УДК 355.40+159.922.27
DOI: 10.33663/1563-3349-2019-86-352

В. Є. ГУНІН

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДІЯЛЬНОСТІ РОЗВІДУВАЛЬНИХ ОРГАНІВ У СУЧАСНИХ УМОВАХ ЕСКАЛАЦІЇ ІНФОРМАЦІЙНОГО (ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО) ПРОТИБОРСТВА

Досліджено основні принципи забезпечення безпеки діяльності розвідувального органу, підпорядкованих йому структурних підрозділів та оперативних співробітників. Проаналізовано понятійно-категорійний апарат теорії забезпечення безпеки діяльності оперативних підрозділів. Доведено пряму залежність між рівнем забезпечення безпеки діяльності оперативних підрозділів та особливостями використання можливостей інформаційного простору іноземними спеціальними службами. Досліджено основні характеристики сучасної країни-агресора. Запропоновано зміни і доповнення, які доцільно внести у наявні визначення в умовах загострення інформаційно-психологічного протиборства.

Ключові слова: *адміністративно-поліцейські умови, контррозвідувальний режим, контррозвідувальний орган, інформаційно-психологічний вплив, інформаційний простір, пошукові системи, об'єкт оперативної зацікавленості, конспірація.*

Hunin Valerii. **Security features of the activities of intelligence agencies in modern conditions of escalation of information (information-psychological) confrontation**

The basic principles of ensuring the safety of the activities of the intelligence body, subordinate structural units and operational personnel are investigated. The current conceptual and categorical apparatus of the theory of ensuring the safety of the activities of operational units is analyzed. A direct relationship has been proved between the level of ensuring the security of operations of operational units and the peculiarities of using the capabilities of the information space by foreign special services. Changes and additions are proposed, which are advisable to make to the current definitions in conditions of aggravation of the information-psychological confrontation.

Key words: *administrative and police situation, counterintelligence mode, counterintelligence agency, informational and psychological influence, information space, search engines, object of operational interest, conspiracy.*

© *ГУНІН Валерій Євгенович* – здобувач Воєнно-дипломатичної академії Міністерства оборони України

Під час аналізу змісту гібридної війни, яку Російська Федерація веде проти України, особливу увагу звертає на себе такий її складник, як інформаційна війна. З усією очевидністю можна стверджувати, що саме інформаційна війна відіграє важливу роль у загальній структурі гібридної війні завдяки своєму руйнівному впливу на державні інституції та різні категорії населення.

З огляду на події останніх років можна дійти висновку, що інформаційна (інформаційно-психологічна) війна з боку РФ проти України розпочалася задовго до розв'язання прямої військової агресії, яка в сучасних умовах проводиться противником під прикриттям так званого «народного ополчення», що дало можливість агресору анексувати Крим й окупувати значну територію Донбасу. Основним завданням такої війни є здійснення психологічного впливу на органи влади й управління та різні верстви населення нашої держави. В результаті такого впливу викривляється свідомість пересічних громадян, руйнуються основні людські цінності, підміняється вербальний ряд, на основі якого здійснюється щоденне спілкування, виникають нові ризики та загрози професійній діяльності різних державних суб'єктів, у тому числі правоохоронних та розвідувальних органів. Такий вплив суттєво позначається на якості виконання фахових завдань розвідувальних структур як на території України, так і за її межами. Особливо відчутним цей вплив стає в умовах тотальної інформатизації суспільства.

Для того, щоб організувати адекватну протидію новим ризикам та загрозам, що виникають у сучасному інформаційному просторі, необхідно постійно вдосконалювати систему забезпечення безпеки розвідувальної діяльності. Зокрема, співробітники розвідки мають своєчасно виявляти ці загрози, правильно здійснювати причинно-наслідковий аналіз їх виникнення, оцінювати характер таких загроз, ступінь їх впливу на власну безпеку та безпеку підрозділів розвідувального органу в цілому, вміти визначити наслідки такого впливу, а головне – бути готовими до їх появи.

