СИГУРНОСТ НА ИНФОРМАЦИЯТА И ВИДОВЕ ЗАЩИТА

Ас. Стоян Боянов, Мариян Митков, Стоян Гаров
Университет по библиотекознание и информационни технологии, София

Резюме: *Докладът представя анализ върху значението на информацията в съвременното общество и държава и обосновава необходимостта от сигурност на информацията. Подходът на изследването се базира върху внимателно и систематично проучване на нормативните документи, регламентиращи видовете защита на информацията, както и позоваване на вече публикувани научни изследвания по темата. Предложено е сравнение на основните направления на работа в тази насока между националното законодателство и ключови документи на НАТО. Авторите поставят въпроса за пресечната точка и противоречието между концепциите за класифициране и достъп до информация от страна на гражданите. Достигнатите изводи потвърждават поставената теза в доклада и биха послужили за по-задълбочена изследователска работа по въпроса.*

Ключови думи: *достъп до информация; защита на информацията; информация; класифицирана информация; НАТО; сигурност*

SECURITY OF INFORMATION AND TYPES OF PROTECTION

Assist. Prof. Stoyan Boyanov, Mariyan Mitkov, Stoyan Garov
University of Library Studies and Information Technologies, Sofia

Abstract: *This report presents an analysis on the importance of information in modern society and state and justifies the need for security of information. The approach of the study is based on a careful and systematic study of the legislation which regulates the types of information protection, as well as references on already published scientific works on the subject. A comparison between national legislation and several NATO documents is proposed, which outlines the key directions of work in the pursuit of such security. The authors raise the question of the intersection and contradiction between the concepts of classification and access to information by citizens. The conclusions reached confirm the thesis put forward in the paper and would serve for more in-depth research work on the issue.*

Keywords: access to information; classified information; information; NATO; protection of information; security

I ВЪВЕДЕНИЕ

С оглед на увеличаващите се заплахи на национално, регионално и глобално равнище, важността на начините, по които информацията се събира, съхранява, обработва и разпространява, нараства значително. Защитата на информацията придобива нови измерения в този контекст. В същото време съвременните общества се стремят към постигане на хармония между конституционното право на обществото за информация и необходимостта от защита на информацията, както на национално ниво, така и на международно ниво. Тези съвременни измерения, касаещи достъпа до информация и

нейното класифициране, налагат допълнителен анализ на съществуващите нормативни документи в България и НАТО, както и търсене на баланс между класифицирана и общодостъпна информация.

II. КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

За целите на настоящата разработка е необходимо на първо време да бъдат посочени основните нормативни документи в Република България, които постановят концепцията на страната за защитата на информацията, създавана, обработвана и съхраняване от държавните органи на управление.

В чл. 1., ал. 3 на Законът за защита на класифицираната информация (ЗЗКИ - Обн. ДВ. бр. 45 от 30 Април 2002 г., последно изм. ДВ. бр. 13 от 13 Февруари 2024 г.) класифицирана информация (КИ) е информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация[1]. В законът са посочени и определения за различните видове класифицирана информация – държавна тайна, служебна тайна, чуждестранна класифицирана информация:

Държавната тайна представлява информация, определена в списъка по Приложение 1, нерегламентираният достъп до която би създал опасност за, или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

Служебната тайна представлява информация, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не съставлява държавна тайна, но нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правозащитен интерес.

Чуждестранната класифицирана информация представлява класифицирана информация, която е бива предоставена от друга държава или международна организация по силата на международен договор, по който Република България е страна.

Понятието "класифицирана информация" намира широко поле за изследване и доусъвършенстване през годините, като днес то се използва, за да опише информация, която е създадена или все още се създава и на която е определено конкретно ниво на класификация, тоест – мерки за защита на информацията и нейния носител. Тази информация може да бъде в различни форми, носители и начини на съхранение и предаване, като общото е, че даденото ниво на класификация изисква създаването и

[1] Закон за защита на класифицираната информация, Обн. Дв. Бр. 45 от 30 април 2002 г., последна попр. изм. Дв. Бр. 13 от 13 февруари 2024 г. – Достъпно на: https://lex.bg/laws/ldoc/2135448577

спазването на специфични мерки за защита срещу нерегламентиран достъп. Концепцията за защитата на класифицираната информация има пряко отношение към сигурността и се реализира в съответствие с националното законодателство.

Защитата на класифицираната информация е от съществено значение за националната сигурност на Република България. Този вид защита се осъществява с цел предпазване на факти и обстоятелства, до които свободният достъп може да застраши териториалната цялост, независимостта и суверенитета на страната. В съответствие със Закона за защита на класифицираната информация (ЗЗКИ), достъпът до класифицирана информация се предоставя само на лица, които са получили специално разрешение за това, като се спазва принципът "необходимост да се знае" (чл. 3, ал. 2 от ЗЗКИ). Този принцип ограничава достъпа до конкретна класифицирана информация само за лица, чиито служебни задължения или специфични задачи изискват такъв достъп.

