ПЪРВОНАЧАЛЕН БРИФИНГ ЗА РАБОТА С КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА НАТО

Въведение

В изпълнение на Вашите служебни задължения Ви е необходим достъп до класифицирана информация на НАТО.

В този първоначален брифинг по сигурността се посочва задължителният минимум информация, който Ви е необходим за работа с класифицирана информация на НАТО (NATO Classified Information). Необходимо е да познавате основните стандарти и процедури за сигурност на класифицираната информацията на НАТО, които в някои случаи се различават от стандартите и процедурите, прилагани за работа с национална класифицирана информация.

Какво е НАТО?

На **4 март 1947** г. Франция и Великобритания подписват т.нар. Договор от Дюнкерк – Договор за съюз и взаимопомощ в случай на евентуално нападение от страна на Германия или Съветския съюз[1] след края на Втората световна война. През 1948 г. към този Алианс се присъединяват страните от Бенелюкс – Белгия, Нидерландия и Люксембург. Междувременно се обсъжда присъединяването и на страните от Северна Америка към договора.

На **4 април 1949** г. е подписан Северноатлантическият договор, като освен вече посочените държави, в него се включват Съединените американски щати, Канада, Португалия, Италия, Норвегия, Дания и Исландия. По такъв начин 12 държави основават Организацията на Северноатлантическия договор – англ. North Atlantic Treaty Organization, с абревиатура NATO (бълг. НАТО).

През 1952 г. се присъединяват Гърция и Турция. Западна Германия се присъединява през 1955 г.; Испания – през 1982 г.; Чехия, Унгария и Полша – 1999 г.; България, Естония, Латвия, Литва, Румъния, Словакия, Словения – 2004 г.; Албания и Хърватия – 2009 г.; Черна гора – 2017 г.; Северна Македония – 2020 г.

Към настоящия момент в НАТО членуват общо 30 държави.

Емблемата на НАТО е утвърдена от Северноатлантическия съвет през октомври 1953 г. като символ на Атлантическия съюз. Кръгът символизира единството и сътрудничеството, а розетката на компаса показва общия път към мир, който следват страните членки на Алианса.

[1] Съюз на съветските социалистически републики (СССР) или съкратено „Съветски съюз“.

Национален орган по сигурността

Всяка държава членка на НАТО има Национален орган по сигурността (НОС), отговорен за сигурността на класифицираната информация на НАТО. Националният орган по сигурността:

– Отговаря за сигурността на класифицираната информация на НАТО в националните военни или цивилни структури и елементи в страната или чужбина.

– Провежда периодични проверки на мерките за сигурност на класифицираната информация на НАТО във всички национални органи, на всички нива, военни и цивилни, за да установи дали мерките за сигурност са в съответствие с актуалните правила на НАТО за сигурност.

– Гарантира, че е извършена процедура по проучване за надеждност на всички лица, за които се изисква достъп до класифицирана информация с ниво NATO CONFIDENTIAL и по-високо, в съответствие с Политиката на НАТО по сигурността C-M(2002)49.

– Гарантира, че националните планове за действие при извънредни ситуации са подготвени по начин да предотвратят нерегламентиран достъп до класифицирана информация на НАТО или попадането ѝ във враждебни ръце.

– Разрешава откриването или закриването на Централни регистратури COSMIC TOP SECRET.

Държавната комисия по сигурността на информацията (ДКСИ) е Национален орган по сигурността в Република България въз основа на международните договорености и притежава изброените по-горе правомощия. Законът за защита на класифицираната информация (ЗЗКИ), приет през 2002 г., конкретизира тези, като предоставя и други правомощия на ДКСИ за общо ръководство и контрол на мерките по защита както на националната, така и на чуждестранната класифицирана информация, вкл. класифицираната информация на НАТО.

Законът определя ДКСИ като държавен орган, който осъществява политиката на Република България за защита на класифицираната информация, вкл. за защита на класифицираната информация на НАТО (по смисъла на чл. 4, ал. 1 във връзка с чл. 1, ал. 3 от ЗЗКИ).

