

# **КОНСПЕКТ**

## **дисциплина „СРС“**

- 1. Основни методи за получаване**
- 2. Подслушване**
- 3. Наблюдение и проследяване**
- 4. Проникване**
- 5. Беязване**
- 6. Обекти и субекти на СРС**
- 7. Подготовка за прилагане на СРС**
- 8. Осигуряване и прилагане на СРС**
- 9. Използване на резултатите СРС**
- 10. Контрол и наблюдение**

# 1. Основни методи за получаване на информация в специалните служби

През последните години настъпи драстична промяна на средата за сигурност в Европа. Предизвикателствата за националната сигурност днес се нуждаят от отговори, които да съчетават аспекти от вътрешната и външната политика. Станахме свидетели на поредица от кризи, извънредни ситуации и терористични актове в държавите-членки на Европейския съюз (ЕС). Рисковете и опасностите на територията на Европа, особено в западна, нарастват. Само през последните години се извършиха над 16 кървави атентата, някои от които взеха много човешки жертви.

Нападенията, които бяха извършени на европейска територия са доказателство, че е необходима адекватна реакция на всяка една държава с оглед адаптиране към опасностите. За България се пораждат допълнителни рискове като потенциален обект на тероризъм след като страната ни взе участие в световната антитерористична коалиция и е на един от главните пътища между Европа и Близкия Изток.

Посочените терористични атентати са основателна причина за оптимизация в дейността на структурите за сигурност и добиване на адекватна разузнавателна информация. Динамичните промени, които са налице, дават основание да се акумулира изпреварваща информация по отношение на бъдещите заплахи и опасности за България.

Разузнаването е важен източник за добиване на информация за защита на националната сигурност и има за своя задача да събира данни от политически, икономически и военен характер. Една от основните функции на разузнаването е не само да събира и обработва информация, но и да доведе тази информация до държавните институции, които могат да вземат външно- и вътрешнополитически решения. Значимостта или важността на разузнавателната информацията е нейното основно качество.

Методите могат да бъдат разделени на три основни групи:

- **на основата на открити източници;**
- **чрез използване на хора** (агенти, секретни сътрудници, доверени лица), носители на необходимата информация;
- **чрез използването на технически средства и системи**, т.е. на специални разузнавателни средства (СРС).

Относителната тежест на трите групи източници за събиране на информация за различните направления в сферата на националната сигурност не е еднаква. Въпреки всичко трябва да се подчертае, че нито при изследване на външната среда, нито при изучаване на вътрешната среда може да бъде пренебрегнат някои от методите за придобиване на информация. При сериозни изследвания, например, на заплахите за националната сигурност и борбата с организираната престъпност като правило се използват и трите източника на информация.

## ***Получаване на информация от открити източници.***

Към използването на открити източници се отнасят способите за добиване на информация по пътя на анализа на вестници, книги, научни и технически издания, официални отчети и особено на рекламни материали. Този способ се използва от болшинството разузнавания в света. Ясно е, че основната работа тогава се извършва от специално подготвени анализатори, през които преминават планини от материали в търсене на “златното зрънце” от необходимата информация. Трябва да се знае основното правило - винаги трябва да се помни за свойството на информацията постепенно да се натрупва. За това, когато се дава външно безобидна реклама или интервю, изпраща се отчет или се прави доклад, винаги трябва да се съпоставя тяхното съдържание с по-рано предоставени за открито ползване материали, в съчетание с които нашите “откровения” ще имат свършено друго значение.

## ***Получаване на информация чрез използване на негласни източници (агентура).***

В практиката на всички разузнавателни централи по света използването на негласни източници се смята за незаменима. Вербуването на негласен източник на място или вкарването му отвън, си остава решаващо средство за преодоляване на преградите, издигани от държавите за защита на националните интереси.

Използването на хора - носители на информация принадлежи към друга група способности в разузнаването. Работата е в това, че техните възможности са значително по-големи. Всеки човек, освен носител на информацията, може да я анализира, обобщава и да прави изводи, т.е. да получава необходимите сведения по съвкупността от косвени данни. При определени условия хората могат да скриват, да крадат, да продават информация и да извършват други криминални действия, включително до встъпване в престъпни връзки с противникови организации.

Придобиването на агент може да стане по пътя на шантажа или чрез подкупване, но практиката е доказала, че ефективна работа от него може да се очаква, когато той действа по убеждение. За това умните разузнавачи се стремят да развият дружески отношения със секретния си сътрудник.

Вербовката на негласен източник не е еднократен акт. Тя представлява продължителен процес, който обхваща някакъв период от време. Негласните източници преминават през етапи на вербовка, обучение, след което специалните служби могат да ги използват за разрешаване на оперативни задачи като се спазват секретните принципи на работа. Внедрените, въведените или вербовани негласни източници са необходими, за да сигнализират за приготвяне и подготовка за извършване тежки престъпления или на терористични актове. Ролята на апарата от негласни източници е превантивна. От изключителна важност за защита на националната сигурност е формирането на ценен набор от негласни източници, който да предоставя изпреварваща информация по отношение на противозаконни прояви.

## ***Получаване на информация чрез специални технически средства, системи и способности.***

Бурното развитие на техниката и технологиите през последните десетилетия предизвика още по-бързо развитие на техническите средства и системи в разузнаването. В създаването на средства и системи за водене на разузнавателна дейност във всички развити страни се влагат огромни средства. Стоици фирми в много страни работят в тази област. Този отрасъл на бизнеса отдавна е заел своето място в общата система на западната икономика и има своята здрава законодателна основа.

Според мненията на водещи експерти стойността на информацията при използване на специални технически средства (електронно наблюдение, проследяване и подслушване и др.) при разследването на някои форми на тежки престъпления или терористични актове е несъмнена. Този метод е от изключителна важност за защитата на националната сигурност в съвременните условия.

Използването на специалните оперативно-технически способности очевидно представлява нарушаване правата на човека в определени случаи и условия.

Съгласно Закона за специалните разузнавателни средства (ЗСРС) в нашата страна право за използването им имат само изрично посочени оперативно-техническите служби от: Държавна агенция „Технически операции“ (ДАТО), Държавна агенция „Национална сигурност“ (ДАНС), Държавна агенция „Разузнаване“ (ДАР) и служба „Военна информация“. При всичките си несъвършенства, той определя случаите, когато могат да бъдат нарушени конституционните права на гражданите на свобода и лична неприкосновеност.

## 2. ПОДСЛУШВАНЕ

Специалните разузнавателни средства (СРС) за подслушване са едни от най-често прилаганите технически устройства за придобиване на разузнавателна информация. Както бе вече отбелязано, за 2016 г. броят на приложения оперативен способ „подслушване“ за цялата страна е 4717, за наблюдение – 1856; за проследяване – 1849. През 2018 г. срещу 2 046 души са използвани специални разузнавателни средства /СРС/. Броят на исканията е 6099, а на издадените разрешения – 5328. Останалите оперативни способности са прилагани много по-малко пъти. Това се дължи на факта, че акустическият сигнал е един от достоверните източници, подлежащ при това на допълнителна проверка и анализ. Освен това информацията да се получава практически в реално време. При това информацията се получава без посредник, което до голяма степен гарантира нейната истинност.

