УДК 355.402

КРАВЧЕНКО Р.М., *кандидат юридичних наук*

ЩОДО ДЕЯКИХ ПІДХОДІВ ДО ВДОСКОНАЛЕННЯ КОНТРРОЗВІДУВАЛЬНОГО ПОШУКУ ОРГАНІВ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ СБ УКРАЇНИ З УРАХУВАННЯМ АНАЛІЗУ ЗАКОНОДАВСТВА США

Анотація. *У статті проведено аналіз окремих нормативно-правових актів, що регулюють суспільні відносини в сфері контррозвідувального забезпечення Армії США, з метою виявлення правових рішень, які можуть бути адаптовані до національного законодавства в інтересах підвищення ефективності контррозвідувального пошуку органів військової контррозвідки СБУ.*

Ключові слова: *контррозвідувальне забезпечення, військова контррозвідка, структура, повноваження, розслідування, збройні сили США, контррозвідувальний пошук, контррозвідувальна обізнаність, інструктаж.*

Summary. *The article analyzes individual legal acts regulating public relations in the field of counterintelligence provision of the US Army in order to identify legal solutions that can be adapted to national legislation in order to increase the effectiveness of the counterintelligence search of the SSU military counterintelligence units.*

Keywords: *counterintelligence support, military counterintelligence, structure, authority, investigation, US armed forces, counterintelligence search, counterintelligence awareness, instruction.*

Аннотация. *В статье проведен анализ отдельных нормативно-правовых актов, которые регулируют общественное отношения в сфере контрразведывательного обеспечения Армии США, с целью выявления правовых решений, которые могут быть адаптированы к национальному законодательству в интересах повышения эффективности контрразведывательного поиска органов военной контрразведки СБУ.*

Ключевые слова: *контрразведывательное обеспечение, военная контрразведка, структура, полномочия, расследование, вооруженные силы США, контрразведывательный поиск, контрразведывательная осведомленность, інструктаж.*

Постановка проблеми. Згідно із Законом України “Про контррозвідувальну діяльність”, Службі безпеки України надано право здійснювати контррозвідувальний пошук з використанням гласних контррозвідувальних заходів, які передбачають використання відкритих (офіційних) форм і методів роботи у сфері забезпечення державної безпеки, та негласних контррозвідувальних заходів, які здійснюються із залучення осіб, які конфіденційно співпрацюють з контррозвідувальними органами і підрозділами, а також з використанням оперативних, оперативно-технічних та спеціальних сил і засобів [1].

Контррозвідувальний пошук є невід’ємною складовою контррозвідувальної діяльності, в ході якої виявляються ознаки зовнішніх та внутрішніх загроз безпеці України тоді, коли ще не встановлено причетність до них конкретних осіб [2]. Одним зі способів підвищення ефективності контррозвідувального пошуку органів військової контррозвідки (далі – ВКР) СБ України є створення нових можливостей добування інформації про ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб,

спрямованої проти Збройних Сил України. Правові норми законодавств іноземних країн, що регулюють контррозвідувальний захист військових формувань, містять приклади вдалого вирішення цього завдання.

Результати аналізу наукових публікацій. Питання вдосконалення законодавчих основ здійснення контррозвідувальної діяльності в сучасному правовому суспільстві, в тому числі з урахуванням іноземного досвіду, постійно знаходяться в полі зору вітчизняних науковців і практиків. С.С. Кудінов, досліджуючи питання правового регулювання забезпечення СБ України антитерористичної безпеки, довів потребу підготовки населення до виявлення ознак терористичної діяльності та вдосконалення правового регулювання запобігання тероризму, як основоположний складник профілактики тероризму в Україні, що має знайти відображення у відповідних законодавчих та підзаконних нормативно-правових актах [3].

І.В. Авдошин, аналізуючи шляхи оптимізації контррозвідувальної системи США з попередження загроз підривного характеру, констатував, що зміна парадигми протидії розвідувально-підривним загрозам супроводжувалася прийняттям низки законів і інструкцій, уніфікацією вимог, підходів і процедури в сфері контррозвідувальної діяльності [4].

Сучасний стан правового регулювання контррозвідувального пізнання, як важливої складової контррозвідувальної діяльності, вивчав А.В. Ватраль і дійшов висновку, що усунення прогалин правового регулювання пізнавального процесу у контррозвідці є запорукою успішного вирішення завдань у сфері забезпечення державної безпеки України [5].