В качеството на НОС и държавен орган по сигурността на информацията Комисията организира, осъществява, координира и контролира дейността по защитата на класифицираната информация и осигурява еднаквата ѝ защита (чл. 8 от ЗЗКИ), вкл. извършва това и по отношение класифицираната информация на НАТО. По-конкретно, ДКСИ:

– организира и осигурява функционирането на регистратурите в областта на международните отношения, респ. Централната регистратура за класифицирана информация на НАТО и нейните подрегистратури в организационните единици;

– организира, контролира и отговаря за изпълнението на задълженията за защита на класифицираната информация, съдържащи се в международни договори, по които Република България е страна, вкл. съдържащи се в Северноатлантическия договор, политиките и директивите на НАТО;

– издава сертификати, потвърждаващи пред чуждестранни власти, че български физически или юридически лица притежават разрешение, съответно удостоверение, вкл. по линия на сътрудничеството с НАТО;

– извършва съвместно със службите за сигурност проучване на български граждани, които кандидатстват за заемане на длъжности или за изпълнение на конкретно възложени задачи, налагащи работа с класифицирана информация на друга държава или международна организация, вкл. НАТО, след постъпване на писмено искане от компетентния орган за сигурност на информацията на съответната държава или международна организация, вкл. НАТО;

– дава разрешения за посещение на лица за извършване на инспекции, провеждани по силата на международни договори за взаимна защита на класифицираната информация, вкл. по линия на НАТО (чл. 9, т. 5, 6, 10 и 11 от ЗЗКИ).

Политика на НАТО по сигурността C-M(2002)49-COR 12

Политиката на НАТО по сигурността C-M(2002)49 е приета с процедура на мълчание на 26 март 2002 г. и заменя предишния документ с номер C-M(55)15(Final).[2]

C-M(2002)49 е съставен от няколко приложения:

- Приложение **C** – Директива по персонална сигурност AC/35-D/2000-REV7;
- Приложение **D** – Директива по физическа сигурност AC/35-D/2001-REV2;
- Приложение **E** – Директива по сигурността на информацията AC/35-D/2002-REV4;
- Приложение **G** – Директива за класифицираните проекти и индустриалната сигурност AC/35-D/2003-REV7;
- Първична директива по сигурността на КИС AC/35-D/2004-REV3;

[2] Значението на числото в скобите на номера на документа е годината на одобряването му.

– Директива по управление на сигурността на КИС AC/35-D/2005-REV3.

Какво е класифицирана информация на НАТО?

Класифицирана информация на НАТО е информация, подготвена от или за НАТО, или вътрешна информация на държава членка, предоставена на НАТО за целите на сигурността. Защитата на тази информация се контролира въз основа на правила за сигурност на класифицирана информацията на НАТО и достъпът до нея се определя от държателя (притежателя – англ. holder) на информацията, ако източникът (изготвителят – originator) на класифицираната информация не е наложил ограничения към момента на изпращането ѝ в НАТО.

Класифициран материал, получен от организация или друга държава членка на НАТО, може да съдържа или класифицирана информация на НАТО, подготвена от структура на НАТО, или вътрешна информация, подготвена от държава членка на НАТО. Ако държавата източник на класифицирана информацията е обозначила материала с NATO, трябва да се приеме, че в него се съдържа класифицирана информация, предоставена на НАТО, и тя се контролира съгласно Програмата за сигурност на класифицираната информацията на НАТО (NATO Security Program).

> **Запомнете!** Ако материалът носи вътрешен гриф за сигурност и няма гриф NATO, поставен от източника на информацията, не използвайте гриф NATO, освен ако не сте информирани в писмена форма от източника на информацията, че материалът е предназначен за НАТО и трябва да бъде защитен съгласно Програмата за сигурност на класифицираната информацията на НАТО! Класифицираният материал или класифицираната информация в него не трябва да се изпраща в системата на НАТО без предварителното писмено съгласие на източника (originator) на класифицирана информация.

Класифицирана информация на НАТО е информация:

– Създадена от НАТО;

– Създадена от страна членка и предоставена на НАТО;

– Създадена от страна членка и предоставена на друга страна членка във връзка с работа по програма, проект или договор на НАТО.

