ALTO SECRETO

(apartado 1.34 de la Lista; Orden núm. 0180 de 2022)

REVISIÓN

de la práctica de detección de acciones de inteligencia dirigidas contra personas con acceso a secretos de Estado, en los ámbitos de actividad asignados a las unidades rectoras de la FSB de Rusia, incluidos los contactos de captación a través de Internet.

En cumplimiento de la decisión del Director de la FSB de Rusia de 15 de enero de 2024, núm. 16/2/753, el **Primer Servicio de la FSB de Rusia**, conjuntamente con las unidades rectoras de la FSB de Rusia, ha efectuado un análisis de la práctica de detección de acciones de inteligencia en los ámbitos de actividad asignados, incluidos los contactos de captación realizados a través de Internet.

Los resultados indican que, tras el inicio de la denominada **"operación militar especial"**, se ha registrado un aumento de varias veces en el número de acciones de inteligencia de servicios especiales extranjeros dirigidas contra personas con acceso a secretos de Estado.

Desde 2022 hasta la actualidad, los órganos de seguridad han detectado **2.874 acciones de inteligencia** de servicios especiales extranjeros, frente a tan solo **1.953 acciones de inteligencia del adversario** entre 2017 y 2021.

Se ha establecido que, durante el período indicado, el mayor número de acciones de inteligencia contra personas con acceso a secretos de Estado fue llevado a cabo por los servicios especiales de Ucrania: **1.960**, cifra que representa más del 50 % del total y que, según el documento, evidencia un aumento de **7,5 veces** en la actividad de los servicios especiales ucranianos respecto de 2017-2021.

Los objetivos de interés de inteligencia de los servicios especiales ucranianos fueron militares de las Fuerzas Armadas de Rusia; trabajadores del complejo industrial de defensa y del complejo nuclear-armamentístico; instalaciones bajo cobertura operativa de la línea "M"; personal de la **OGVU** (agrupación operativa de tropas), de la **KFS** (Servicio Federal de Contrainteligencia) y del cuerpo diplomático; personal del sector del transporte; y representantes de los ámbitos científico, educativo y de las comunicaciones.

En el ámbito de los desplazamientos al extranjero, las acciones de inteligencia fueron realizadas por los servicios especiales de Estados Unidos y sus aliados de la OTAN contra personas:

- que se encontraban en viajes de servicio al extranjero, de larga o corta duración;
- empleadas en organizaciones rusas sometidas a sanciones y conocedoras de información sensible.

La recopilación de datos sobre ciudadanos de la Federación de Rusia de interés se lleva a cabo por el adversario mediante el uso de redes de agentes, la monitorización de fuentes abiertas y recursos electrónicos sectoriales y corporativos.

Los servicios especiales estadounidenses, utilizando información procedente de sistemas de reserva de billetes, hoteles y registros para actos internacionales, siguen la llegada de ciudadanos rusos de interés para la inteligencia y crean con antelación condiciones para su estudio con fines de captación. Se da prioridad a las personas que realizan repetidamente viajes oficiales al extranjero.

Para establecer contactos personales, los servicios especiales estadounidenses utilizan los puestos de control fronterizo y migratorio en aeropuertos, recurriendo a personal local.

Durante el control fronterizo, los objetivos de captación son sometidos a interrogatorios “duros” sobre su ámbito profesional de actividad, incluida la obtención forzosa de material biométrico, la incautación de documentos, medios de comunicación y equipos informáticos, así como la exigencia de combinaciones de usuario y contraseña de dispositivos y cuentas de correo electrónico.

A las personas objeto de captación se les ofrecen formas concretas de incentivo por una cooperación confidencial, por ejemplo, ayuda para obtener un visado estadounidense; o se ejerce presión mediante la amenaza de anular el visado. Tras un análisis integral de los perfiles personales y conductuales de los objetivos de interés, se adopta una decisión sobre la conveniencia de continuar su desarrollo operativo, incluida su captación.