Результати оцінки загроз у сучасних умовах показують, що найбільшу небезпеку становлять загрози в інформаційній сфері. Йдеться про накопичення інформації особистого характеру сто-

совно співробітників розвідки в різних базах даних, що актуалізує проблему її захисту. Зокрема, відбувається накопичення біографічної інформації та характеризуючих даних, відомостей про особисте життя розвідників, їх зв'язки та контакти з громадянами нашої держави та іноземцями, факти перетину ними державного кордону тощо. Таку інформацію може бути отримано з численних відкритих засобів масової інформації (ЗМІ), інтернет-ресурсів (блогів, соціальних мереж), технічних засобів спостереження (державних та приватних засобів фото-відео фіксації, спеціальних засобів правоохоронних органів). Аналіз процесу обігу такої інформації показує, що вона нікуди не зникає, а завдяки різним спеціальним технічним пристроям накопичується в закритих та відкритих базах даних, обробляється, формується та надалі використовується різними зацікавленими структурами (спецслужбами іноземних держав, недержавними громадськими об'єднаннями, терористичними організаціями).

Значну небезпеку для фахової діяльності співробітників розвідки становить те, що ці бази даних можуть використовувати не тільки державні структури, а й різні приватні організації (переважно неконтрольовані державою), що діють на території України під прикриттям і працюють в інтересах спецслужб іноземних держав. Професійні фахівці (хакери), що проникають до відкритих баз даних й отримують спеціальну службову інформацію та особисті дані із закритих джерел, дають можливість будь-якій приватній структурі (зокрема, кримінальній) зібрати достатньо відомостей про об'єкт, який їх цікавить (фізичну або юридичну особу), ідентифікувати цей об'єкт, а завдяки різним технічним засобам – візуалізувати й розшукати особу, на яку надалі чинитимуть вплив[1]. Можна стверджувати, що в умовах швидкого розвитку інформаційних технологій немає належної гарантії захисту закритої інформації про особисті дані співробітників розвідки.

Особливості використання пошукових систем суттєво впливають на якість, ефективність та своєчасність виконання розвідниками фахових завдань. Унаслідок використання сучасних пошукових систем створюються певні передумови для викриття іноземними правоохоронними органами та недержавними організаціями співробітників розвідки під час виконання ними про-

фесійних завдань за кордоном і в районі проведення операції об'єднаних сил (ООС). Зокрема, інформаційний простір будь-якої іноземної держави дає можливість її правоохоронним органам за короткий проміжок часу виявити та встановити ту особу, яка може бути причетною до діяльності розвідки іншої країни.

Результати аналізу сучасних подій у світі, пов'язаних із викриттям протиправних дій співробітників ГУ ГШ (Головного управління Генерального штабу) Збройних сил РФ за кордоном, підтверджують те, що російські розвідники нехтували правилами дотримання власної безпеки, виконуючи завдання за кордоном. Зокрема, вони не врахували можливості пошукових систем розвідуваної держави, не звернули увагу на численні державні та приватні бази даних та різні технічні засоби фіксації інформації, що зрештою призвело до їх ідентифікації та викриття контррозвідувальними органами (КРО)[2]. Якщо ж співробітник розвідки здатен своєчасно оцінити такі загрози, він може правильно зреагувати на них та організувати адекватну протидію ще на етапі підготовки до виконання завдань розвідувального органу, а також буде готовий реагувати на подібні загрози вже в процесі виконання професійних завдань.

Концептуальні засади сучасної агентурної розвідки описано О. Іващенком, В. Курдюком, А. Огарком[3]. Змістовно розкрито сучасні агентурні технології, які використовують спецслужби провідних іноземних держав, в монографії О. Ворони[4]. Основні принципи забезпечення безпеки співробітників правоохоронних та розвідувальних органів під час виконання заходів оперативно-розшукової діяльності викладено низкою авторів, серед яких І. Татарчук, Т. Дякін[5]. Проте на сучасному етапі недостатньо досліджено особливості діяльності оперативних підрозділів розвідки в умовах загострення інформаційно-психологічного протиборства, неврахування яких негативно впливає на систему забезпечення безпеки діяльності оперативних співробітників розвідувального органу[6]. Передусім це стосується особливостей використання пошукових систем та баз даних на шкоду діяльності розвідувальних підрозділів у сучасних умовах.

Безпека співробітника розвідки в контексті посилення сучасних викликів та загроз є одним з елементів системи забезпечення безпеки розвідувального органу, яка є складовою загаль-

ної системи забезпечення безпеки нашої держави. Ця загальна система складається із взаємодіючих елементів, які повністю залежать один від одного. Забезпечення безпеки співробітників розвідки – це процес злагодженої роботи всіх підрозділів, служб і департаментів розвідувального органу. Насамперед це стосується підрозділів, які здійснюють відбір, перевірку, подальшу підготовку співробітників розвідки та укомплектування ними своїх підрозділів.