Нива на класификация и гриф за сигурност (classification markings)

НАТО има четири нива на класифицирана информация (NATO Classified Information – NCI):

– COSMIC TOP SECRET (CTS – „Строго секретно“ на НАТО);[3]
– NATO SECRET (NS – „Секретно на НАТО“);[4]
– NATO CONFIDENTIAL (NC – „Поверително на НАТО“),[5] и
– NATO RESTRICTED (NR – „С ограничен достъп, на НАТО“).[6]

COSMIC TOP SECRET (CTS). Този гриф за класификация (security classification) се използва за информация, чието неразрешено разкриване би причинило изключително тежки вреди за НАТО.

> **Запомнете!** Думата COSMIC обозначава СТРОГО СЕКРЕТЕН материал, притежание на НАТО. Терминът NATO TOP SECRET не се използва!

NATO SECRET (NS). Този гриф за класификация се използва за информация, чието неразрешено разкриване би причинило сериозни вреди на НАТО.

NATO CONFIDENTIAL (NC). Този гриф за класификация се използва за информация, чието неразрешено разкриване би нанесло вреда на интересите на НАТО.

NATO RESTRICTED (NR) – този гриф за класификация се използва за информация, неразрешеното разкриване на която би било неблагоприятно за интересите на НАТО.

> **Запомнете!** НАТО разграничава също така служебна, некласифицирана информация (official, unclassified information).

NATO UNCLASSIFIED (NU). Това обозначаване се използва за служебна информация, която е притежание на НАТО, но не отговаря на критериите за класифицирана информация. Достъпът до информация от структури извън НАТО е разрешен, когато подобен достъп не би бил във вреда на НАТО. Информацията, обозначена с NATO UNCLASSIFIED, е информация,

[3] COSMIC TOP SECRET се произнася „космик топ сикрет“; CTS – „Сий Тий Ес“.
[4] NATO SECRET се произнася „нейто сикрет“; NS – „Ен Ес“.
[5] NATO CONFIDENTIAL се произнася „нейто конфиденшъл“; NC – „Ен Сий“.
[6] NATO RESTRICTED се произнася „нейто рестриктед“; NR – „Ен Аар“.

подобна на официалната информация, която трябва да бъде прегледана преди да стане обществена.

От средата на 2002 г. НАТО изисква класифицирана информация да бъде обозначавана параграф по параграф, т.е. с надпис за сигурност към всеки заглавен параграф и т.н.

Сертификат за достъп до класифицирана информация на НАТО

Служителят по сигурността на информацията ще ви информира за вашето ниво на достъп до класифицирани материали на НАТО. Освен това в организационната единица се поддържа списък, в който са посочени нивата на достъп за всяко назначено лице, което има сертификат за достъп до информация на НАТО, за да може Вие да проверявате сертификатите за достъп до класифицирана информация на НАТО за други служители.

> **Запомнете!** Достъпът не се определя от заеманата длъжност, ранга или нивото на сертификата за достъп до класифицирана информация на неговия притежател. Достъпът е основан на принципа „необходимост да се знае“ (need-to-know).
>
> **Запомнете!** Принципът „необходимост да се знае“ се състои в ограничаване на достъпа само до определена класифицирана информация и само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп и които едновременно с това притежават сертификат за достъп със съответното ниво класификация и са преминали инструктаж за достъп до конкретното ниво и вид класифицирана информация на НАТО.
>
> **Запомнете!** Преди да предоставите достъп на някого, Ваше задължение е да се уверите, че лицето, на което предоставяте достъпа, има сертификат за достъп до конкретен вид или/и ниво на класифицирана информация на НАТО. Това Ваше задължение се отнася до всички форми на предаване на информация, напр. устна, писмена, визуална и електронна. При съмнение, потърсете помощ от вашия ръководител/офицер по сигурността (security officer) или от централната регистратура на НАТО, подрегистратура на НАТО или контролен пункт (control point).
>
> **Запомнете!** Само след одобрението на източника на информацията Вие можете да предоставите информация на НАТО на страни и организации, които не са членки на НАТО. Задължително следва да получите такова предварително одобрение чрез съответния комитет на НАТО.

Регистратури за класифицирана информация на НАТО

Във всяка държава членка на НАТО се създава Централна регистратура (Central Registry) за осигуряване на контрол и отчетност на класифицираните материали на НАТО при получаването, отчета, обработването, разпространението и унищожаването на такава информация.