Водночас слід зазначити, що дослідження питань вдосконалення законодавчого врегулювання контррозвідувального пошуку, що здійснюється в межах контррозвідувального забезпечення Збройних Сил та інших військових формувань, створених відповідно до законодавства України, наразі не проводилося.

Метою статті є аналіз окремих нормативно-правових актів, що регулюють суспільні відносини в сфері контррозвідувального забезпечення Армії США, з метою виявлення правових рішень, які можуть бути адаптовані до національного законодавства в інтересах підвищення ефективності контррозвідувального пошуку органів військової контррозвідки СБУ.

Виклад основного матеріалу. Аналіз іноземних нормативно-правових актів свідчить про наявність прикладів суттєвого розширення можливостей отримання органами військової контррозвідки інформації, що належить до їх компетенції, за рахунок правового закріплення обов'язку кожного військовослужбовця, працівника та найманого співробітника збройних сил проходити контррозвідувальні інструктажі й навчання, а також повідомляти відповідним підрозділам ВКР інформацію про факти та ознаки розвідувальної, терористичної та іншої підривної діяльності. При цьому такий обов'язок підкріплюється функцією командирів всіх рівнів здійснювати контроль за його виконанням, а також можливістю настання для порушників правових наслідків у вигляді адміністративної та дисциплінарної відповідальності. Таким чином, в результаті реалізації вказаного механізму забезпечується систематичний профілактичний вплив на весь особовий склад збройних сил, а кожний його представник в обов'язковому порядку стає джерелом надходження контррозвідувальної інформації.

"Програма контррозвідувальної обізнаності та інструктажу", яка була введена в дію Інструкцією Департаменту оборони США № 5240.6, вперше ввела в обіг термін "контррозвідувальна обізнаність" (Counterintelligence Awareness) [6]. Зі змісту цієї Програми вбачається, що контррозвідувальна обізнаність передбачає, по-перше,

проведення підрозділами, що виконують функції військової контррозвідки в Департаменті Оборони та Армії США, інструктажів всього особового складу, а також суб'єктів господарювання, які виконують роботи чи надають послуги оборонного характеру, з метою доведення інформації про загрози в сфері протидії іноземній розвідувальній і терористичній діяльності, а по-друге обов'язок військовослужбовців та працівників надавати до вказаних підрозділів передбачену інструктажами інформацію.

Безпосереднє формулювання терміна "контррозвідувальна обізнаність" містить Директива Департаменту оборони № 5240.06, яка визначає її як рівень усвідомлення особою інформації про загрози, методи та ознаки діяльності іноземних розвідувальних служб, а також вимоги доповідати про таку інформацію [7].

Інструкція № 5240.6 встановлює, що військовослужбовці дійсної служби та резерву, а також цивільні працівники Армії США повинні доповідати командуванню та до органів військової контррозвідки інформацію про всі контакти та події, які можуть становити загрозу особовому складу, майну, таємній та чутливій інформації. Суб'єкти господарської діяльності, що виконують контракти в сфері оборони, також зобов'язані повідомляти таку інформацію до ФБР або Служби розслідувань Департаменту оборони.

Весь особовий склад Армії повинен проходити періодичні інструктажі стосовно загроз з боку іноземних спецслужб, іноземних підприємницьких структур, терористичних організацій, незаконного втручання в роботу комп'ютерів та розголошення інформації. В межах цих інструктажів доводиться інформація стосовно іноземних розвідувальних служб, цілей їхньої діяльності, методів проведення розвідувальних операцій, кадрових співробітників, способів підтримання зв'язку, фінансування, міжнародного тероризму та споріднених загроз безпеці особового складу, майну збройних сил та інформації військового характеру.

Особовий склад Армії повинен надавати (усно чи письмово) до органів військової контррозвідки інформацію стосовно власних контактів (у формі зустрічей, особистого спілкування, з використанням радіо-, телефонного зв'язку, листування, чи в інший спосіб, незалежно від того, хто започаткував контакт, а також його соціальної, офіційної чи приватної основи) з особами (незалежно від громадянства), які пропонували: співробітництво з іноземною спецслужбою чи терористичною організацією з метою участі у проведенні ними розвідувальної діяльності, надання несанкціонованого доступу до таємної чи іншої інформації з обмеженим доступом; з встановленими чи ймовірними співробітниками розвідки будь-якої країни; з членами іноземних дипломатичних представництв в будь-якій країні на офіційній чи приватній основі. Також підлягає доповіді інформація про діяльність, що стосується шпигунства, тероризму, незаконної передачі технологій, саботажу, антиурядової агітації, диверсії, зради, розголошення таємної чи нетаємної контрольованої інформації, несанкціонованого втручання в автоматизовані інформаційні системи.