Ефективність функціонування системи забезпечення безпеки сил та засобів розвідки залежить від того, чи правильно її побудовано та як вона працює у взаємодії з іншими елементами загальної системи забезпечення безпеки держави. Слід зазначити, що система забезпечення безпеки співробітників розвідувального органу складається з комплексу спеціальних заходів, яких повинен дотримуватися кожен співробітник та які залежать від багатьох факторів, що впливають на злагодженість взаємодії підрозділів розвідувального органу. Дотримання співробітником розвідки цього комплексу заходів забезпечуватиме своєчасне виявлення нових ризиків та загроз, що виникають в інформаційному просторі та негативно впливають на його діяльність, а також деформують загальну систему безпеки розвідувального органу. Тому співробітник розвідки має усвідомити, що попередження таких загроз залежить від процесу забезпечення безпеки кожного розвідника та структурних підрозділів у цілому[7].

Для того, щоб визначити нові шляхи вдосконалення системи забезпечення безпеки розвідувального органу, насамперед необхідно з'ясувати, якими є нові загрози, як можна їх класифікувати та яке місце вони займають в умовах інформаційно-психологічного протиборства. Нові зовнішні загрози, спрямовані проти діяльності розвідувального органу, – це насамперед загрози, що виникають внаслідок динамічних змін сучасного інформаційного середовища. Такі загрози пов'язані зі змінами порядку доступу до відкритих або закритих баз даних. Їх джерелами, як правило, виступають державні та недержавні структури (адміністративно-поліцейські, контррозвідувальні органи та організації, що співпрацюють з ними, зокрема опозиційні партії, радикальні або терористичні угрупування). Сюди ж слід віднести загрози, що виникають у процесі впливу окремих осіб

(агентів-провокаторів, хакерів або сторонніх осіб, що сприяють роботі правоохоронних органів). Такі загрози суттєво впливають як на загальні процеси забезпечення безпеки всередині структурних підрозділів розвідувального органу, так і на безпеку окремих співробітників.

Основними зовнішніми загрозами, що виникають внаслідок змін сучасного інформаційного простору, є:

– можливий витік інформації в процесі підбору та підготовки співробітників розвідки (брак фахівців, що забезпечують надійність збереження особистих даних);

– перехід співробітників розвідки в інші організації та відомства з більш комфортними умовами праці (відомості й дані щодо співробітників розвідки потрапляють до суміжних організацій);

– вивчення іноземними державними органами та недержавними організаціями через інформаційний простір структури розвідувального органу та його окремих співробітників ще у процесі їх підготовки до виконання фахових завдань на території України або за кордоном;

– постійне використання іноземними КРО інформаційного простору для здійснення психологічного тиску на співробітників розвідки під час виконання ними фахових завдань за кордоном або на розвідуваній території (на підставі отриманої правоохоронними органами або недержавними організаціями інформації щодо співробітника розвідки, яка була недостатньо прихованою та зберігалася в різних базах даних);

– посилення контррозвідувального режиму (КРР) в іноземній країні завдяки використанню можливостей інформаційного простору (пропаганда боротьби з радикально налаштованими (терористичними) організаціями, заохочення різних зацікавлених верств населення тощо) для ускладнення повсякденної діяльності співробітника розвідки, який знаходиться на її території на посаді прикриття.

З огляду на вищеперераховані основні зовнішні загрози можна стверджувати, що захищеність діяльності структурних підрозділів та окремих співробітників розвідувального органу від негативного впливу такого зовнішнього середовища повністю залежить від їх здатності своєчасно реагувати на них або заз-

далегідь пристосовуватися до таких загроз, які існують в тій чи іншій іноземній країні (на розвідуваній території) і які можуть лише опосередковано негативно впливати на діяльність співробітника розвідки.

Окрім зовнішніх загроз безпеці розвідувального органу, велику небезпеку становлять внутрішні загрози, які виникають в результаті навмисних, ненавмисних або необачних дій співробітників розвідки під час виконання фахових завдань в іноземній країні (на розвідуваній території). Фіксація такої поведінки різними технічними засобами (елементами інформаційного простору), накопичення цієї інформації та її аналіз правоохоронними органами або недержавними організаціями в результаті дає підстави КРО зацікавитися особою співробітника розвідки, який працює під прикриттям, і у подальшому поступово викрити та довести його причетність до розвідувального органу. Такі загрози залежать від особливостей поведінки розвідника, легендування своєї діяльності, дотримання умов конспірації та службової дисципліни. Безперечно, зазначені дії негативно впливають не тільки на безпеку співробітника розвідки, а й на безпеку окремих структурних підрозділів розвідувального органу.