Ограничаването на достъпа до информация има за цел да предпази интересите на Република България, които включват суверенитета, независимостта, териториалната цялост, отбраната, конституционно установения ред, външната политика, международните отношения и др. Стремежът е да се предотвратят потенциални заплахи и вреди, както и да се изградят работещи механизми за реакция при осъществен нерегламентиран достъп, както и да бъдат преодолени или максимално намалени потенциалните щети за обществото и държавата.

Защитата на тези интереси, чрез осигуряването на сигурност на класифицираната информация, е от съществено значение за функционирането на демократичната система на държавата и за работата на гражданските институции. В Република България Държавната комисия по сигурността на информацията (ДКСИ) е създадена със ЗЗКИ, където в чл. 4., ал. 1 е разпоредена ролята ѝ на държавен орган, отговорен за осъществяването на политиката на страната за защита на класифицираната информация.

III. ВИДОВЕ ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Видовете защита на класифицираната информация в България са 6 (шест): физическа, документална, персонална, криптографска, сигурност на комуникационните и информационните системи (КИС), индустриална сигурност.

3.1. Физическа сигурност

Физическата сигурност на класифицираната информация включва система от мерки, способи и средства за предотвратяване на нерегламентиран достъп до материали, документи, техника и съоръжения, класифицирани като държавна или служебна тайна

(чл. 72, ал. 1 от ЗЗКИ). Системата е вписана в общите стандарти за сигурност, свързани със защитата на класифицирана информация. Тя включва широк набор от мерки, които варират от общи до конкретни, включително оценка на потенциалните заплахи, както и изисквания и стандарти за физическа защита на класифицираната информация.

Способите за предотвратяване на заплахите за физическата сигурност включват анализ на риска, план за гарантиране на физическата сигурност на класифицираната информация; защита на сградите, помещенията и съоръженията, в които се създава, обработва и съхранява класифицирана информация.

Средствата за физическа сигурност се сертифицират за всяко ниво на класификация за сигурност на класифицираната информация и се определят в списък, утвърден от ДКСИ (съгласно чл. 4 от Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване)[2].

Ръководителите на различните организационни единици са отговорни за изпълнението и спазването на мерките, методите и средствата за физическа защита на класифицираната информация. Тази система се прилага и за чуждестранна класифицирана информация, предоставена от друга държава или международна организация, освен ако в международен договор, към който Република България е страна, не е предвидено друго.

Постигането на целите за осигуряване на физическа сигурност на информацията не се изчерпва само с предотвратяването на нерегламентиран достъп. Мерките включват още дейности по пресичане и установяване на действия, които поставят под съмнение надеждността на служителите, групиране на служителите в зависимост от издаденото им разрешение за достъп и в съответствие с принципа „необходимост да се знае" и др.

Мерките за физическа сигурност на класифицираната информация са общи, конкретни и специални, като съобразно конкретните условия те се различават по своята специфика и начина на тяхното прилагане, като например избора на конкретни технически средства и технологии за защита.

[2] Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване, Приета с ПМС № 52 от 4.03.2003 г., обн., ДВ, бр. 22 от 11.03.2003 г., в сила от 11.03.2003 г. – Достъпно на: https://www.dksi.bg/media/1620/naredba_za_sistemata_ot_merki_sposobi_i_sredstva_za_fiziceskata_sigurnost_na_klasificiranata_informa.pdf

3.2. Документална сигурност

Документалната сигурност се състои в система от мерки, способи и средства за защита на класифицираната информация, при създаването, обработването и съхраняването на документи, както и при организирането на работата на регистратури за класифицирана информация (чл. 80., ал. 1 от ЗЗКИ). В допълнителните разпоредби на закона е посочено работното определение за „документ“, както и на „сбор от материали и/или от документи“, които са важни при тълкуването на разпоредбите, отнасящи се до защитата на документалната сигурност.

Документалната сигурност се ангажира с маркиране на класифицирана информация и обозначения върху материалите; класифициране на информацията; регистратури за класифицирана информация; регистриране и отчет на материалите; изпращане, предаване, пренасяне и приемане на материали; задължения на служителите, получили разрешения за достъп до класифицирана информация; размножаване или правене на извадки от документи; сборове от документи; унищожаване на материали или предаването им в архив; контрол върху регистратурите; маркиране и отчет на класифицирана информация в КИС; регистриране, маркиране, отчет и унищожаване на материални носители за многократен запис на класифицирана информация.

Ръководителят на организационната единица, в която се съхранява и обменя чуждестранна класифицирана информация, организира под ръководството на ДКСИ регистратура в областта на международните отношения. В ДКСИ се създава централна регистратура в областта на международните отношения.