В разі невиконання вказаних вимог, до винних осіб можуть бути застосовані норми, які передбачають юридичну та/або адміністративну відповідальність згідно з Кодексом військової юстиції.

За результатами аналізу повідомлень, що надійшли від особового складу, щорічно органами військової контррозвідки здійснюється аналіз та узагальнення інформації за наступними категоріями:

Категорія І. Доповіді про контакти чи запити інформації, причетність до яких іноземної розвідувальної служби підтверджена.

Категорія ІІ. Доповіді про контакти чи запити інформації, причетність до яких іноземної розвідувальної служби є ймовірною (імовірність грунтується на даних про

прізвище особи, яка встановила контакт, зовнішній опис, застосовані методи, характер інформації, до якої проявлений інтерес).

Категорія III. Доповіді про намагання отримати таємну чи іншу інформацію з обмеженим доступом поза офіційними каналами чи встановленими процедурами, причетність до яких іноземної розвідувальної служби є малоймовірною.

Категорія V. Доповіді про міжнародні чи внутрішньодержавні терористичні групи чи окремих терористів, які становлять загрозу особовому складу та майну збройних сил.

Категорія VI. Доповіді про навмисну компрометацію таємної інформації військовослужбовцями чи працівниками збройних сил, а також її передачу стороннім особам.

Інформація, отримана за вказаними категоріями підлягає обліку для забезпечення контролю та оцінки ефективності реалізації Програми, в тому числі проведених на підставі неї контррозвідувальних розслідувань та операцій. Результати аналізу та узагальнення річних підсумків реалізації програми повинні доповідатися керівництву Контррозвідки Армії.

Як бачимо, отримана в порядку виконання Інструкції № 5240.6 інформація складає ґрунтовну і, що найважливіше, достатньо об’єктивну сукупність емпіричних даних для проведення контррозвідувального аналізу. При цьому Директива Департаменту оборони № 5240.02 визначає, що контррозвідувальний аналіз – це процес вивчення та оцінки інформації, спрямований на визначення природи, функцій, взаємозв’язків, учасників та намірів, що стосуються можливостей іноземних розвідувальних служб [8].

Іншим нормативно-правовим актом, який передбачає участь усього особового складу Армії США у своєчасному виявленні та попередженні розвідувально-підривної діяльності, є Інструкція № 381-12 “Диверсія та шпигунство, спрямовані проти Армії США” [9]. Цим документом регламентується проведення контррозвідувальних тренувань, а також встановлюються обов’язки командирів щодо контролю за виконанням вимог Інструкції підлеглими. Дається визначення, що контррозвідувальний пошук – це систематичне отримання інформації, що стосується шпигунства, саботажу, тероризму та споріднених видів діяльності, що здійснюються іноземними державами, організаціями чи особами і спрямовані проти інтересів оборони.

Згідно з Інструкцією, діючі військовослужбовці Армії, Національної гвардії, Резервної армії США, цивільний персонал, працівники суб’єктів господарювання, які виконують контракти оборонного призначення, та наймані іноземні працівники підрозділів та установ Армії США за кордоном повинні проходити контррозвідувальне тренування принаймні один раз на рік. Зміст тренування може варіюватись у залежності від категорії осіб, з якими він проводиться, та географічного положення, в умовах якого відбувається несення військової служби. В ході тренування може використовуватись нетаємна інформація для широкої аудиторії, а також таємні відомості для визначених категорій осіб.

Тренування повинно містити наступні складові:

1) Доведення, що іноземні розвідувальні служби вважають особовий склад Армії цінним джерелом таємної і чутливої інформації. Пояснення про те, як це стосується підрозділу чи виду діяльності, до якої мають відношення учасники тренування;

2) Роз’яснення видів кримінального покарання за шпигунство, передбачених Кодексом США та Об’єднаним кодексом Військової юстиції; наведення прикладів засудження осіб за шпигунство, призначених покарань, у тому числі допустимості смертної кари;

3) Розкриття, зокрема, на конкретних прикладах, методів і технік, які застосовуються іноземними розвідками для втягування осіб у залежність, збирання інформації про спроможності, бойове застосування, особовий склад і технології; специфіка підходів під "чужим прапором";

4) Види ситуацій (обставин) про які необхідно доповідати та ознаки шпигунства;

5) Характер збитків, які можуть бути завдані внаслідок шпигунства;

6) Попередження про дисциплінарну відповідальність, яка може бути застосована до особи в разі недотримання вимог Інструкції;

7) Доведення порядку надання доповіді про виявлені факти і ознаки;

8) Роз'яснення загроз внутрішнього та міжнародного тероризму щодо особового складу та членів родин, методи попередження та уникнення шкідливих наслідків;

9) Визначення розвідувальних загроз, які можуть становити недержавні розвідувальні служби та організації, що здійснюють міжнародний наркотрафік.

