tablet. An operator can choose a signal to jam from the set of standard signals and synthesize it how he needs. The device can be programmed to block all known standards of mobile communication and wireless access, including 2G, 3G, 4G, Wi-Fi, Bluetooth and etc. In radio monitoring mode our device allows an operator to jam all suspicious signals after their detection by setting the jammer to a certain frequency range.

When the signal is forming, we use DDS technologies and multiplexing of channels in time, which helps achieve high blocking efficiency and significantly reduce power consumption and minimize dimensions and weight of the device and its harmful impact on the operator. These technologies allow creating a compact jamming system using only two modules RS6000 and two built-in antennas. Such portable jammer designed in a case is presented in picture 2. It features an integrated forced cooling system and can be used for jamming of mobile telephones and channels of wireless access of all the existing standards as well as for neutralization of other detected sources of unauthorized radio emissions. Also it’s possible to connect external directional and omnidirectional antennas. The same equipment, but designed in a plastic case, is used for portable jamming of control signals and data transmission of drones. In this case an external antenna system is used, which is mounted on a sport carbine’s butt. Eight channels of such jammer are programmed for blocking of global positioning signals and control lines of drones in unlicensed bands 2.4 GHz and 5.8 GHz.

The system is completely autonomous, every module has its own IP-address, which allows an operator to carry out remote control and set the needed bands and power levels using Ethernet or Wi-Fi connections. The technical specifications of RS6000/2 are presented in table 1.

***Table 1. Technical specifications of RS6000/2 jamming system***

|  |  |
| --- | --- |
| ***Jamming frequency range*** | ***400 – 6000 MHz*** |
| Numbers of jamming channels  | 8 (12 optional) |
| Adjusted channel bandwidth | 0 – 100 MHz |
| Maximum channel bandwidth in 4 – 6 GHz band | 200 MHz |
| Output power in continuous mode | 20 W (100 W optional) |
| Total effective power in multiplexing mode  | 80 W (400 W optional) |
| Adjustment of output power | 30 dB |
| Antenna system | Directivity 5 – 12 dB, two built-in directional antennas |
| Control | PC with Windows, smartphone, tablet |
| Power source  | Removable batteries or adapter with alternating current/charger |
| Type of batteries  | Li-Ion 14.8 W |
| Operating time from 1 set of batteries | 1.5 – 2 hours |
| Cooling system’s noise level within 1 m distance  | Not more than 35 dB |
| Temperature range | From -10…..+55 °C |
| Weight (8 channels with built-in antennas in a case) | 10 – 12 kg |
| Dimensions (8 channels with built-in antennas in a case | 45x30x20 cm |



Pic. 2 Mounted in a case portable jammer

***Reactive Jamming***



Pic. 3. Spectrum Jet 3.0 spectrum analyzer (receiver)

***Table 2. Technical specifications of Spectrum Jet 3.0 real time spectrum analyzer (RTSA)***

|  |  |
| --- | --- |
| ***Frequency range***  | ***9 kHz - 6 GHz*** |
| Scanning speed with 10 kHz frequency resolution  | 30 – 50 GHz/s |
| Intermediate frequency | 140 MHz |
| Intermediate-frequency passband | 24 MHz |
| Spectrum analyzer’s passbands | 160 kHz – 32 MHz |
| Displayed average noise level 30 MHz – 6 GHz | -155 dB/Hz |
| Noise ratio  | Not more than 12 dB |
| Image channel selectivity | Not less than 70 dB |
| Spurious-free dynamic range | Typ. 80 dB |
| Time of adjustment of linear receiver  | Not more than 150 µs |
| Phase noise of heterodyne at 10 kHz detuning (on frequency 1 GHz)  | Not more than -86dBn/Hz |
| Heterodyne long-term instability  | 10 ppm |
| Maximum level of input HF signal | Not more than 20 dBm |
| Operating temperature range  |  -20…..+60 °C |
| Dimensions  | 174x80x32 mm |
| Weight | 400 gm |