Всяка държава членка на НАТО може да създаде до две Централни регистратури до ниво COSMIC TOP SECRET, действащи като главни точки за приемане и предаване информация на НАТО за съответната държава. Централните регистратури могат да изпълняват функции на „обикновени“ регистратури и за друга отчетна информация.

> **Запомнете!** Според директивите на НАТО отчетна е информацията до нива COSMIC TOP SECRET и NATO SECRET.

Отчетността на COSMIC TOP SECRET и NATO SECRET задължително се извършва чрез системата от регистратури, за останалите две нива на класификация – NATO CONFIDENTIAL и NATO RESTRICTED, не се изисква информацията да минава през системата от регистратури, освен ако не е предвидено друго като изрично изискване в националното законодателство.

Съхранението се извършва в съответствие с изискванията на Политиката на НАТО по сигурността C-M(2002)49 и Приложение D – Директива по физическа сигурност AC/35-D/2001.

Служители от регистратури за национална класифицирана информация могат да отговарят за класифицирана информация на НАТО, ако са получили сертификат за достъп до класифицирана информация на НАТО и са инструктирани.

Регистратурата на Държавната комисия по сигурността на информацията с ниво COSMIC TOP SECRET е Централна регистратура на НАТО в Република България. На територията на Република България организационните единици създават свои подрегистратури и контролни пунктове (control points) въз основа на своето местонахождение и обема класифицирани материали на НАТО, с които работят.

Отчитане до ниво COSMIC TOP SECRET и NATO SECRET

При получаване, разпореждане (изписване), унищожаване и изпращане на информация до ниво COSMIC TOP SECRET и NATO SECRET, трябва да се издават разписки и да се извършва вписване в дневник. Всяко лице трябва да

се подпише контролния лист (disclosure record) при придобиване на достъп до всяка част от материал COSMIC TOP SECRET със специални ограничения (special limitation restrictions).

Отчитане до ниво NATO CONFIDENTIAL и NATO RESTRICTED

Вие трябва да поддържате административен контрол на материали NATO CONFIDENTIAL и NATO RESTRICTED, достатъчен да не се допусне нерегламентиран достъп. Конкретни отчетни документи (accounting records) не са необходими, освен ако не се изискват от източника на информацията.

Обозначаване и отчитане на документи, съдържащи класифицирана информация на НАТО

Новосъздаден класифициран документ на дадено правителство, в който се съдържа класифицирана информация на НАТО, трябва да носи надпис за сигурност, който отразява най-високото ниво на класифицирана информация на НАТО, съдържаща се в него.

Указания за декласификация (declassification) и понижаване на степента на класификация (downgrading) следва да посочват, че информацията на НАТО е освободена от декласификация и понижаване на нивото на класификация без предварителното съгласие на НАТО.

Причината, която трябва да се посочи, е „Информация на чуждо правителство“ (Foreign Government Information). Надписът „Този документ съдържа класифицирана информация на НАТО“ (This document contains NATO classified information) се поставя на заглавната страница или на първата страница, ако няма заглавна. Части, които съдържат класифицирана информация на НАТО, трябва да се обозначават, за да се идентифицира информацията (напр. с NS).

Средства за съхранение на информация на автоматизирани информационни системи или мрежи (комуникационни информационни системи, communication and information systems, CIS) се управляват според описаното в C-M(2002)49 и съпътстващите директиви и в Раздел X на USSAN 1-69.

Съхранение на материали на НАТО

Общо. Във връзка с изискванията на Политиката на НАТО по сигурността C-M(2002)49 всички помещения, сгради, офиси, стаи и други зони, в които се съхраняват и/или обработват класифицирана информация и

материали на НАТО, трябва да бъдат защитени с подходящи мерки за физическа сигурност.

Материал с гриф NATO RESTRICTED може да се съхранява в заключваща се картотека, шкаф за книги, бюро или друг подобен контейнер или в стая или сграда, която е заключена в извънработни часове, при условие че достъпът до стаята или сградата се контролира, така че само оторизиран персонал може да получи достъп до информацията. Всички служители с достъп до контейнер, който се използва за съхранение на класифицирана информация на НАТО, трябва да бъдат инструктирани и да притежават сертификат за достъп до нивото и вида класифицирана информация на НАТО, която се съхранява в контейнера.