Інструкція визначає категорії інформації або ситуацій, які потребують доповіді:

1) Спроби неуповноважених осіб отримати таємну чи нетаємну інформацію щодо спроможностей, персоналу, діяльності, технологій збройних сил шляхом опитування, вивідування, введення в оману, підкупу, погроз, шантажування, фотографування, спостереження, збирання документів чи матеріалів, проникнення до комп'ютерів;

2) Відомі, підозрілі чи ймовірні шпигунські дії представника особового складу Армії США;

3) Контакти військовослужбовців та працівників збройних сил або членів їх родин з особами, підозрюваними у причетності до іноземних спецслужб чи терористичних організацій;

4) Контакти представників особового складу Армії з будь-якими іноземними громадянами, якщо вони виявляють надмірне володіння інформацією чи невиправданий інтерес до представників особового складу Армії або їх обов'язків, американських технологій, досліджень, випробувань, систем озброєння чи наукової інформації; намагаються отримати таємну чи нетаємну інформацію; створити умови залежності представника особового складу Армії США через особливе ставлення, надання переваг, подарунків, грошей чи в інший спосіб; започатковують будь-які підприємницькі відносини, що виходять за межі їх офіційних обов'язків;

5) Випадки, коли під час перебування за кордоном військовослужбовцям або членам їх родин пропонують розповісти про свої службові обов'язки, надати інформацію військового характеру, розпочати співробітництво з іноземним урядом чи розвідкою із застосуванням погроз або тиску будь-якого характеру;

6) Інформація стосовно буд-якої внутрішньодержавної чи міжнародної терористичної діяльності чи саботажу, незаконної передачі за кордон американських технологій;

7) Відомі або ймовірні факти зради з боку військовослужбовців Армії США, заклики до захоплення державної влади неконституційним шляхом;

8) Відомі або ймовірні факти несанкціонованого втручання у військові таємні або нетаємні автоматизовані інформаційні системи;

9) Використання родичів, що мешкають за кордоном з метою здійснення впливу чи тиску на військовослужбовців Армії США;

10) Виявлення в приміщеннях, де запроваджені заходи безпеки, підозрілих підслуховуючих пристроїв чи інших засобів технічного спостереження;

11) Безпідставна відсутність за місцем служби (роботи) військовослужбовців, які мали доступ до інформації з обмеженим доступом, криптографічних даних;

12) Самогубства чи спроби покінчити з життям з боку військовослужбовців, які протягом останнього року мали доступ до інформації з обмеженим доступом;

13) Порушення заходів комп'ютерної безпеки;

14) Факти та наміри військовослужбовців, працівників збройних сил здійснити перехід на бік ворога в період воєнного стану або в умовах збройного конфлікту.

Також Інструкція вимагає надання доповідей у разі виявлення ознак шпигунства:

1) Будь-які спроби отримати розширений доступ до таємної інформації шляхом наполегливого намагання зайняти відповідну посаду чи виконання обов'язків понад встановлений обсяг, а також спроби ознайомитися з відомостями, що виходять за межі наданого доступу;

2) Безпідставне переміщення таємних матеріалів з робочого місця, або їх зберігання в особистому автотранспорті та за місцем мешкання;

3) Використання копіювальної, факсимільної або комп'ютерної техніки для розмноження чи передачі таємних матеріалів, що не пов'язано зі службовою необхідністю;

4) Повторне і не викликане потребою залишення на роботі понад норми робочого часу, особливо наодинці;

5) Підписання документів про анулювання таємних матеріалів без фактичної присутності при їх знищенні;

6) Занесення засобів реєстрації інформації (відеокамер, записуючих пристроїв, комп'ютерів чи модемів) у приміщення, де зберігається, обробляється чи обговорюється таємна інформація;

7) Немотивоване різке покращення майнового стану (придбання нерухомості, транспортних засобів, коштовного відпочинку, покриття великих боргів, кредитів), намагання пояснити це отриманням спадку, виграшом, прибутковим бізнесом;

8) Відкриття декількох банківських рахунків зі значними сумами коштів, без об'єктивного пояснення їх походження;

9) Часті, нетривалі виїзди до іноземних країн;

10) Намагання запропонувати додатковий дохід від імені сторонньої зацікавленої особи військовослужбовцю, який має доступ до чутливої інформації, або втягування його в кримінальну ситуацію, яка може призвести до підкупу;

11) Неодноразові порушення заходів безпеки;

12) Жартування на тему співробітництва з іноземною спецслужбою, відвідання іноземних дипломатичних установ, консульств, торгових чи прес-офісів.

