потужнішою зброєю (встановити на безпілотники протитанкові ракети, гранатомети чи лазерні системи для підвищення їхньої ударної ефективності.)

Ефективне використання дронів і ройового інтелекту вимагає створення спеціалізованої інфраструктури. Продовжувати удосконалювати і впроваджувати платформи ситуаційної обізнаності (приклад "Дельта"). Визначити принципи координації між піхотою, дронами та артилерією через цифрові платформи, замість традиційного радіозв'язку.

Розробляти стійкі системи зв'язку: Використовувати mesh-мережі та альтернативні канали (напр., оптичний зв'язок) для забезпечення роботи дронів у зонах РЕБ. Впроваджувати алгоритми, які дозволяють дронам виконувати завдання без постійного зв'язку з оператором, спираючись на локальні сенсори. Оснащувати піхотні підрозділи портативними пристроями для глушіння ворожих дронів на відстані 1–2 км.

Горбатенко Андрій,
викладач,
ВСП «Фаховий коледж Інформаційних технологій
НУ «Львівська політехніка»,
молодший лейтенант

ПРЕВЕНТИВНА ДІЯЛЬНІСТЬ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ СБУ У ПІДРОЗДІЛАХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Умови широкомасштабної збройної агресії російської федерації проти України значно актуалізували завдання посилення внутрішньої безпеки у підрозділах сектору безпеки і оборони.

Одним із ключових суб'єктів, відповідальних за нейтралізацію внутрішніх загроз у військових формуваннях, є військова контррозвідка Служби безпеки України. У межах її повноважень формується комплекс превентивних заходів, спрямованих на виявлення, документування та недопущення проникнення ворожих агентів, деструктивних елементів і осіб, схильних до державної зради, дезертирства, незаконного обігу зброї та вчинення терористичних актів та інших дій, що становлять загрозу національній безпеці.

Ключовим напрямом такої превентивної роботи виступає систематичний контроль і перевірка особового складу, особливо в зонах бойових дій, тилових підрозділах із доступом до стратегічної інформації та під час ротацій. Цей процес не обмежується лише перевіркою анкетних даних чи формальним опитуванням. На практиці йдеться про багаторівневий аналіз поведінкових, інформаційних, комунікаційних і психологічних маркерів, які можуть свідчити про потенційні загрози.

Одним із інструментів сучасної контррозвідувальної діяльності є OSINT – відкритий аналіз джерел інформації, передусім соціальних мереж, публічних месенджерів, форумів, онлайн-відео, а також цифрового сліду, який лишають військовослужбовці. В умовах війни кожен лайк, підписка чи коментар можуть стати сигналом. Моніторинг персональних сторінок військових нерідко дозволяє виявити прояви симпатії до рф, проросійських наративів, підписки на сумнівні

або відверто ворожі ресурси, публікації, що дискредитують командування, підривають довіру до державних інституцій або розпалюють панічні настрої, пости про продаж або купівлю зброї або наркотичних засобів, та інших фактів.

У поєднанні з іншими формами аналітики, OSINT стає інструментом «раннього попередження», який дозволяє «взяти на олівець» потенційно небезпечних осіб ще до того, як вони встигнуть реалізувати злочинні наміри.

Особливої уваги заслуговує конфіденційне співробітництво в самих підрозділах. В умовах війни воно набуває не лише оперативного, а й морального змісту. Мова йде про добровільну передачу інформації щодо осіб, які, до прикладу: висловлюють наміри дезертирства або переходу на бік противника; готують злочини проти бойових побратимів; мають сумнівні контакти з цивільними особами в зоні бойових дій або представниками проросійських структур; висловлюють підтримку ворогу або сумніваються в доцільності оборони країни тощо.

Окремої уваги заслуговують випадки, коли військовослужбовці практикують «трофеювання», розкрадання, незаконне вивезення за межі ЛБЗ вогнепальної зброї. Військовослужбовці, співробітники правоохоронних органів, які проходять службу в підрозділах, де вже зафіксовані підозрілі дії, можуть становити оперативний інтерес як потенційні конфіденти.