Чл.6 от ЗСРС дава следната дефиниция за подслушването:

“При подслушването чрез използването на технически средства, слухово или по друг начин се усвоява устна, телефонна или електронна информация на контролираните лица”.

Определението показва, че чрез подслушването се извършва три вида контрол на информация, получавана от обекти, интересоващи правоохранителните органи:

- **контрол на устните разговори (слухов контрол);**
- **телефонен контрол;**
- **контрол на електронните комуникации.**

**Контрол на устните разговори (слухов контрол).**

Постиженията на техниката и технологията позволиха понастоящем да се създадат огромно количество СРС за подслушване, различаващи се по принцип на действие, начин за предаване на придобитата информация, по радиус на действие. Особено голямо е разнообразието по отношение на габаритните им размери и външното им оформление, да не говорим за предметите, в които те са монтирани (т.н. “камуфлажи”).

Най-малките СРС за подслушване имат пренебрежимо малки габаритни размери (не превишаващи няколко милиметра). Независимо от това те предават придобитата информация на стотици метри. В момента не представлява техническа трудност да се получава информация чрез подслушване от обект, който се намира в другия край на нашата страна. Естествено, само във възможностите на големите държави и техните мощни разузнавателни служби е осъществяването на глобален контрол върху комуникациите по цялото земно кълбо. Още през 80-те години на миналия век подобни данни вече бяха налице.

**Режими на работа на СРС**

В зависимост от режима на работа на СРС във времето, те могат да бъдат разделени на три групи:

- **с непрекъснато предаване на информацията;**
- **с дистанционно управление;**
- **с автоматично включване при поява на сигнал.**

**Захранващи източници на СРС.**

В зависимост от захранващите източници СРС могат да бъдат разделени на две групи:

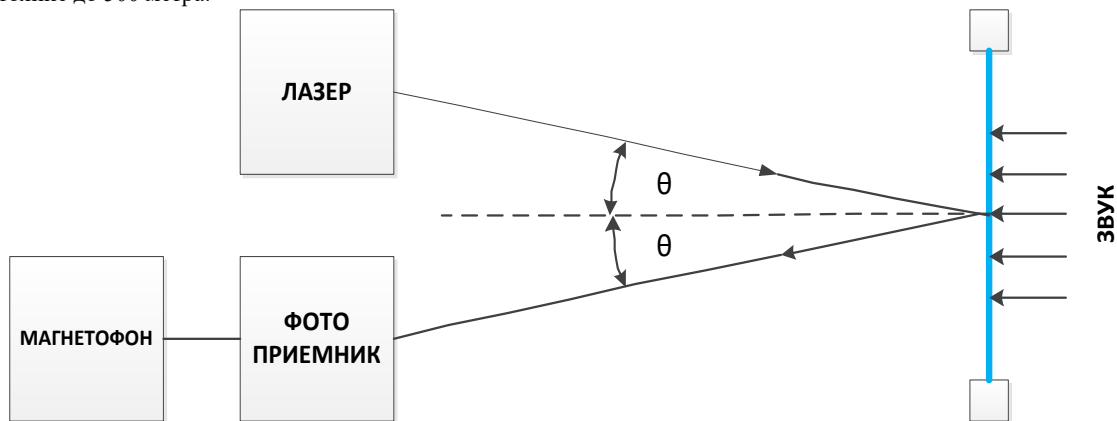
- **със собствен източник;**
- **със захранване от външен източник.**

Първият вариант е по-често срещан и предполага наличието на собствена захранваща батерия.

**СРС, използващи оптически (инфрачервен) канал.**

Едно от перспективните направления за подслушване чрез ВЧ сондиране се явяват лазерните микрофони. Според някои данни те са били приети на въоръжение още през 60-те години на миналия век. В качеството на сондиращ сигнал тук се използва лазерен лъч. Като правило, лазерните микрофони работят в близкия до видимата светлина инфрачервен диапазон (0.8-1.0  $\mu\text{m}$ ) за да се избегне откриването на петното на облъчвания сигнал. Мощността обикновено не превишава 10 mW.

Поради малката дължина на вълната не представлява техническа трудност ИЧ лъчи да се фокусират в много тесен лъч, което ги прави трудно откриваеми, дори със специализирана апаратура. Радиусът на действие на тези системи може да бъде много голям, но обикновено се използват на разстояние до 500 метра.



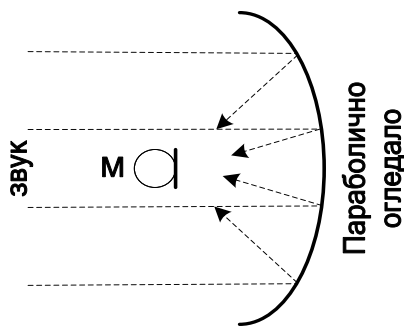
Принцип на действие на лазерните микрофони.

Принципът на действие на лазерните микрофони става ясен от фиг. 9 по-горе. Генериращият от лазера оптически сигнал се разпространява през атмосферата, достига до контролирания обект и се отразява от отразяващата повърхност. Най-често тази роля се отнежда на стъклото на прозореца от контролираното помещение. Това стъкло, обаче, вибрира поради въздействието върху него на звуковите вълни от провежданите разговори (да не забравяме, че същото въздействие оказват и външните шумове от улицата). Поради тази причина се получава модулация на отразения сигнал, която се приема от фотоприемника, демодулира се и по този начин се извлича необходимата информация.

**Насочени микрофони**

**А) Принципи на действие. Видове.**

Насочените микрофони се използват преди всичко за подслушване на разговори на открито. Оперативната необходимост за това възниква, когато контролираните лица се срещат с други хора в паркове, градини, на разходка извън населени места или в планината. Като правило в този случай се прилага и оперативния способ „проследяване“, което означава контрола на разговорите на открито обикновено се извършва от екипите на тези оперативно-технически структури.



Параболичен насочен микрофон – принцип на действие, външен вид.

#### Особености при използването на насочените микрофони

Разстоянието, от което може да се осъществи контрол на разговори с помощта на насочен микрофон, зависи не само от техническите му характеристики, но и от условията на разпространение на звука. Говорът като акустически процес се характеризира с физически параметри: честотен спектър, скорост на разпространение, звукова мощност, интензивност, ниво на силата на звука и т.н., които също оказват влияние върху разбираемостта на възприеманата информация.

Основни определящи фактори за крайния резултат по отношение на разбираемостта се явяват:

- **затихването на звука;**
- **нивото на страничните шумове.**

#### Телефонен контрол.

На съвременния етап от развитие на човешкото общество ние не можем да си представим света без средства за комуникация. Едва ли има направление в човешката дейност, което да се е развивало с по-бързи темпове от комуникациите. Телефонът е едно от най-често използваните средства за общуване между хората. И това е така, защото освен информация чрез него в определена степен се предават чувства, настроения, т.е. той приближава най-много хората до живото общуване.