Закріплена Інструкцією процедура надання доповіді передбачає наступний порядок.

1. Особи, які є учасниками або володіють інформацією про випадки, описані Інструкцією, повинні негайно доповідати до найближчого контррозвідувального офісу. Якщо це не є представляється можливим, то інформація повинна надаватись офіцеру безпеки чи командуванню, які зобов'язані протягом 24-х годин передати її до підрозділу контррозвідки.

2. Доповідь повинна містити максимально деталізовану інформацію, ні за яких обставин не дозволяється проводити власне розслідування чи переслідувати підозрюваного. В разі надходження особі пропозиції про співробітництво, відповідь повинна бути ухильною, не містити ні згоди, ні відмови.

3. В період перебування за кордоном, особи, в разі термінової потреби (наявності загрози життю чи майну), повинні надавати інформацію найближчій військовій посадовій особі, офіцеру розвідки чи безпеки, військовому аташату, до американського

посольства чи консульства. В іншому випадку, доповідь повинна надаватися до контррозвідувального підрозділу після повернення з-за кордону.

Заслуговує на увагу, що в межах реалізації Інструкції № 381-12 на командирів всіх рівнів покладаються наступні обов'язки:

1) Забезпечувати надання підлеглим особовим складом доповідей до відповідних контррозвідувальних підрозділів щодо фактів та ознак шпигунства, диверсії, інших визначених Інструкцією ситуацій;

2) Вживати належних заходів, аби інформація за визначеними Інструкцією категоріями надходила безпосередньо до контррозвідувальних підрозділів, а не по лінії військового командування, аби не зашкодити можливому проведенню подальшого розслідування;

3) Включати контррозвідувальні тренування до всіх інших тренувальних програм, в тому числі поєднувати їх з тренуваннями з питань безпеки. Забезпечувати щорічне проходження контррозвідувального тренування військовослужбовцями та працівниками Армії;

4) Здійснювати моніторинг якості та ефективності контррозвідувальних тренувань.

За результатами виконання Інструкції складається щорічний звіт, який містить наступну інформацію:

1) Кількість представників особового складу, які пройшли щорічне контррозвідувальне тренування;

2) Кількість доповідей, що надійшли за визначеними Інструкцією категоріями;

3) Кількість розслідувань, які були розпочаті на підставі наданих доповідей;

4) Кількість розслідувань, які мали результатами:

- Планування і проведення контррозвідувальних операцій;
- Підтверджені випадки шпигунства;
- Підтверджене несанкціоноване розголошення інформації з обмеженим доступом;
- Призначення кримінальних та адміністративних покарань особам, винним у здійсненні шпигунства чи пов'язаних з ним правопорушень;
- Призначення адміністративних чи іншого роду покарань за ненадання передбачених Інструкцією доповідей;
- Призначення адміністративних чи іншого роду покарань за інші порушення, які були виявлені в результаті доповідей, наданих згідно Інструкції;

5) Кількість доповідей щодо терористичних загроз Армії США та іншим національним інтересам;

6) Кількість спроб та фактів несанкціонованого втручання в автоматизовані системи Армії.

Американське законодавство в сфері оборони також містить норми, які встановлюють вимоги щодо надання доповідей до контррозвідувальних підрозділів Армії про ознаки, контакти, поведінку та діяльність, пов'язані з тероризмом, а також кіберзагрози, до яких можуть бути причетні іноземні спецслужби. Зокрема, Директива Департаменту оборони № 5240.06 зобов'язує доповідати про наступне [7].