В першу чергу, необхідно забезпечити безпеку самого інформатора (конфідента), не допустити його викриття, адже конспіративний обмін інформацією є ключовим аспектом, що забезпечує результативність таких заходів.

Високий рівень конспіративності в межах конфіденційного співробітництва між оперативним співробітником та конфідентом є основою успішної співпраці в рамках негласних заходів та підвищує їх результативність. Використання системи «закладок», кодової мови та захищених месенджерів значно підвищує безпеку обох сторін і дає змогу зберегти конфіденційність навіть за умов підвищеної загрози розкриття та мінімізуючи її ризик як самої співпраці, так і інформації, яка передається.

Реальна ефективність таких заходів значною мірою залежить від навичок та професійної етики військового контррозвідника, якого не можна ототожнювати з каральним органом, що часто роблять військовослужбовці – навпаки, у бойових умовах він повинен виступати гарантом безпеки для всього підрозділу.

Водночас, слід враховувати, що превентивна модель є значно ефективнішою за модель реактивну. Тобто замість реагування на вчинені злочини, діяльність ВКР СБУ має зосереджуватись на виявленні потенційних ризиків до моменту їх реалізації, тобто саме на попереджувальній (профілактичній) роботі. Це вимагає не лише розширення агентурного апарату серед підрозділів, а й впровадження технологічних рішень, аналітичних платформ, а також тісної співпраці з командирами підрозділів, які повинні розуміти логіку і завдання військової контррозвідки, а не боятися чи уникати її присутності.

Контроль і перевірка особового складу в сучасних умовах є не відлунням радянських традицій, а необхідним елементом безпеки бойового підрозділу, який дозволяє зберігати цілісність, боєздатність і довіру між військовослужбовцями, а впровадження як сучасних методик (до прикладу, засобів OSINT), так і покращення давно вивчених (конфіденційного співробітництва) дозволить здійснювати справді якісну профілактичну роботу в підрозділах сектору безпеки та оборони України.

Давиденко Микола,
кандидат юридичних наук,
Національна академія Служби безпеки України

ДО ПИТАННЯ ПОПЕРЕДЖЕННЯ ТЕРОРИСТИЧНИХ ЗАГРОЗ В КОНТЕКСТІ АНТИТЕРОРИСТИЧНОЇ ПІДГОТОВКИ НАСЕЛЕННЯ

На сьогодні терористична загроза значно еволюціонувала: поряд із діяльністю терористичних груп зросла загроза атак терористів – одинаків, які діють автономно, під ідеологічним чи інформаційним впливом, а відсутність чіткої приналежності останніх до конкретних терористичних організацій ускладнює їх ідентифікацію, виявлення і нейтралізацію підготовки терактів, а також розслідування таких діянь.

Згідно чинної Стратегії воєнної безпеки однією із проблем формування стабільного безпекового середовища у контексті воєнної безпеки є поширення міжнародного тероризму та злочинності, загроза розповсюдження зброї масового знищення. А у преамбулі Закону України «Про боротьбу з тероризмом» зазначено, що цей Закон має за мету захист особи, держави і суспільства від тероризму, виявлення та усунення причин і умов, які його породжують, визначає правові та організаційні основи боротьби з цим небезпечним явищем, повноваження і обов'язки органів виконавчої влади, об'єднань громадян і організацій, посадових осіб та окремих громадян у цій сфері, порядок координації їх діяльності, гарантії правового і соціального захисту громадян у зв'язку із участю у боротьбі з тероризмом.

У зв'язку з цим, удосконалення загальнодержавної системи боротьби з тероризмом вимагає пошуку нових методик дослідження і попередження тероризму, прогнозування та моделювання загроз терористичного характеру, виявлення і мінімізації його суспільно небезпечних наслідків. Недосконаліть системи антитерористичного захисту об'єктів можливих терористичних посягань, невирішеність питання щодо дій населення у разі виникнення загрози або скоєння терористичного акту, вчинених, насамперед, у громадських місцях, підвищують вірогідність збільшення кількості можливих жертв, відповідно й соціального резонансу, що може бути використано задля дестабілізації обстановки в суспільстві.

У новій Стратегії розвитку Служби безпеки України на 2025-2030 роки зауважено на впровадженні сучасних підходів до управління кадрами та їх