Това е една от причините телефонният контрол да има изключително важно значение. Телефонът дава много добра възможност за проникване в дейността на контролираното лице. С помощта на телефонния контрол се получава навременна информация за връзките на обекта, за характера на неговите взаимоотношения, за неговите действия, навици и намерения, което позволява да се предприемат мерки за предотвратяване и пресичане на престъпни замисли.

Без никакви съмнения може да заявим, че в света съществува глобална информационна система, по която във всеки един момент протича огромно количество информация. Тази информация обаче интересува не само нейните потребители, но при определени ситуации и специалните служби на различните държави. Търговската и служебна информация на фирмите и корпорациите представлява голям интерес за техните конкуренти. Поради това от гледна точка на сигурността и защита срещу промишления шпионаж е необходимо познаването на структурата на телефонните мрежи и техните опасни зони.

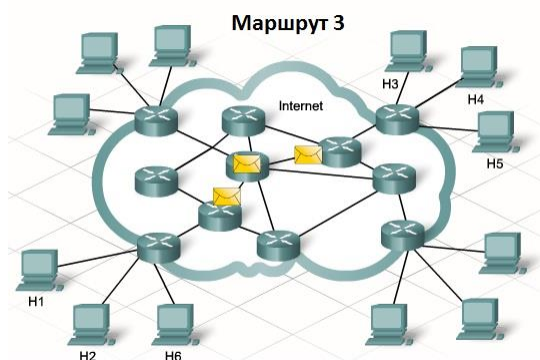
#### Контрол на електронните комуникации.

През последните години голям интерес представлява контрола на глобалната мрежа Интернет. Този интерес се засили особено след 11 септември 2001 г., когато стана известно, че мрежата се използва за връзка между терористични организации и групи от международната организирана престъпност.

За да се разбере какво е Интернет, трябва първо да сме наясно с това какво е мрежа. Мрежа, на езика на компютрите, се нарича група от компютри, способни да комуникират помежду си и да обменят информация. По своята същност Интернет представлява глобална мрежа от мрежи. Интернет е съставен от множество мрежи на разни организации – университети, компании и организации. Същността на Интернет е не толкова в мрежовия хардуер, в компютрите и в свързващите ги линии, а по-скоро във взаимодействието между всички тези неща. Липсата на централизиран контрол е една от най-силните и същевременно една от най-слабите страни на Интернет. Липсата на контрол улеснява свободния обмен на информация и идеи, но лошото е, че няма организация, която да наблюдава Интернет и да прочиства неуместните неща. Накратко: Интернет е средство за общуване почти без правила относно съдържанието.

В Интернет комуникацията между всички отделни точки се осъществява от компютрите. Нереалистично е да очакваме, че всички компютри, които се използват по света от различните групи и организации, ще бъдат едни и същи или ще работят по един и същ начин. Интернет всъщност работи благодарение на създадените за него протоколи. В Интернет се използва протоколът, наречен TCP/IP (Transmission Control Protocol / Internet Protocol, - Протокол за управление на предаването / Протокол за Интернет).

Хората най-често получават своята връзка към Интернет от ISP (Internet Service Provider - Доставчик на Интернет услуги). Това дава обяснение на начина, по който е възможен контрол на Интернет – комуникациите – чрез провайдерите. Влизайки в „облака“, под каквото име е известно интернет-пространството, съобщението може да достигне до крайния потребител по различни маршрути, което прави невъзможно проследяването му от друго място.



Обща блокова схема на Интернет – комуникациите.

По тази причина Закона за електронните съобщения<sup>1</sup> в чл. 251б възлага това задължение на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.

В заключение трябва да се подчертае, че под общото наименование „подслушване“ оперативния способ обхваща прилагането на изключително голям брой технически средства и методи.

<sup>1</sup> ЗАКОН ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ - Обн. ДВ. бр.41 от 22 Май 2007г., изм. ДВ. бр.109 от 20 Декември 2007г.,..... изм. и доп. ДВ. бр.21 от 9 Март 2018г.

### 3. Наблюдение и проследяване

За осъществяване на тези два оперативни способа е необходимо присъствие на обекта в контролираната зона, т.е. информацията се придобива чрез зрението. Наблюдението може да се извърши с помощта на: оптически прибори (монокулярни и бинокъларни), телевизионни системи за наблюдение (CCTV), прибори за нощно виждане, термовизионни апарати. Документирането действията на обекта се извършва чрез фотографиране и видеозапис (кинозаписа, въпреки че е отбелязан в ЗСРС на практика вече не се използва).

Наблюдението и проследяването се използва от правителствата за събиране на разузнавателни данни, предотвратяване или разследване на престъпления, защита на процеси, на лица, група лица или на обект. То се използва и от престъпни организации за планиране и извършване на престъпления като грабежи и отвлечения, от страна на бизнеса - за събиране на разузнавателна информация за конкуренти, а така също и от частни детективи. Може да се изпълнява с помощта на хора, но често - чрез телевизионни системи за наблюдение и документиране на събитията.

Визуалното наблюдения се използва за наблюдение на помещения (частни или обществени), на открити площи (в обекти или населени места). При наблюдение на помещение камерите са камуфлирани в някакъв предмет в него и сигнала се предава по кабел или чрез радиосигнал. През последните години създаването на така наречените затворени телевизионни системи (CCTV), особено в градовете, добива все по-широки размери.

Двата оперативни способа могат да се използват *постоянно*, т.е. денонощно (при обекти, представляващи сериозна заплаха за националната сигурност или преди сериозни оперативни операции), *периодично* (например, за проверка на изменения в оперативната обстановка) и *епизодично* (за проверка на сигнали и изясняване на определени факти).

Като правило, наблюдението и проследяването са изключително *тайни, конспиративни методи*, които изискват висок професионализъм при прилагането им. За това не трябва да разбира нито контролираното лице, нито неговите близки и обкръжението му. Това, обаче, изисква ангажирането на големи сили и средства, което прави тези способности едни от най-скъпите.

Понякога се прилага *открито, явно наблюдение и проследяване*, наричано още „японско“. То се използва обикновено спрямо доказани служители в разузнавателни резидентури, работещи на прикритие в дипломатическите представителства на страни, заплаха за националната ни сигурност.

При изпълнение на определени оперативни задачи може да се използва *комбинирано проследяване*, например, прилага се явно и в определен момент се имитира, че обекта се е откъснал от проследяващите, след което други сили продължават проследяването тайно.

#### *Наблюдение на стационарни обекти*

Наблюдение на стационарни обекти - помещения, сгради, открити пространства, се прилага, когато е необходимо:

- наблюдение действията на контролираното лице с цел провеждане на конкретна акция;
- установяване на посетителите и техните взаимоотношения с обекта;
- откриване на издирвано лице.

Внимателно наблюдение на контролираното лице и неговите посетители може да стане само от удачно избрано място, от което да се контролират не само възможните действия на обекта, но и всички възможни подходи към него. То трябва да позволява продължително пребиваване, без да предизвиква подозрение в околните – например, маса в кафе, спирка на градския транспорт, имитация на ремонтна работа, използване на търговски пункт и т.н. Понякога, особено при сериозни обекти със солидна професионална подготовка, се предпочита изцяло незабележимото наблюдение от тавана, покрива или дом в подходяща сграда.