Разделяне (segregation). Вие трябва да осигурите отделното завеждане на материал на НАТО и не-НАТО. Това може да се постигне с използване на отделен контейнер или с използване на отделни чекмеджета или разделители на папките в същия контейнер.

Комбинации (combinations). Комбинациите на контейнери, съдържащи класифицирана материали на НАТО, трябва да се променят поне веднъж годишно при напускане на лице с достъп до комбинацията или ако комбинацията е или има съмнения, че е разкрита.

Предаване (transmission). Вътрешно или международно предаване на материали с гриф CTS се извършва през регистрационната система, като се използва оторизирана държавна куриерска служба, например: дипломатическа поща или военна куриерска служба. Вътрешното и международното предаване на материали с грифове NS и NC се извършва от оторизиран куриер или от съответно оторизирани и инструктирани служители, които притежават куриерска идентификация и оторизация, или с препоръчана поща. Разписки се изискват за материали CTS и NS.

Комуникационни и информационни системи (КИС).[7] Системите трябва да са специално оторизирани да работят с класифицирана информация на НАТО. Организации с AIS системи, оторизирани за работа с класифицирана информация на НАТО, трябва да издават указания за обработка, работа и

[7] Англ. Communication and Information Systems (CIS), съотв.: бълг. „автоматизирани информационни системи (АИС), англ. Automated Information Systems (AIS).

отчитане на класифицирана информация на НАТО. Осигурете получаване на тези указания и ги прилагайте.

Унищожаване (destruction). Унищожаването на материали CTS, NS и NC се извършва само от персонал на регистрационната система, като се използва сертификат за унищожаване и одобрен начин за унищожаването на материали на НАТО. NATO RESTRICTED и NATO CONFIDENTIAL се унищожават със средствата, разрешени за унищожаване на материали с ограничен достъп, непозволяващ възстановяване на информацията.

Процедурите по унищожаване на класифицирана информация на НАТО зависят на първо място от нивото на класификация на всеки документ/материал и съответно от начина на водене на отчет. Според чл. 53 от Директивата по сигурността на информацията AC/35-D/2002, класифицирана информация, която не е нужна за официални цели, включително излишна, заместена информация или остатъци от документи и материали, следва да бъде унищожавана по начин, непозволяващ нейното възстановяване. В този случай не трябва да се чакат инструкции за унищожаване. Следователно, особено внимание трябва да се обръща на работата с подготвителни документи и материали, които имат сравнително много кратък жизнен цикъл.

Не се регистрират и подлежат на унищожаване след приключване на работа с тях документи и материали с ниво NATO RESTRICTED.

> **Запомнете!** Документиране на унищожаването и съхраняването на контролните протоколи за информация NATO CONFIDENTIAL и NATO RESTRICTED не е задължително, освен когато е изискано от създателя или когато се изисква специално от националните правила и разпоредби по сигурността.
>
> **Запомнете!** На особен отчет и контрол подлежат материалите с гриф за сигурност COSMIC TOP SECRET. Съгласно чл. 54 от Директивата по сигурността на информацията AC/35-D/2002 цялата информация с гриф CTS следва да бъде върната в регистратурата, предназначена да я съхранява в готовност за унищожаване.

Сертификатите за унищожаване и контролните протоколи за CTS информация се съхраняват най-малко 10 години в регистратурата, за да могат да се използват при разследвания. Копия от протоколите за унищожаване не се изпращат на създателя или на съответната централна регистратура, освен ако са специално поискани. Протоколите за унищожаване на информация NATO

SECRET се съхраняват най-малко 5 години в регистратурата или в службата, извършила унищожаването.

Протоколите трябва да съдържат информация, достатъчна за извършването на оценка на вредите или за осъществяване на разследване на сигурността, компрометирането или загубата на класифицирана информация.

Според чл. 51 от Директивата по сигурността на информацията AC/35-D/2002 правилното управление на класифицирана информация на НАТО се разпростира върху целия процес на съществуване на информацията, включително премахването на нивото на класификация и унищожаването на информация. За обозначаване на този процес се използва понятието „жизнен цикъл“ на информацията, което изразява разбирането, че информацията периодично трябва да бъде преглеждана с цел преценка дали нивото на класификация трябва да бъде понижено или премахнато, както и дали информацията следва да бъде унищожена.

