Top Secret (p. 1.34 List - Order No. 0180 - 2022)
REVIEW of the practice of detecting intelligence actions against holders of classified information in the areas assigned to the main divisions of the FSB of Russia, including recruitment attempts via the Internet

In accordance with the decision of the Director of the FSB of Russia dated 15.01.2024 No. 16/2/753, the FSB Service of Russia, together with the main divisions of the FSB of Russia, conducted an analysis of the practice of detecting intelligence actions in assigned areas, including recruitment attempts via the Internet. The results show that after the start of the Special Military Operation (SMO), there has been a multiple increase in the number of intelligence actions by foreign intelligence services against holders of classified information. From 2022 to the present, security agencies have detected 2,874 intelligence actions by foreign intelligence services, whereas from 2017 to 2021, only 1,953 enemy intelligence actions were detected.

It was established that during this period, the largest number of intelligence actions against holders of classified information were carried out by Ukrainian intelligence services—1,960, which is more than 50% of the total and indicates a 7.5-fold increase in the activity of Ukrainian intelligence services compared to 2017-2021. The targets of Ukrainian intelligence services were Russian Armed Forces personnel, employees of the defense industry and nuclear weapons complex, operational support facilities along the "M" line, employees of OGVU, KFS, and the diplomatic corps, transport sector, representatives of scientific and educational fields, and the "communications" sector.

At the channel of departure abroad, intelligence actions were carried out by US intelligence services and their NATO allies against persons:
- on long-term or short-term foreign assignments;
- employed in Russian organizations under sanctions and knowledgeable about "sensitive" information.

Data collection regarding Russian citizens of interest is conducted by the enemy using agent networks, monitoring open sources, electronic industry and corporate resources. US intelligence services, using information from ticket booking systems, hotels, and registration at international events, track the arrival of Russian citizens of intelligence interest and create conditions in advance for their recruitment study. Priority is given to those who repeatedly travel on official business trips. To establish personal contacts, US intelligence services use border and migration control points at airports, involving local personnel. During border control, recruitment targets undergo "rigorous" interrogation about their professional activities, including forced collection of biomaterial, seizure of documents, communication devices, and computers, as well as requests for password-login combinations to devices and email accounts. Recruits are offered specific incentives for confidential cooperation, such as assistance in obtaining a US visa, or are pressured with threats of visa cancellation. After a comprehensive analysis of the personal and behavioral

profiles of targets, a decision is made on the advisability of further development, including recruitment.

Due to the reduction in foreign trips by holders of classified information to NATO countries caused by Western sanctions and the tightening of regime measures in the field of state secrets protection, there has been an increase of more than 5.5 times in the number of recruitment attempts against holders of classified information via the Internet, with 3,457 cases detected from 2022 to 2024. Their share in the total volume of detected intelligence actions increased from 6% in 2017 to 90% at present, and for Ukrainian intelligence services—from 20% to 98%.

In 2024, the enemy adjusted its search and recruitment tactics. The number of personalized probing and recruitment attempts against intelligence targets in Internet messengers increased fivefold, and mass phone calls and spam mailings with offers of cooperation or information provision to Russian holders of classified information, employees of communications, transport, and industry facilities, and military personnel in virtual thematic groups on platforms such as "VKontakte" and "Odnoklassniki" became aggressive and are carried out from positions controlled by Ukrainian intelligence services, so-called "fraudulent call centers." This method, in our opinion, is aimed at distracting counterintelligence resources and masking intentions toward real targets.

To search and study recruitment targets, foreign intelligence services actively use modern OSINT (Open Source Intelligence) methods and "probiv" Internet services containing personal and contact data of Russian citizens (work addresses, communication details, vehicle numbers, etc.), monitor correspondence of participants in destructive and other operationally interesting virtual groups in social networks and Internet messengers. According to materials available to the FSB Service of Russia, in January-May 2024, the enemy collected data in the OTKS regarding more than 13,500 Russian citizens, of whom 1,860 are holders of classified information, and 603 are military personnel of the Russian Ministry of Defense.

During contact establishment, representatives of Ukrainian intelligence services:
- demonstrate awareness of biographical data and family ties of the target, offer monetary rewards for information, exert psychological pressure by threatening to report alleged past transfers of secret materials to Ukrainian authorities, publication of compromising information, threats to life and health;
- use social engineering methods to obtain hidden remote access to messenger accounts of Russian citizens under recruitment study, primarily former and current holders of classified information in the defense industry and military personnel;
- use fraudulent schemes to initiate transfers of funds by Russian citizens to accounts used to support Ukrainian military formations, subsequently encouraging them to conduct intelligence or sabotage actions under threat of reporting the fact of "financing the Armed Forces of Ukraine" to Russian intelligence services.

It is noted that the vast majority of intelligence actions were uncovered by the OBV (68% of the total) as a result of proactive appeals to security agencies by military personnel about contacts with foreign intelligence services, indicating an effective preventive system at

Ministry of Defense facilities. This trend has been most evident since the start of the SMO. However, analysis of information obtained by the FSB Service of Russia about enemy targets shows that the share of military personnel does not exceed 30%. This circumstance is believed to be due to shortcomings in preventive work at operational support facilities, weakened interdepartmental interaction, and the coordinating role of counterintelligence units.

Repeatedly, as a result of developing enemy accounts, mass recruitment and probing attempts against employees of defense industry enterprises were identified, about which the operational support team had no information for several months. Additionally, the study of reporting materials shows that information independently obtained locally about network details of holders of classified information and other employees of regime facilities, as well as their groups, is sometimes passively accumulated and not used in search activities to detect signs of search and recruitment activity by foreign intelligence services. Attempts to intercept enemy intentions and technically penetrate their communication means are fragmented and significantly delayed, which does not allow timely identification of targets, suppress recruitment attempts, create conditions for counter-development, and conduct counterintelligence activities. In some cases, information about contacts with signs of recruitment and probing attempts is received from the operational support team to the FSB Service of Russia with delays.

Given the above, it is necessary to:
1. Intensify preventive work at counterintelligence protection facilities, ensure current accounting of virtual groups and communities of regime organizations, strengthen agent control over the actions of their participants and administrators, as well as interdepartmental interaction in this area of operational-service activity. Information about the activities carried out and their results should be included in reporting materials for KP "Passage."
2. Inform the FSB Service of Russia about the presence of operational positions in OSINT and "probiv" Internet services for subsequent joint identification and development of accounts of representatives of foreign intelligence services.
3. Organize the accumulation of information about participants in pro-Ukrainian and other destructive Internet communities and use it for automated comparative analysis with communication details of holders of classified information (including military personnel) and the results of counterintelligence searches on technical communication channels. The obtained materials should also be sent to the FSB Service of Russia for inclusion in auxiliary information databases. At the same time, it is reported that generalized information about participants in destructive "Telegram" channels must be obtained from the CBD. UKAKD FSB Service.