En el contexto de la reducción de los viajes al extranjero de personas con acceso a secretos de Estado hacia países de la OTAN, provocada por la política de sanciones de los países occidentales, y del endurecimiento de las medidas de seguridad para proteger secretos de Estado, se observa un incremento de más de **5,5 veces** en los contactos de captación por Internet dirigidos a personas con acceso a secretos de Estado. Entre 2022 y 2024 se detectaron **3.457 casos.**

Su proporción dentro del volumen total de acciones de inteligencia detectadas aumentó, desde 2017 hasta la

actualidad, del 6 % al 90 %; en el caso de los servicios especiales ucranianos, pasó del 20 % al 98 %.

En 2024, el adversario modificó la táctica de sus actividades de búsqueda y captación. Así, se multiplicó por cinco el número de contactos personalizados de tanteo y captación dirigidos a objetivos de interés de inteligencia a través de mensajería por Internet.

Las llamadas telefónicas masivas y los envíos de spam con propuestas de cooperación o de entrega de información a personas rusas con acceso a secretos de Estado, empleados de instalaciones de comunicaciones, transporte e industria, y militares que participan en grupos temáticos virtuales de las plataformas VKontakte y Odnoklassniki, adquirieron un carácter agresivo y se realizan desde los denominados "centros de llamadas fraudulentas" controlados por los servicios especiales de Ucrania.

Según la valoración del documento, este último método está dirigido a distraer las fuerzas y los recursos de las unidades de contrainteligencia y a encubrir las intenciones dirigidas contra los verdaderos objetivos de desarrollo operativo.

Para buscar y estudiar objetivos de interés para la captación, los servicios especiales extranjeros utilizan activamente metodologías modernas de inteligencia de fuentes abiertas —**OSINT**— y servicios de Internet de "probiv", que contienen datos personales y de contacto de ciudadanos rusos, tales como direcciones de trabajo, identificadores de medios de comunicación, matrículas de vehículos y otros datos similares.

Asimismo, monitorizan la correspondencia de participantes de grupos virtuales considerados destructivos y de otros grupos de interés operativo en redes sociales y servicios de mensajería de Internet.

Según la información disponible en el Primer Servicio de la FSB de Rusia, entre enero y mayo de 2024 el adversario recopiló, a través de las **OTKS** (canales técnicos operativos de comunicación), datos relativos a más de **13.500 ciudadanos rusos**, de los cuales **1.860** tenían acceso a secretos de Estado y **603** eran militares del Ministerio de Defensa de la Federación de Rusia.

Durante el establecimiento de contactos, los representantes de los servicios especiales ucranianos:

- demuestran conocer los datos biográficos y vínculos familiares del objetivo de interés; ofrecen recompensas económicas por la entrega de información; y ejercen presión psicológica mediante intimidación, amenazando

con informar a los órganos de seguridad rusos sobre supuestos casos previos de entrega de materiales secretos a la parte ucraniana, con publicar información comprometedora o con amenazar la vida y la salud de las personas afectadas;

- emplean métodos de ingeniería social para obtener acceso remoto encubierto a las cuentas de mensajería de ciudadanos rusos sometidos a estudio con fines de captación, principalmente antiguos y actuales titulares de acceso a secretos de Estado en instalaciones del complejo industrial de defensa y militares del Ministerio de Defensa ruso;
- utilizan esquemas fraudulentos para inducir a ciudadanos rusos a transferir fondos a cuentas empleadas para apoyar a formaciones militares de Ucrania, con el fin posterior de coaccionarlos para que realicen acciones de inteligencia o sabotaje bajo la amenaza de comunicar a los servicios especiales rusos el hecho de una supuesta "financiación de las Fuerzas Armadas de Ucrania".