Причинами виникнення таких загроз є:

– недостатньо ефективна організація системи управління персоналом розвідувального органу;

– професійні помилки в процесі планування та підбору кадрів;

– недостатня якість підбору кандидатів на посади в розвідувальний орган (передусім, це стосується оперативних посад);

– недосконала організація системи навчання особового складу розвідки;

– недостатня мотивація співробітників розвідки;

– недосконала організація підготовки несправжніх імітаційних засобів (НІЗ), зокрема документів прикриття;

– низький рівень якості легендування співробітників розвідки на посадах прикриття;

– недостатній рівень фахової (спеціальної) підготовки співробітників перед відрядженням за кордон (на розвідувану територію);

– недотримання окремими співробітниками розвідки умов конспірації та оперативної дисципліни в процесі повсякденної діяльності.

Внаслідок впливу зовнішніх та внутрішніх загроз на діяльність будь-якого окремо взятого державного органу відбувається так звана деформація системи забезпечення безпеки держави в цілому, що може поступово привести до деформації інших складових загальної системи національної безпеки. Таким чином деформується система забезпечення безпеки діяльності розвідувального органу, підпорядкованих йому підрозділів та співробітників розвідки. Зокрема, відбувається деформація порядку дотримання та застосування тих заходів безпеки, який існував і успішно використовувався розвідувальними підрозділами та співробітниками розвідки до сьогодення. В результаті такої деформації суттєво знижуються якість та ефективність виконання суб'єктами розвідки фахових завдань.

З огляду на викладене можна зазначити, що деформацією (спотворенням) системи забезпечення безпеки діяльності розвідувальних підрозділів та співробітників розвідки слід вважати процес настання незворотних змін негативного характеру внаслідок інформаційно-психологічного впливу воєнного противника. В результаті суттєво знижується якість та ефективність виконання фахових завдань розвідувальними підрозділами, відбувається розрив зв'язків між окремими елементами цієї системи, порушується порядок взаємодії між системами забезпечення безпеки діяльності державних органів у цілому.

З огляду на запропоноване визначення поняття деформації системи забезпечення безпеки діяльності розвідувальних підрозділів можна виділити три її основних види.

Горизонтальна деформація – результат впливу зовнішніх та внутрішніх загроз на діяльність окремих співробітників розвідки, завдяки чому відбуваються вимушені (навмисні), ненавмисні або необачні (несвідомі) порушення з їхнього боку особистих заходів безпеки під час виконання фахових завдань, в результаті чого завдається певна шкода системі забезпечення безпеки діяльності одного окремого розвідувального підрозділу (який представляють ці співробітники) або навіть усій системі забез-

печення безпеки діяльності розвідувального органу як основного виконавця таких завдань.

Вертикальна деформація – результат впливу зовнішніх та внутрішніх загроз на діяльність державних органів, задіяних у проведенні єдиного в інтересах країни заходу, що призводить до руйнації порядку взаємодії між цими органами і завдає шкоди їх систем забезпечення безпеки, у тому числі системі забезпечення безпеки діяльності розвідувального органу як державної інституції.

Об'ємна деформація – результат впливу зовнішніх та внутрішніх загроз на діяльність усіх державних органів у тому чи іншому обсязі, що в цілому приводить до руйнації системи забезпечення безпеки нашої держави.

Щодо можливих шляхів у удосконалення системи забезпечення безпеки розвідувального органу. Для вдосконалення системи забезпечення безпеки діяльності підрозділів та співробітників розвідки, попередження та усунення зазначених деформаційних процесів необхідно посилювати не тільки можливості підрозділу власної безпеки розвідувального органу, не тільки дотримуватися всіма співробітниками розвідки рекомендованих заходів безпеки, а й насамперед керівникам структурних підрозділів потрібно налагодити комплексну роботу з організації контролю за їх дотриманням на всіх рівнях управлінської ланки.