Негласното наблюдение на помещения е изключително полезно за разследващите органи, но в същото време е изключително трудно за осъществяване. Това наблюдение се извършва с помощта на специални визьори от съседни помещения или чрез камуфлирана телевизионна техника, монтирана тайно в помещението. Визьорът се характеризира с много малък диаметър на отвора, през който се наблюдава, поради което много трудно може да бъде открит. При използване на визьор може да се наблюдава всяко действие в онази част от помещението, която попада в обектива на оптичния прибор. За фиксиране на отделни моменти могат да се правят фотоснимки. В тези случаи визьорът се съчетава с фотоапарат. Наблюдението на помещение само с помощта на специалните оптични прибори е уморително и неудобно за ОР, който води наблюдението. Поради това той може да пропусне интересно от оперативна гледна точка събитие.

Проследяването на лица се прилага за изпълнение на конкретни цели:

- Предотвратяване или прекъсване на престъпен акт;
- Придобиване на информация, която може да се използва като веществен доказателствено средство пред съда;
- За проверка и допълване на информация, получена от друг източник;
- Подкрепа на доказателства, получени от ОР под прикритие;
- Осигуряване сигурността на ОР, работещи под прикритие и много други.

Към служителите, извършващи проследяване, се предявяват редица изисквания, продиктувани от секретния характер на тяхната дейност, при това извършвана на открито, пред погледите на много хора. На първо място те трябва да имат незабележима външност (без особени белези и ярки, запомнящи се дрехи), отлична памет; оптимална издръжливост; голямо търпение, бърза реакция, отлично зрение, превъзходен слух, умение да импровизират и да се ориентират бързо в ситуацията.

Поради факта, че периодичното появяване на едни и същи лица може да изостри вниманието на обекта, се използват средства за лична маскировка - очила, перуки, мустаци, дрехи с две лица, които периодично се сменят. Трябва да се знае, че понякога е по-добре да се загуби обекта, отколкото той да бъде предупреден

## 4. Проникване

Това са едни от често провежданите операции на контраразузнаването, при които се цели придобиване на актуална, достоверна и навременна информация, директно от нейния носител чрез използване на технически средства.

Операцията по оперативно-техническо проникване може да бъде определена като сложна и високоорганизирана форма на контраразузнавателно противодействие, насочена към създаване на организация и условия за секретно и тайно преодоляване защитите за сигурност на престъпника и безпрепятствено монтиране, експлоатация и демонтиране на технически средства, които да позволят събирането на оперативно значима информация за лица, предмети, вещи, документи или други носители на информация, които пряко или косвено са свързани с осъществяването на шпионска дейност.

Значимостта на операциите по техническо проникване се определя и от невъзможността в конкретни случаи и при конкретни обстоятелства да бъде набавена необходимата информация по друг начин. Това дава основание контраразузнавателната операция по техническо проникване да бъде разглеждана като *комплекс от контраразузнавателни действия и мероприятия, обединени от един замисъл, провеждани в определена последователност и ръководени от един център, които са осъществявани с цел овладяването на разузнавателни позиции, временно или постоянно, с помощта на технически средства в средата на противника и установяване на слухов, визуален, електронен, компютърен или друг контрол върху комуникациите или каналите за пренос на данни на чуждите разузнавания, прикрити на наша територия.*

### **Обекти на оперативно - техническо проникване**

Обектите на такива операции са *носителите на информация*. Такива носители могат да бъдат:

- отделни лица и техните връзки, които се явяват носители на информация или чрез действията и поведението си издават признаци на разузнавателна дейност.

- Вещи, предмети или документи, които също съдържат информация или признаци за осъществявана посегателска дейност.

- Специално оборудвани помещения, сейфове и др., както и технически устройства за съхранение или пренос на данни.

В зависимост от пространствената определеност обектите могат да бъдат:

- жилища, служебни, обществени или помощни помещения, които се използват за провеждане на разговори или срещи.

- Различни превозни средства в това число и обекти на обществения транспорт, но в по-голямата си част това са лични моторни превозни средства.

- Специално оборудвани помещения, в които се съхранява информация или технически средства за нейното съхранение.

Основна цел на техническото проникване е да се придобият разузнавателни позиции чрез технически средства в средата на чуждите разузнавания на наша територия, в онези обекти, където се систематизира, обработва и шифрова събраната секретна информация или се подготвя и изпраща до разузнавателните центрове.

Задачите, които се решават с помощта на разглежданите операции могат да бъдат определени по следния начин:

- придобиване на данни за характера, обема и съдържанието на разузнавателната информация, намираща се на разположение в чуждите разузнавания

- получаване на информация за организацията, тактиката и насоките на разузнавателната дейност на противника

- разкриване на сътрудници на чуждите разузнавания из средите на българските граждани, както и на такива, влизачи в състава на основната, резервната, спомагателната или консервираната резидентура на наша територия

- провеждане на дезинформационни мероприятия и подготовка на условия за осъществяването на оперативни игри с противника, както и за провеждане на мероприятия с изпреварващо значение спрямо нашата национална сигурност.

Възможно е разглеждането на операциите по техническо проникване да бъде подчинено на различна от досегашните класификации по отношение на етапите и стadiите, през които преминава. Характерно е, че самата операция има подготвителна и същинска част. Отделните елементи, които се включват в различните стadiи и етапи, могат да бъдат разгледани самостоятелно.

**Подготвителен етап** по организацията на операцията:

- определяне на целта и поставяне на задачите пред контраразузнавателната служба

- определяне на обекта

- очертаване на местата, начините за проникване и времето за неговото осъществяване

- определяне на участниците в операцията и разпределяне на функциите между тях

- възлагане на конкретни задачи на отделните изпълнители

- определяне на ръководен център на операцията и създаване на система за вземане на решения

- финансово и материално-техническо осигуряване на операцията

- създаване на координация, възможности за взаимодействие и определяне на начините за връзка между отделните звена, участващи в операцията

За етапа на експлоатацията се разработва допълнителен план за осигуряване на опазването на техническото мероприятие. В плана се предвиждат действия на основата на различни варианти, които могат да се предположат като ситуации, предполагащи разкриването на мероприятието. Необходимо е за различните варианти да бъдат предвидени комбинации с цел демонтиране или запазване на мероприятието. Обикновено контролът върху сигурността на мероприятието, както и отговорността за неговото запазване пада върху службите за сигурност. Елемент от запазване на мероприятието е начина на използване на придобитата от него информация.

Независимо от условията или факторите, които налагат демонтирането на техническото мероприятие за неговото осъществяване се налага създаването на същата организация и провеждането на същите действия, както при неговото монтиране.

## 5. Белязване

Общите задачи, изпълнявани с оперативния способ “белязване”, са формулирани в член 9 от ЗСРС.: “При белязването чрез използването на технически средства и вещества се поставят белези на предмети и вещи за установяване на тяхното движение, придобиване или мястото на съхранението им”.

Белязването позволява да се разкрива маршрута на движение на маркирани вещи и предмети, както и местата на тяхното съхранение. По този начин сравнително лесно могат да се установят съучастниците на обекта в извършваната от него престъпна дейност. Наблюдението на маркираните хора и автомобили позволява да се осъществи по-пълно документиране действията на обектите и откриване на скривалищата, в които те съхраняват материалите и вещите, използвани за реализация на престъпни цели.