1) Виправдування насильства, погроз насильства, або застосування сили для досягнення цілей в інтересах відомих чи підозрюваних міжнародних терористичних організацій, прояви підтримки цих організацій;

2) Надання фінансової чи іншої матеріальної підтримки відомим чи підозрюваним міжнародними терористичним організаціям чи міжнародним терористам;

3) Передача обладнання чи знаряддя, придбання складових для виготовлення бомб, отримання інформації про конструкцію вибухових пристроїв в інтересах відомих чи підозрюваних міжнародних терористичних організацій;

4) Підтримання контактів з терористичними організаціями, в тому числі через соціальні мережі, збір інформації в їх інтересах;

5) Спроби завербувати інших осіб для участі в терористичній діяльності;

6) Родинні або інші зв'язки з членами терористичних організацій;

7) Відвідання веб-сайтів міжнародних терористичних організацій, які пропагують насильство, не пов'язане з виконанням службових обов'язків;

8) Злам паролів, акаунтів, розмежування доступу, криптозахисту;

9) Витік чи компрометація комп'ютерної інформації;

10) Впровадження в інформаційні системи непередбачених програмних чи технічних елементів;

11) Несанкціоноване завантаження чутливої комп'ютерної інформації, а також впровадження несанкціонованих комп'ютерних програм;

12) Несанкціонований мережевий доступ, електронне листування на адреси, розташовані на іноземних серверах;

13) DOS-атаки чи підозрілі мережеві помилки;

14) Передача даних до недозволених доменів;

15) Безпідставне накопичення криптованої інформації;

16) Соціальний інжиніринг, фішінг, підлаштування хибних електронних адрес;

17) Виявлення вірусів, комп'ютерних хробаків, троянів, логічних бомб, інших шкідливих програм.

Висновки.

Таким чином, у теперішній час військовослужбовці Збройних Сил України та інших військових формувань фактично не мають нормативно визначених обов'язків у сфері контррозвідувального режиму, крім зобов'язань, які виникають в зв'язку з отриманням допуску до державної таємниці. Водночас нині існує необхідність вжиття дієвих заходів щодо вдосконалення загальнодержавної системи забезпечення контррозвідувального режиму в Україні, про що свідчить затвердження Указом Президента України від 6 жовтня 2017 року № 310/2017 Концепції забезпечення контррозвідувального режиму в Україні [10]. Відтак вбачається, що одним з напрямків підвищення ефективності контррозвідувального режиму є внесення змін до законодавчих актів України в частині визначення завдань, повноважень та функцій суб'єктів системи забезпечення контррозвідувального режиму в Україні, а також посилення юридичної відповідальності фізичних та юридичних осіб за порушення у сфері дії окремих елементів контррозвідувального режиму в Україні.

Упровадження норм, аналогічних вищерозглянутим, у законодавство України, зокрема у відомчі нормативні акти Міністерства оборони, Збройних Сил та Служби безпеки України, а також накази та розпорядження, які мають міжвідомчий характер, може мати суттєве значення для посилення контррозвідувального режиму та підвищення ефективності контррозвідувального пошуку органами військової контррозвідки СБ України.

Використана література

1. Про контррозвідувальну діяльність: Закон України. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89.

2. Про внесення змін до законів України, що регулюють оперативно-розшукову та контррозвідувальну діяльність: пояснювальна записка до проекту Закону України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=54666&pf35401=336780

3. Кудінов С.С. Шляхи удосконалення правового регулювання забезпечення Службою безпеки України Антитерористичної операції. URL: http://pgp-journal.kiev.ua/archive/2019/2/45.pdf

4. Авдошин І.В. Оптимізація контррозвідувальної системи США з попередження загроз підривного характеру. URL: http://science.univ.kiev.ua/sbu.pdf

5. Ватраль А.В. Сучасний стан правового регулювання контррозвідувального пізнання. URL: http://pravoisuspilstvo.org.ua/archive/2017/5_2017/part_2/53.pdf

6. DepartmentofDefense INSTRUCTION NUMBER 5240.6 July 16, 1996 Counterintelligence (CI) AwarenessandBriefingProgram. URL: www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524006p.pdf

7. DepartmentofDefense DIRECTIVE NUMBER 5240.06. URL: https://fas.org/irp/doddir/dod/d5240_06.pdf

8. DepartmentofDefense DIRECTIVE NUMBER 5240.02. URL: https://fas.org/irp/doddir/dod/d5240 _02.pdf

9. ArmyRegulation 381–12. SubversionandEspionageDirectedAgainstthe U.S. Army (SAEDA). URL: https://fas.org/irp/doddir/army/ar381-12-1993.pdf

10. Про рішення Ради національної безпеки і оборони України від 13 вересня 2017 року "Про Концепцію забезпечення контррозвідувального режиму в Україні": Указ Президента України від 6.10.17 р. № 310/2017. URL: http://zakon4.rada.gov.ua

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~