Для забезпечення високої ефективності функціонування системи безпеки діяльності співробітників розвідувального органу керівникам усіх рівнів управління необхідно зосередити увагу на якості виконання таких заходів:

– планування та всебічний контроль за результатами реалізації заходів щодо забезпечення безпеки співробітників у процесі виконання фахових завдань;

– планування та контроль усіх заходів щодо пошуку, прийому, адаптації, навчання та закриття співробітників розвідки від сторонніх осіб;

– ведення на належному рівні службового діловодства в підрозділах розвідки з урахуванням усіх вимог безпеки інтелектуальної власності розвідувального органу та його співробітників;

– впровадження в усі підрозділи оптимальних інформаційних технологій, що дасть можливість забезпечити макси-

мальний рівень захисту в сфері безпеки та передачі інформації;

– організація злагоджених дій керівників розвідувальних підрозділів усіх рівнів щодо забезпечення безпеки співробітників розвідки.

Для якісного проведення зазначених заходів необхідно:

– постійно та своєчасно виявляти нові, реальні та прогнозувати можливі потенційні небезпеки та загрози;

– знаходити ефективніші способи запобігання таким загрозам, ослаблення або ліквідації наслідків їх впливу;

– знаходити різні можливості та запроваджувати нові способи закриття та легендування відокремлених від розвідувального органу структурних оперативних підрозділів та їх співробітників;

– організувати більш ефективну та якісну взаємодію з правоохоронними та державними органами із закриття співробітників розвідки, що діють під прикриттям;

– оформляти відповідні документи (НІЗ) з метою запобігання негативним впливам, що перешкоджають роботі розвідувального органу;

– постійно вдосконалювати роботу підрозділів власної безпеки з огляду на виявлені нові небезпеки та загрози.

Підвищення ефективності системи забезпечення безпеки діяльності співробітників та об'єктів розвідувального відомства доцільно реалізовувати так:

– організація – побудова досконалої системи забезпечення безпеки співробітників структурних підрозділів розвідувального органу. Побудова такої системи відбувається шляхом організаційного проектування посад прикриття, в процесі якого визначаються кількісний та функціональний склад підрозділів, посадові обов'язки персоналу, що працює під прикриттям, формується система їх зв'язків для ефективної взаємодії організаційних елементів, а за необхідності здійснюється максимально глибоке закриття співробітників, оформляється для них весь пакет НІЗ, враховуючи наявну відкриту інформацію щодо них у пошукових системах та базах даних;

– планування – розв'язання двох принципових питань: яку мету планується досягти в процесі вдосконалення заходів

із забезпечення безпеки співробітника розвідки і як її можна досягти з огляду на сучасні умови агентурно-оперативної обстановки (АОО) в іноземній країні (на розвідуваній території), де розвідник планує виконувати фахові завдання;

– аналіз – вибір одного з можливих варіантів виконання фахових завдань на підставі виявлення зовнішніх загроз з боку адміністративно-поліцейських та контррозвідувальних органів, що діють у тому ж інформаційному просторі;

– контролья та регулювання – виявлення та усунення недоліків у процесі функціонування системи забезпечення безпеки співробітників й об'єктів розвідувального органу; пошук форм і засобів їх захисту від можливих негативних наслідків, постійний моніторинг діяльності структурних підрозділів та співробітників для своєчасного їх захисту та локалізації провалів.

Результати аналізу сучасних загроз в умовах інформаційно-психологічного протиборства свідчать, що під час виконання фахових завдань співробітнику розвідки особливу увагу необхідно зосереджувати передусім на тих загрозах, які виникають внаслідок використання сучасних пошукових систем іноземними КРО, правоохоронними органами, різними державними та недержавними організаціями, що діють у сучасному інформаційному просторі. Для того, щоб вдосконалити систему забезпечення безпеки діяльності співробітника розвідки та розвідувального органу в цілому під час підготовки та виконання фахових завдань за кордоном (на розвідуваній території), необхідно зважати на зміст накопиченої в базах даних інформації, що не відповідає легендам прикриття задіяних у проведенні заходу співробітників та підрозділів розвідувального органу, і може стати підставою для їх викриття.