### Видове белязване

#### *Механично белязване*

Очевидно чрез механично белязване не могат да се проследяват предмети и вещи, но това не намалява неговото значение. Чрез поставянето на характерни белези на определени места на предмета се цели предотвратяване на подмяната му с друг (например фалшификат или друг предмет от същия вид). Когато белега се поставя за изпълнение на определена оперативна задача, то той трябва да бъде трудно откриваем и с малки размери.

В разузнаването механичното белязване се използва, за да се провери дали специалните служби на противника не са имали достъп до предмета (писмо, колет, тайник и т.н.). Чрез поставяне на миниатюрни белези, например с малък по дължина конец или къс хартия разузнавачи проверяват дали е извършено негласно проникване в обитавани от тях помещения. Механични белези се използват и за предаване на съобщение - например поставен знак с тебешир на определено място може да означава искане за среща, информация за изпратена (получена) пратка, сигнал за опасност и т.н.

#### *Химическо белязване*

Химическото белязване се използва отдавна като един от оперативно-техническите способности в работата на полицията. Предметите или вещите се обработват с химически вещества, които оставят върху тях следи. Като правило, тези следи са невидими, но стават видими при обработка с други химически вещества или при облъчване с ултравиолетова (УВ) светлина (макар и по-рядко се използват вещества, реагиращи при облъчване с инфрачервена светлина).

Химическото белязване се използва например при маркиране на пари с цел документиране получаването на подкуп или при рекетиране на граждани.

Чрез белязване с химически вещества може да се установят хората, които са се докосвали до вещи, предмети и документи, интерес към които се очаква да проявят шпиони, престъпни групи или даже обикновени крадци.

#### *Радиоизотопно белязване*

Някои автори отнасят радиоизотопното белязване към химическото. Поради съвършено различните принципи за откриване на белязаните предмети е по-правилно то да се разглежда като самостоятелен вид.

Белязаните предмети се обработват с радиоизотопи, излъчването от които, както е известно, не могат да се открият с нито едно от човешките сетива. Откриването на радиоактивност става с помощта на специални прибори (така наречените дозиметри или радиометри). Това позволява да се установи преминаването на белязани предмети през определени контролни пунктове или тяхното откриване между множество други подобни вещи.

#### *Радиоелектронно белязване (маркиране)*

Устройствата за радиоелектронно маркиране понякога се наричат “радиофар”. Постиженията на технологиите в радиоелектронното производство позволи този вид да придобие твърде широко приложение. Най-често електронните системи се използват за маркиране на коли, но размерите им станаха толкова малки, че не представлява трудност с тяхна помощ да се маркират и други предмети (например колети, пратки и т.н.).

Основното предимство на радиоелектронното белязване е факта, че то на практика е единственото, позволяващо проследяване движението на маркираните предмети, при това понякога от значителни разстояния, включително с използване на спътникови канали за връзка.



GPS приемник за определяне местоположението на транспортни средства

До скоро се считаше, че системата GPS не може да се използва за белязване на предмети. Постиженията на електрониката обаче направиха това възможно. Размерите на GPS приемниците станаха достатъчно малки. Само приемникът обаче не е достатъчен. Необходим е предавател, който да предаде изчислените от GPS-приемника координати до центъра на заинтересованата организация. В нашата страна е създадена фирма (GPS-България), предлагаща подобна услуга. В нейната система се използва комбинацията между GPS приемник и апарат от клетъчната радиотелефонна система GSM. Сигналът за изчисленото местоположение на обекта се предава периодично или при повикване.

Белязването чрез използване възможностите на системата GPS позволява проследяването на пратки и коли на много големи разстояния, включително и на трансконтинентални трасета (например от Близкия Изток до Западна Европа).

## 6.Обекти и субекти на СРС

За първи път с Закона за изменение и допълнение на Закона за специалните разузнавателни средства от 9.08.2013 г. СРС се използват, когато това се налага за предотвратяване и разкриване на тежки умишлени престъпления, подробно изброени в чл.3 ал. 1 от закона. Най-общо казано, към тях се отнасят **престъпленията срещу републиката** (измяна, предателство и шпионство, диверсия и вредителство, други престъпления); **престъпленията срещу личността** (убийство, телесна повреда, отвличане и противозаконно лишаване от свобода, принуда, разврат, трафик на хора), **престъпленията против политическите права на гражданите, престъпленията против собствеността** (кражба, грабеж, присвоявания, измама, изнудване, вещно укривателство, унищожаване и повреждане); **престъпленията против стопанството** (престъпления в отделни стопански отрасли, против митническия режим, против паричната и кредитната система); **престъпленията против дейността на държавни органи, обществени организации и лица, изпълняващи публични функции, против спорта; компютърни престъпления; общоопасни престъпления** (извършени по общоопасен начин или с общоопасни средства, престъпления в транспорта и съобщенията, против народното здраве и против околната среда, други общоопасни престъпления); **престъпленията против отбранителната способност на републиката, против информацията, представляваща държавна тайна и против чуждестранната класифицирана информация; военни престъпления и против мира и човечеството**. В тези случаи специалните разузнавателни средства се използват за изготвяне на вещствени доказателствени средства (ВДС) при условията и по реда, предвидени в закона.

### **Обекти, спрямо които се прилагат специалните разузнавателни средства**

Съгласно чл. 12 ал. 1 от ЗСРС СРС могат да се използват по отношение на:

1. лица, за които са получени данни и има основание да се предполага, че подготвят, извършват или са извършили тежко умишлено престъпление от изброените по чл. 3, ал. 1от ЗСРС.;
2. лица, за чиито действия са получени данни и има основание да се предполага, че се използват от лица по т. 1, без да им е известен престъпният характер на извършваната дейност;
3. лица и обекти, свързани с националната сигурност.
4. обекти за установяване самоличността на лицата по т. 1 или 2.

Съгласно ал. (2) на същия член специалните разузнавателни средства могат да се използват и за опазване на живота или имуществото на лица, които са дали писмено съгласие за това.

Съгласно ал. (3) (Нова - ДВ, бр. 42 от 2015 г.) СРС могат да се използват и спрямо свидетел по наказателно производство, който е дал съгласието си за това, за установяване на престъпна дейност на други лица по чл. 108а, чл. 143 - 143а, чл. 159а - 159г, чл. 301 - 305 и чл. 321 от Наказателния кодекс.<sup>1</sup>

### **Субекти, имащи право да изискват използването на специални разузнавателни средства.**

Право да искат използване на специални разузнавателни средства, съгласно чл.13 ал.1 и ал.2 от ЗСРС, и да използват събраните чрез тях данни и вещствени доказателствени средства съобразно тяхната компетентност имат:

1. Главна дирекция "Национална полиция", Главна дирекция "Борба с организираната престъпност", Главна дирекция "Гранична полиция", дирекция "Вътрешна сигурност", областните дирекции на Министерството на вътрешните работи, специализираните дирекции (с изключение на дирекция "Технически операции"), териториалните дирекции и самостоятелните териториални отдели на Държавна агенция "Национална сигурност";

2. Службите "Военно разузнаване" и "Военна полиция" към министъра на отбраната.