В Алианса се обръща особено внимание на необходимостта, потвърдена в хода на инспекциите, по-гъвкаво да се определят сроковете на защита на информацията, т.е. нейният жизнен цикъл като класифицирана информация, а не да се прилага само фиксираната в закона продължителност на защита на информация, класифицирана със съответното ниво.

Размножаване (reproduction). Документите CTS се размножават от Централната регистратура, която трябва да докладва броя направени копия пред автора на документа. Размножаването на информация с ниво NS и по-ниско може да се извършва от получателя на принципа „необходимост да се знае“ и при условие че източникът на информацията не е ограничил размножаването. Възпроизведените копия се отчитат и съхраняват по същия начин като оригинала.

Правила за работа с информация NATO UNCLASSIFIED

Понятието UNCLASSIFIED е нетипично за Република България и като правило се превежда „некласифицирано“, от което се прави извод, че информация с това обозначение подлежи на свободно разпространение. По същество обаче това не е така.

> **Запомнете!** UNCLASSIFIED обозначава информация на НАТО, която не е класифицирана, с която се работи по-свободно, но която също така не подлежи на свободно разпространяване и с нея следва да се запознават лица, чиито служебни задължения или задачи налагат това.

Работата с документи и материали, носещи обозначение UNCLASSIFIED, се регламентира от отделен документ на Алианса – Документ C-M(2002)60, който е приет в подкрепа на документ Политика за управление на информацията на НАТО (PO(99)47).

В Документ C-M(2002)60 се посочва, че некласифицираната информация на НАТО се дели на две категории:

– маркирана с UNCLASSIFIED, която може да носи административна маркировка или ограничителни разпореждания до адресатите и чието разпространение става по определени процедури (параграфи 11-15).

– некласифицирана информация, определена за публично предоставяне, която задължително не носи каквито и да било маркировки.

За работата с некласифицирана информация на НАТО също се прилагат някои основни изисквания, като например за осигуряване на нейната цялост и достъпност и дори публично предоставяната информация трябва да отговаря на тези изисквания. Промяната на съдържанието се разглежда като загуба на целостта, а невъзможността за достъп до такава информация – като загуба на наличността. Смята се, че всяка загуба на целостта и/или загуба на наличността дори на некласифицирана информация на НАТО може да доведе до настъпване на вреди за интересите на Алианса.

Административните ограничения са свързани с основния характер на информацията като „търговска“, „управленска“, „медицинска“, „лична“… Към работата с некласифицирана информация на НАТО, носеща административни ограничения, също се поставят изисквания за защита от нерегламентиран достъп, за пренасяне (в един непрозрачен пощенски плик и обикновени пощенски услуги) и за унищожаване (така че да е невъзможно нейното разпознаване или възстановяване).

Мерки за сигурност се прилагат и при създаване, обработване и съхраняване на маркирана с административни ограничения информация в електронна среда и при използване на магнитни носители. При това трябва да бъде създадена и поддържана обкръжаваща среда, която да осигурява постигането на следните цели: защита на поверителния характер на информацията; защита целостта на информацията и поддържане на системните услуги и ресурси; защита наличността на информацията и поддържане на системните услуги и ресурси.

Мерките за сигурност на всички автоматизирани информационни системи, работещи с информация NATO UNCLASSIFIED трябва да отговарят на следните основни изисквания: да осигуряват надеждно разпознаване и

установяване на самоличността на лицето с разрешен достъп до такава информация и да дават възможност за контрол върху достъпа съобразно принципа „необходимост да се знае“.

Нарушаване на сигурността и възможна загуба/разкриване на класифициран материал на НАТО

Нарушение на мерките за сигурност (breach of security, security breach). Нарушението на мерките за сигурност е действие или бездействие, противоречащо на съществуващите общи или местни правила на НАТО за сигурност, резултатите от които могат да застрашат или изложат на риск класифицираната информация.