Se señala que la inmensa mayoría de las acciones de inteligencia —el 68 % del total— fue descubierta por los **OBV** (órganos de seguridad militar), como resultado de comunicaciones voluntarias de militares a los órganos de seguridad sobre contactos efectuados con ellos por servicios especiales extranjeros. Según el documento, ello demuestra la existencia de un sistema eficaz de trabajo preventivo en las instalaciones del Ministerio de Defensa ruso. Esta tendencia se habría hecho especialmente visible desde el comienzo de la denominada "operación militar especial".

Al mismo tiempo, el análisis de la información obtenida por el Primer Servicio de la FSB de Rusia sobre los objetivos de interés del adversario indica que la proporción de militares dentro de ese conjunto no supera el 30 %. El documento considera que ello se debe a deficiencias existentes en la organización del trabajo preventivo en instalaciones bajo cobertura operativa de los **TOB** (órganos territoriales de seguridad), al debilitamiento de la coordinación entre líneas operativas y a la pérdida de peso de la función coordinadora de las unidades de contrainteligencia.

En repetidas ocasiones, como resultado de la explotación operativa de cuentas del adversario, se detectaron contactos masivos de captación y tanteo dirigidos a empleados de empresas del complejo industrial de defensa, respecto de los cuales los **TOB** (órganos territoriales de seguridad) no habían dispuesto de información durante varios meses.

Además, el estudio de los materiales de informe muestra que la información obtenida de forma autónoma sobre el terreno acerca de los identificadores de red de personas con acceso a secretos de Estado, de otros empleados de instalaciones sujetas a régimen especial y de los grupos que los agrupan, en algunos casos se acumula pasivamente y no se utiliza en actividades de búsqueda destinadas a detectar indicios de actividad de búsqueda y captación por parte de servicios especiales extranjeros.

Los intentos de interceptar las iniciativas del adversario y de penetrar técnicamente en sus medios de comunicación tienen un carácter fragmentario.

En algunos casos, los datos sobre contactos que presentan indicios de captación o tanteo llegan desde los **TOB** (órganos territoriales de seguridad) al Primer Servicio de la FSB de Rusia con retrasos considerables. Ello impide identificar a tiempo los objetivos de interés de los servicios especiales extranjeros, neutralizar sus contactos de captación y crear condiciones para realizar un desarrollo operativo de respuesta y medidas de contrainteligencia.

A la vista de lo expuesto, es necesario:

1. Intensificar el trabajo preventivo en las instalaciones sometidas a protección de contrainteligencia; garantizar un registro actualizado de grupos y comunidades virtuales de organizaciones sometidas a régimen especial; reforzar el control mediante fuentes y agentes sobre las actuaciones de sus participantes y administradores; y mejorar la coordinación entre líneas operativas en esta dirección de actividad operativa y de servicio.

La información sobre las medidas realizadas y sus resultados deberá incluirse en los materiales de informe relativos al **KP "Passazh".**

2. Informar al Primer Servicio de la FSB de Rusia de la existencia de accesos o posiciones operativas en servicios de Internet de OSINT y de "probiv", para la identificación y el desarrollo operativo conjunto posterior de cuentas pertenecientes a representantes de servicios especiales extranjeros.

3. Organizar la acumulación de información sobre participantes de comunidades de Internet prorrusas, proucranianas y de otras comunidades consideradas destructivas, y utilizarla en análisis comparativos automatizados con los identificadores de medios de comunicación de personas con acceso a secretos de Estado, incluidos militares, y con los resultados de la búsqueda de contrainteligencia en canales técnicos de comunicaciones.

Los materiales obtenidos deberán remitirse igualmente al Primer Servicio de la FSB de Rusia para su registro en los ficheros auxiliares de información existentes.

Al mismo tiempo, se comunica que la información agregada sobre participantes de canales “destructivos” de Telegram deberá obtenerse de la **Base Centralizada de Datos (TsBD).**

UKAKD (Dirección de Coordinación, Análisis y Control de la Actividad) del Primer Servicio