3. Държавна агенция "Разузнаване";

4. Окръжните прокуратури - за престъпления по чл. 167, ал. 3 и 4 и чл. 169г от Наказателния кодекс<sup>2</sup>.

5. (нова - ДВ, бр. 7 от 2018 г.) дирекцията по чл. 16, ал. 2 от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество.

6. Наблюдаващият прокурор подава писмено мотивирано искане до съда за използване на специални разузнавателни средства по досъдебно производство.

В същия този член закона подробно регламентира правото за подаване на искане за използване на СРС за престъпления, осъществени от съдия, прокурор или следовател, както и други по-висши представители на съдебната власт. В определени случаи искания могат да подават също заместник на главния прокурор при Върховната касационна прокуратура, главния прокурор, министърът на вътрешните работи, председателят на Държавна агенция "Национална сигурност", председателя на Държавна агенция "Разузнаване", директора на служба "Военно разузнаване" или оправомощени техни заместници и от главния секретар на МВР.

Други органи не могат да искат и да използват специални разузнавателни средства.

Законът изрично разпорежда (чл. 20. ал.1), че специалните разузнавателни средства се осигуряват и прилагат от Държавна агенция «Технически операции» и от специализирана дирекция "Технически операции" на Държавна агенция "Национална сигурност.

С едно допълнение (чл.20 ал.2 от 2008 г) Държавната агенция „Разузнаване“ и разузнавателните служби на Министерството на отбраната могат да притежават и използват специални разузнавателни средства в рамките на своята компетентност. Със Закона за Държавна агенция «Разузнаване» е посочено, че разузнавателна информация е всяка придобита от Агенцията информация за чужди страни, организации и лица или за свързани с тях български организации и лица, която е от значение за националната сигурност на Република България. Изпълнението на дейностите на Агенцията се осигурява чрез (чл. 10 от ЗДАР):

1. използване на специални разузнавателни средства на територията на Република България при условия и по ред, определени със Закона за специалните разузнавателни средства;

2. използване на разузнавателни средства и способи извън територията на Република България при условия и по ред, определени от председателя на Агенцията;

Т.е. за първи път открито се предоставя правото на Агенцията да притежава и използва СРС, включително и на територията на нашата страна. Агенцията ползва информация от информационни фондове на Министерството на вътрешните работи, Държавна агенция „Национална сигурност“ и служба „Военна информация“ по начин, непозволяващ разкриване на интереса на Агенцията, и при спазване на принципа „необходимост да се знае“. Все пак трябва да се подчертае, че на Държавна агенция „Разузнаване“ не могат да се възлагат задачи от вътрешнополитически характер.

<sup>1</sup> НК – чл.108а-за тероризъм, подпомагането му чрез финансови средства или обучение; чл.143– за принуда някои да извърши, да пропусне или да претърпи нещо, противно на волята му, и 143а – за задържане на заложник; чл. 159 –за порнография; чл.159а – за трафик на хора; чл. 301-305 за подкуп; чл. 321 – за организиране, ръководство или участие в организирана престъпна група.

<sup>2</sup> За престъпления по време на избори.



## 7. Подготовка за прилагане на СРС

При необходимост от използване на СРС, когато са изчерпани всички други оперативни способности за разкриване на престъпна дейност, службата-заявител *съгласува* с оперативно-техническата служба условията и възможностите за прилагане на СРС. Макар, че това съгласуване може да се извърши в работен порядък, то е необходимо поради твърде сложната процедура по прилагане на СРС като гаранция за техническите и оперативни възможности на изпълнителя.

В случаите, когато специалните разузнавателни средства ще се използват за опазване на живота или имуществото на лице или свидетел по наказателно производство (чл. 12, ал. 2 и 3), към искането се прилага и неговото писменото съгласие, оформено като **ДЕКЛАРАЦИЯ** по бланка - образец.

След като се попълни по посочения начин, искането се подписва от административния ръководител на органите по чл. 13 ал. 1 или наблюдаващия прокурор и се представя на Председателя на Софийски градски съд, на съответния окръжен съд или на специализирания наказателен съд. Искането може да бъде представено и на заместник-председател, писмено оправомощен от горните лица. За военнослужащи документите се представят на председателите на съответните окръжни военни съдилища (чл. 15 ал.1). Посочените по-горе ръководители на съдилища в срок до 48 часа дават писмено разрешение за използването на специални разузнавателни средства или отказват използването им, като мотивират актовете си. Посоченият срок е съкратен до 24 часа, когато искането е във връзка с борбата с тероризма.

Заявителят е длъжен да предостави на органа, издаващ разрешението, всички материали, на които се основава искането.

Разрешение за използването на специални разузнавателни средства по отношение на всички участници за престъпления, осъществени от съдии, прокурори и следователи, се дава от председателя на Софийския апелативен съд или от изрично оправомощен от него заместник-председател, ако делото е подсъдно на Софийския градски съд; в останалите случаи разрешението се дава от председателя на Военно-апелативния съд или от председателя на апелативния специализиран наказателен съд или от оправомощен техен заместник;

Разрешение за използване на СРС спрямо председател на Софийския апелативен съд, Военно-апелативния съд и апелативния специализиран наказателен съд и негов заместник се дава от заместник-председателя на Върховния касационен съд, ръководещ Наказателната колегия.

Органът издава писмено **РАЗРЕШЕНИЕ** по бланка-образец. Разрешението се извежда в специалния регистър на компетентния съд и заедно с предоставеното искане се връчват на изготвилния го.

След получаване на писменото разрешение председателят на Държавна агенция „Технически операции“ или писмено оправомощеният от него заместник-председател дава писмено **РАЗПОРЕЖДАНЕ** за прилагане на специалните разузнавателни средства.

Законът за СРС е предвидил два случая за съкращаване на процедурата. В неотложни случаи в съответствие с чл. 17 прилагането на специални разузнавателни средства може да започне веднага след получаване на писменото разрешение по чл. 15, за което незабавно се уведомява председателят на Държавна агенция „Технически операции“ или писмено оправомощеният от него заместник-председател, съответно председателят на Държавна агенция "Национална сигурност" или писмено оправомощеният от него заместник-председател или главният секретар на МВР или писмено оправомощеният от него заместник-главен секретар. На оперативно-техническата служба освен искането, разрешението и справката се предоставя подписано **УВЕДОМЛЕНИЕ** по образец, в което задължително се посочва датата, часа и по какъв начин е извършено.

Във втория случай, съгласно чл.18 от ЗСРС при непосредствена опасност за извършване на тежки умишлени престъпления или заплаха за националната сигурност СРС могат да се използват и без разрешение на съда, а само въз основа на разпореждане председателя на ДАТО (председателя на ДАНС или главния секретар на МВР), а в негово отсъствие от оправомощения заместник-председател на ДАТО или ДАНС. Използването се прекратява, ако в срок от 24 часа не бъде дадено разрешение от органа по чл. 15, който се произнася по съхраняването или унищожаването на събраната информация. При получаване на разрешение събраната информация може да бъде запазена и използвана.