1. Locating The Netherlands Most Wanted Criminal By Scrutinising Instagram. URL: http://bellingcat.com/materialy/casestudies/2019/04/05/holland-most-wanted. **2.** Scripal Suspects Confirmed as GRU Operatives: Priorr European Operations disclosed. URL: http://bellingcat.com/news/uk-and-europe/2018/09/20/ scripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/. **3.** Іващенко О., Курдюк В., Огарок А. Концептуальні засади адаптації розвідки Збройних Сил України відповідно до стандартів НАТО. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 2(35). С. 3-38. **4.** Ворона О. Сучасні агентурні технології:

світовий досвід: монографія. Київ: МО України. 2016. 498 с. **5.** Татарчук І., Дякін Т. Оперативно-розшукова діяльність: навч. посіб. Київ: Центр учбової літератури. 2014. 212 с. **6.** Україна-2018: дорога між викликами й ризиками. Але дорога... *Дзеркало тижня*. 2017. № 49–5. С. 1–3. **7.** Татарчук І., Дякін Т. Цит. праця.

References

1. Locating The Netherlands Most Wanted Criminal By Scrutinising Instagram. URL:http://bellingcat.com/materialy/casestudies/2019/04/05/holland-most-wanted. **2.** Scripal Suspects Confirmed as GRU Operatives: Priorr European Operations disclosed. URL: http://bellingcat.com/news/uk-and-europe/2018/09/20/ scripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/. **3.** Ivashchenko O., Kurdyuk V., Ogarok A. Conceptual bases for the adaptation of Ukraine's Armed Forces to NATO standards. *Science and Technology of the Air Force of the Armed Forces of Ukraine*. 2019. No. 2 (35). P. 3-38. **4.** Vorona O. Modern Agent Technologies: World Experience: Monograph. Kyiv: Ministry of Defense of Ukraine, 2016. 498 p. **5.** Tatarchuk I., Dyakin T. Operational search activity: Tutorial. Kyiv: Center for Educational Literature, 2014. 212 p. **6.** Ukraine 2018: The Road Between Challenges and Risks. But the road ... *The mirror of the week*. 2017. № 49–5. Pp. 1–3. **7.** Tatarchuk I., Dyakin T. Op. labor.

Hunin Valerii. **Security features of the activities of intelligence agencies in modern conditions of escalation of information (information-psychological) confrontation**

The main components of the hybrid war that the Russian Federation is waging against Ukraine are examined, among which special attention is paid to the information war, which plays an important role in the structure of the hybrid war due to its destructive influence on state institutions and various categories of the country's population, which is experiencing aggression. It is certain that during the information war the aggressor country forms such an information space in the country and its environment that has suffered from aggression, due to which the consciousness of ordinary citizens is distorted, basic human values are destroyed, the verbal line is replaced, on the basis of which daily communication is carried out, new risks arise and threats to the professional activities of various government entities, including law enforcement and intelligence agencies, which significantly affects the quality of ve fulfilling their professional tasks. It is proved that in order to organize adequate counteraction to new risks and threats that arise in the modern information space, it is necessary to constantly and simultaneously improve the existing security systems for the activities of all state bodies, including the intelligence agency. To this end, the threats existing in the current conditions are analyzed and it is proved that the greatest danger among them is represented by threats in the information sphere. In particular, we are talking about the accumulation of personal information regarding government officials, including intelligence officers, in different databases, which actualizes the problem of its protection. It is clear that a significant danger to the professional activities of intelligence

officers is that these databases can be used not only by government agencies, but also by various private organizations (mainly uncontrolled by the state) that operate under the cover of Ukraine and work in the interests of foreign intelligence services. It has been investigated that the use of the existing modern search engines by the indicated structures significantly affects the quality, effectiveness and timeliness of scouts to complete professional tasks. It is certain that due to the influence of external and internal threats on the activities of any individual state body, the so-called deformation of the current state security system as a whole occurs, as well as the security systems for the activities of all state bodies, including the intelligence body, subordinate units and employees, are deformed intelligence. It is proved that as a result of the informational-psychological influence (informational aggression) from the military adversary, the noted deformation processes lead to irreversible negative changes in society, which significantly reduce the quality indicators and the effectiveness of the intelligence units in fulfilling professional tasks, there is a disconnection between the individual elements of the security system activities of the intelligence agency, the current order of interaction between dr coal safety systems for the activities of state bodies as a whole. Changes and additions that are advisable to make in the existing security system of the intelligence agency to improve the level of performance indicators and the quality of intelligence tasks are proposed.

Key words: administrative and police situation, counterintelligence mode, counterintelligence agency, informational and psychological influence, information space, search engines, object of operational interest, conspiracy.