Излагане на риск (compromise). Излагането на риск е загуба на поверителността, целостта или достъпността на класифицираната информация заради нарушение на мерките за сигурност или заради вражески действия (като шпионаж, тероризъм, саботаж или кражба). Включва например, предоставяне или риск от предоставяне на лица без разрешение или например, физическа загуба или риск от загуба.

> **Запомнете!** Ако намерите материал на НАТО, който не е обезопасен и е оставен без внимание, незабавно се свържете с вашия офицер по сигурността или завеждащия регистратура. Останете с материала и изчакайте пристигането на офицера по сигурността или завеждащия регистратурата. Не размествайте мястото или материала. Не позволявайте на друго лице да пипа в зоната или неоторизиран персонал да има достъп до материала.
>
> Ако се налага да напуснете зоната преди вашия офицер по сигурността или завеждащия регистратура да осигури съхранение, поставете материала в контейнер и го заключете. Ако контейнерът вече е заключен и вие нямате оторизиран достъп или няма контейнер, занесете материала директно на съответно оторизирания служител по сигурността или в регистратурата, изложете обстоятелствата и получете разписка за материала.

Шпионаж, саботаж (диверсия), тероризъм и умишлено разкриване

Информация относно умишлено разкриване на материал на НАТО, опит за шпионаж или действителен шпионаж, насочен срещу информация на НАТО, или действителна или планирана терористична или диверсионна дейност срещу съоръжения или ползватели на класифицирани материали на НАТО

трябва да се докладва веднага на вашия офицер по сигурността. По-долу са представени типичните случаи, които подлежат на докладване:

1. Опити от неоторизирани лица да получат класифицирана информация относно съоръжения, дейности, персонал или материали на НАТО, вкл. чрез задаване на въпроси, извличане на информация (разузнаване), подкупване, заплахи или принуда (насилие) или/и чрез преки или непреки контакти или кореспонденция.

2. Опити от неоторизирани лица да получат класифицирана информация чрез фотографиране, подслушване на телефонни разговори, подслушване, наблюдение или с други средства.

3. Опити от лица с известно, подозирано или възможно чуждестранно разузнавателно минало, връзки или дейности за установяване на приятелски, социални или бизнес отношения или опити да ви задължат чрез специално отношение, услуги, подаръци, пари или други средства.

4. Информация относно терористични планове и дейности, представляващи директна заплаха за съоръжения, формирования, персонал или материали на НАТО.

5. Известни или подозирани действия или заговори за увреждане или разрушаване на имущество на НАТО чрез саботаж.

Запомнете! Всеки с достъп до класифицирана информация на НАТО може да бъде потенциална мишена. Ако узнаете за дейности, като описаните по-горе, или някой се обърне към Вас директно, за да ви включи в подобни дейности, не забравяйте следното:

1. **Запазете спокойствие!** Не сте виновни, че са Ви избрали за мишена.
2. **Не изразявайте отношение!** Бъдете неопределени дали ще предоставите или няма да предоставите материала или информацията!
3. **Докладвайте за случая веднага!** Дори и да изглежда чисто съвпадение или незначително, малък детайл може да бъде ключът към откриването и парирането на шпионаж, саботаж или терористичен акт. Не обсъждайте инцидента с приятели, семейството, колеги и др., освен ако не е указано от Вашия офицер по сигурността или представител на контраразузнаването!
4. **Никога не е прекалено късно** да докладвате, че сте предоставили материал или информация на неоторизиран получател.
5. **Докладвайте!**

Пътуване в чужбина

Вашите лични пътувания няма да бъдат ограничени само поради факта, че имате достъп до класифицирана информация на НАТО. Но има рискове, които са свързани с пътувания в някои страни. Обърнете се към офицера по сигурността за консултация и съдействие. Ако решите да пътувате до страни с висок риск, Вие трябва да съгласувате с Вашия ръководител, който разрешава отпуска за пътуване и с офицера по сигурността и да получите инструктаж за сигурността по време на пътуването. При завръщане следва да докладвате за всеки случай, който може да е представлявал опит за събиране на информация от особено значение.

Помощ

Запомнете! При проблеми или по конкретни въпроси, свързани с класифицирана информация на НАТО, Вашият служител по сигурността и завеждащ регистратура/контролен пункт могат да Ви помогнат.