## 8. Осигуряване и прилагане на СРС от оперативно-техническите служби

СРС се осигуряват и прилагат съгласно чл. 20 (1) от ЗСРС единствено от Държавна агенция "Технически операции" и от специализирана дирекция "Технически операции" на Държавна агенция "Национална сигурност и техните структурни звена в страната. Министерството на вътрешните работи има право да осигурява и прилага специални разузнавателни средства по чл. 10б и 10в (доверителна сделка и служител под прикритие), както и за специални разузнавателни средства по чл. 10а (контролирана доставка), в случаите, когато се използва служител под прикритие.

Съгласно чл. 21 ал.1 срокът за прилагане на специални разузнавателни средства е до:

1. двадесет дни в случаите на чл. 12, ал. 1, т. 4<sup>1</sup>;
2. две години по отношение на дейности, свързани със защитата на националната сигурност в случаите на предотвратяване на тежки умишлени престъпления по глава първа от особената част на Наказателния кодекс<sup>2</sup>;
3. два месеца в останалите случаи.

В случай на необходимост срокът по ал. 1 може да бъде продължен по реда на чл. 15:

1. до двадесет дни, но за не повече от шестдесет дни общо в случаите по ал. 1, т. 1;
2. за не повече от три години общо в случаите по ал. 1, т. 2;
3. за не повече от шест месеца общо в случаите по ал. 1, т. 3.

В случай на необходимост от продължаване на срока заявителя изготвя ново искане и го предоставя на органа, дал първоначалното разрешение. Искането и полученото разрешение се предоставят в оперативно-техническата служба преди изтичане на срока на първото разрешение. В искането за продължение задължително се отразяват извършените до момента действия, получените резултати от използването на СРС и причините, които налагат продължаване на срока.

Използването на специалните разузнавателни средства от органите по чл. 22, ал. 1 и 2 се прекратява:

- с изтичане на срока на разрешението;
- когато е постигната предвидената цел с използването им;
- когато използването не дава резултати.

В първия случай прекратяването се извършва служебно от органа, прилагащ СРС. В последните два случая органът, заявил прилагането на СРС уведомява писмено изпълнителя.

Оперативно-техническите органи могат да не започнат прилагането на СРС или да го прекратят в процеса на използването му (чл. 22 ал.3), когато:

- когато е дадено разрешение за прилагане на специални разузнавателни средства за разкриване на престъпления, извън посочените в чл. 3, ал. 1;
- при явни фактически грешки в искането на органа по чл. 13 или в разрешението на органа по чл. 15;
- е налице конкретна опасност от разкриване на СРС при получаване на данни за това;
- по технически или други причини е невъзможно прилагането на СРС или то не може да продължи.
- при възникване на опасност за живота или здравето на служителя под прикритие или на неговите възходящи, низходящи, братя, сестри, съпруг или лица, с които се намира в особено близки отношения, когато опасността произтича от възложените задачи.

В тези случаи ръководителят на оперативно-техническата структура разпорежда прекратяване прилагането на СРС, като в писмен вид уведомява незабавно заявителя и органа, дал разрешението.

В първите два случая органът по чл. 20 незабавно писмено уведомява органа, издал разрешението, както и заявителя. Органът по чл. 15 отменя, изменя или потвърждава разрешението, изпраща своя акт на органа по чл. 20 и уведомява органа по чл. 13. След получаване на съдебния акт, с който разрешението е изменено или потвърдено, органът по чл. 20 незабавно предприема действия по прилагане на специалните разузнавателни средства.

Ефективността от прилагането на СРС зависи много от взаимодействието между заявителя и оперативно-техническата служба. По тази причина на оперативно-техническата служба трябва да се предоставят пълни, изчерпателни и актуални данни за лицето и обекта, спрямо които се прилага СРС, и да подпомогнат създаването на условия за осигуряване на оперативните способности.

<sup>1</sup> Когато става дума за обекти за установяване самоличността на лицата, подготвящи, извършващи или извършили тежки умишлени престъпления.

<sup>2</sup> Престъпления против републиката: измяна; предателство и шпионство; диверсия и вредителство; други престъпления.

## 9. Използване на резултатите от прилагане на СРС

В процеса на прилагане на СРС оперативно-техническата служба, след получаване на информация, която засяга целта на искането, предоставя резултатите на хартиен или друг носител, във вид, съгласуван със заявителя, като ги изпраща за оценка. Информацията трябва да съответства на информацията от използването на СРС, записана върху материален носител. Материалните носители се съхраняват в оперативно-техническата служба за целия срок на използване на СРС. Върху документа се поставя гриф за сигурност, съответстващ на грифа за сигурност върху искането за използване на СРС. По писмено искане, подписано от ръководителя на органа - заявител, оперативно-техническата служба заедно с документа може да изпраща снимки, скици или записи. Ако в оперативно-техническата служба са налице условия и има такава оперативна необходимост, на заявителя се осигурява възможност за запознаване със събираната информация. При наличие на техническа възможност структурата по чл. 20, ал. 1 предоставя достъп до информацията чрез автоматизирана информационна мрежа.

Когато при използването на оперативните способности са получени резултати, нямащи отношение към направеното искане, а са от компетентността на други органи по чл. 13 от ЗСРС, председателят на Държавна агенция „Технически операции“ в срок от 24 часа уведомява заявителя за получените резултати. От своя страна заявителят уведомява компетентния орган за тях в срок от 24 часа от получаването на уведомлението.

Когато резултатите се отнасят до заявителя или негов ръководител, председателят на Държавна агенция „Технически операции“ или писмено оправомощеният от него заместник-председател, съответно председателят на Държавна агенция "Национална сигурност" или писмено оправомощеният от него заместник-председател, изпраща материалите незабавно на главния прокурор или на писмено оправомощения от него заместник главен прокурор.

Когато органът, направил искането за използване на СРС, прецени, че е постигната предвидената цел преди изтичане на срока, незабавно уведомява оперативно-техническата служба за прекратяване използването на СРС и писмено изисква изготвянето на ВДС и протокол, отразяващ неговото изготвяне. Същото се отнася и за случая, когато е изтекъл срокът за използване на СРС и е постигната предвидената цел. Тогава органът, направил искането, не по-късно от десет дни след изтичане на срока, писмено изисква от съответната оперативно-техническа служба изготвянето на ВДС и протокол, отразяващ неговото изготвяне.

Оперативно-техническата служба изготвя ВДС и протокола в два екземпляра и ги предава в запечатан вид на органа, направил искането за използване на СРС и на органа, издал разрешението. Това трябва да се извърши в срок от 24 часа от изготвянето на ВДС и протокола в съответствие с изискването на НПК. Когато това е необходимо за нуждите на наказателното производство, при използване на специални разузнавателни средства наблюдаващия прокурор може да постанови веществените доказателствени средства да се изготвят в повече от два екземпляра. В тези случаи в срок до 24 часа от изготвянето на веществените доказателствени средства запечатан екземпляр се изпраща на органа по чл. 15, а останалите екземпляри се изпращат на наблюдаващия прокурор.

Протоколът, отразяващ изготвянето на ВДС, се изготвя от оперативно-техническата служба, която е приложила СРС, и в него се посочват:

1. времето и мястото на прилагането на специалните разузнавателни средства;
2. видовете използвани оперативни способности и технически средства;
3. получените данни за контролираните лица и обекти;
4. текстовото възпроизвеждане на съдържанието на вещественото доказателствено средство;
5. условията, при които са възприети резултатите от ползването.

Към протокола могат да се приложат скици, планове, схеми и други графични изображения, ако естествено се налага тяхното изготвяне.

Когато използването на СРС е по искане на лица за опазване на живота или имуществото им, към него се прилага и тяхната писмена декларация за съгласие.

Когато използването на СРС е започнало по условията и реда на чл. 17 от ЗСРС (след получено разрешение от съда и уведомяване на председателя на ДАТО или председателя на ДАНС) към протокола се прилага и писменото уведомление.

Протоколът се изготвя върху бланка по образец и се подписва от ръководителя на оперативно-техническата служба.

Веществените доказателствени средства се съхраняват от органите по чл. 13, ал. 1 до образуване на досъдебното производство. След образуване на досъдебното производство веществените доказателствени средства се съхраняват от съответните органи на съдебната власт.

Унищожаване на събраните данни и писмените документи се извършва в десетдневен срок от прекратяване на прилагането на специалното разузнавателно средство. Това се извършва от комисии, назначени със заповед от ръководителите на службата-заявител и оперативно-техническата служба. Комисиите, извършили унищожаването, съставят протокол с подробна спецификация на всички унищожени материални носители и документи.

Информацията по линия защита на националната сигурност (чл. 21, ал. 1, т. 2 и ал. 2, т. 2) се съхранява от съответната специализирана дирекция, териториална дирекция или самостоятелен териториален отдел на Държавна агенция "Национална сигурност", от служба "Военно разузнаване" към министъра на отбраната или от Държавна агенция разузнаване за срок до 15 години. Срокът започва да тече от прекратяване на прилагането на специалното разузнавателно средство.

Необходимо е да се знаят някои важни особености на информацията, получена с помощта на СРС:

- резултатите, получени чрез СРС, не могат да бъдат използвани за друго, освен за предотвратяване, разкриване и доказване на престъпления при условия и по реда, посочени в Закона за специалните разузнавателни средства.
- оперативни работници, на които са станали известни факти и сведения, придобити чрез СРС, са длъжни да не ги разгласяват;
- обвинението и присъдата съгласно чл.177, ал.1 от НПК не могат да се основават само на ВДС, изготвени чрез СРС.

## 10. Контрол и наблюдение върху прилагането на СРС

Контролът върху прилагането и използването на СРС се осъществява от председателя на Държавна агенция „Технически операции“, когато специалните разузнавателни средства се прилагат и използват от агенцията, от председателя на ДАНС, когато СРС се прилагат и използват от структурите на ДАНС или от министъра на вътрешните работи, когато се прилагат и използват специални разузнавателни средства по чл. 10в в ЗМВР. Ръководителите на структурите на оперативно-техническите служби осъществяват контрол за правомерното прилагане на СРС.

Оперативен контрол, обаче, осъществява и съдията, издал разрешението. В едномесечен срок след прекратяване прилагането на СРС органът по чл. 13 е длъжен да предаде доклад на съдията, който трябва да съдържа данни за вида, началото и края на прилагане на СРС, изготвени ли са ВДС, както и дали е унищожена събраната чрез тях информация.

Председателите на окръжните или апелативните съдилища, дали разрешения за използване на СРС, включват в годишните си доклади данни за броя на издадените разрешения и изготвените ВДС.

Контролът върху прилагането на СРС се осъществява от възстановеното през 2013 г. Национално бюро. Националното бюро за контрол на специалните разузнавателни средства е независим държавен орган, който осъществява наблюдение на процедурите по разрешаване, прилагане и използване на специалните разузнавателни средства, съхраняването и унищожаването на информацията, получена чрез специални разузнавателни средства, както и за защита на правата и свободите на гражданите срещу незаконосъобразното използване на специални разузнавателни средства.

Националното бюро е колегиален орган и се състои от 5 членове, включително председател и заместник-председател, които се избират от Народното събрание за срок 5 години. Националното бюро е постоянно действащ орган, който се подпомага от администрация. При встъпването си в длъжност членовете и служителите подписват декларация, че няма да разгласяват информацията по време на заемане на длъжността и след освобождаването им.

Членове на Националното бюро могат да бъдат само дееспособни български граждани, които имат не по-малко от 8 години юридически стаж или професионален стаж в службите за сигурност или в службите за обществен ред и са получили разрешение за достъп до класифицирана информация с ниво на класификация „Строго секретно“.

Предложенията за членове на Националното бюро се внасят в Народното събрание, придружени от автобиография, документ за професионален стаж, свидетелство за съдимост, медицинско удостоверение, че лицето не страда от психическо заболяване, необходимите документи за извършване на проучване за надеждност по смисъла на Закона за защита на класифицираната информация.

Председателят на специализираната постоянна комисия на Народното събрание изпраща в Държавна агенция „Национална сигурност“ документите на кандидатите за членове на Националното бюро за извършване на проучване за надеждност. Държавна агенция „Национална сигурност“ извършва специално проучване по смисъла на Закона за защита на класифицираната информация в едномесечен срок. Комисията изслушва кандидатите, които отговарят на изискванията на закона, и в 7-дневен срок от провеждането на изслушването внася доклад, който обобщава резултатите от него.

Народното събрание избира поименно членовете на Националното бюро, а от членовете на бюрото избира председател и заместник-председател. След избора членовете на Националното бюро полагат пред Народното събрание клетва.

Националното бюро ежегодно до 31 май внася в Народното събрание доклад за извършената дейност, който съдържа обобщени данни за разрешаването, прилагането и използването на специалните разузнавателни средства, съхраняването и унищожаването на информацията, получена чрез тях, както и за защита на правата и свободите на гражданите срещу незаконосъобразното използване на специални разузнавателни средства.

Народното събрание чрез постоянна комисия осъществява парламентарен контрол върху държавните органи, които извършват дейностите по разрешаване, прилагане и използване на специалните разузнавателни средства. Длъжностните лица, когато бъдат поканени, са длъжни да се явяват пред комисията и да предоставят исканата информация.

Националното бюро уведомява служебно гражданите, когато спрямо тях са били прилагани неправомерно специални разузнавателни средства.

Гражданите не се уведомяват, когато това ще създаде опасност:

1. за постигане на целите по чл. 3 или чл. 4 от ЗСРС;

2. от разкриване на оперативните способности или техническите средства;

3. за живота или здравето на служителя под прикритие или на неговите възходящи, низходящи, братя, сестри, съпруг или лица, с които се намира в особено близки отношения, когато опасността произтича от възложените задачи.

При наличие на данни за неправомерно използване и прилагане на специални разузнавателни средства, съответно съхраняване или унищожаване на придобитата чрез тях информация, Националното бюро сезира органите на прокуратурата и ръководителите на органите и структурите по чл. 13, 15 и 20.