Регистратурите се оборудват, за да се гарантира защитата на КИ от нерегламентиран достъп и да не се позволи разкриването на вида и характера на извършваната в тях работа. Регистратурите се откриват след проверка за изпълнение на изискванията за защита на КИ и получаване на уникален идентификационен номер (УИН) от ДКСИ.

В помещенията на регистратурите могат да влизат само служителите от регистратурата, ръководителят на организационната единица, служителят по сигурността на информацията и лицата от ДАНС, имащи контролни функции, определени със заповед на председателя на ДАНС. Класифицирана информация може да се ползва, обработва и съхранява в служебните помещения на потребителите от организационната единица само ако са в съответната зона за сигурност и са защитени с необходимите мерки за сигурност на информацията.

Дейността в регистратурата и служителите в нея се ръководят от завеждащ регистратурата, който е пряко подчинен на служителя по сигурността на информацията. Завеждащият и служителите в регистратурите отговарят за приемане, съхранение и разпределение на класифицирана информация, поддържат списъци на допуснатите лица и следят за сроковете за защита. Осигуряват предаване на материали в архива и предлагат мерки за подобряване на сигурността.

3.3. Персонална сигурност

Персоналната сигурност представлява система от принципи и мерки, прилагани от компетентните органи по съответния ред спрямо лица с цел гарантиране на тяхната надеждност с оглед защита на класифицираната информация. Принципите и мерките по персонална сигурност включват принципа „необходимост да се знае“, процедурата по проучване на лицата и издаването на разрешение за достъп по глава пета от ЗЗКИ, провеждането на обучение на лицата по реда на закона и правилника за неговото прилагане и осъществяването на контрол в тази област (чл. 83, ал. 1 и 2 от ЗЗКИ).

Основополагащ елемент на мерките по гарантиране на персоналната сигурност е процедурата по проучване за надеждност на българските граждани, които желаят да заемат длъжност, изискваща разрешение за достъп до класифицирана информация или сертификат за достъп до такава на НАТО. Редът за извършването на проучванията за надеждност и правилата за тяхното провеждане са определени в ЗЗКИ и Правилника за прилагане на Закона[3]. Тези разпоредби включват отговорностите и функциите на службите за сигурност в процеса по проучването, както и взаимодействието между службите и останалите държавни институции, органи на местното самоуправление, финансови институции и др.

3.4. Криптографска сигурност

Криптографската сигурност представлява система от криптографски методи и средства, които се прилагат с цел защита на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне (чл. 84. от ЗЗКИ). Прилагането на криптографски методи и средства се осъществява единствено след одобрение и регистрация от Държавна агенция „Национална

[3] Правилник за прилагане на Закона за защита на класифицираната информация, Приет с ПМС № 276 от 2.12.2002 г., обн., ДВ, бр. 115 от 10.12.2002 г., в сила от 10.12.2002 г., последно изм. и доп., бр. 68 от 22.08.2017 г., бр. 79 от 8.09.2020 г., в сила от 8.09.2020 г. – Достъпно на: https://www.dksi.bg/media/6596/pravilnik_za_prilagane_na_zakona_za_zashtita_na_klasificiranata_informaciq.pdf

сигурност“, чийто председател предлага на Министерски съвет условия и ред за употреба, производство и внос на подобни технически прибори.

Държавната комисия по сигурността на информацията осъществява общо ръководство и контрол на дейностите по криптографска сигурност на класифицираната информация.

Орган по криптографската сигурност на Република България (ОКС) по смисъла на „Наредба за криптографската сигурност на класифицираната информация” е Държавна агенция „Национална сигурност”. Задачите включват: прилагане на националната политика за криптографска сигурност, предоставяне на указания и препоръки, оценка и одобряване на криптографски методи, въвеждане на криптографски мрежи, разпределяне на ключове, обучение, ръководство, контрол, становища и регистрация на одобрени средства.

Задълженията на служител по криптографската сигурност могат да се изпълняват и от служителя по сигурността на информацията. Служителят по криптографската сигурност е лице, което е получило разрешение за работа с криптографски средства.

За защита на класифицирана информация, обменяна с други страни или международни организации, с които Република България е сключила международни договори, могат да се използват криптографски методи, одобрени от компетентните органи, съобразно двустранните споразумения или националното законодателство. Внедряването на криптографска мрежа изисква одобрение от комисия, включваща представители на органа за класификация и сертификация и на административното звено по сигурността на съответната организационна единица, след проверка на изпълнението на задълженията.

Служителите и администраторите по криптографската сигурност осъществяват текущ контрол по използването на криптографските средства. Разрешението за работа с криптографски средства се издава за срок 5 години.

3.5. Сигурност на комуникационните и информационните системи (КИС)

Сигурността на комуникационните и информационните системи (КИС) представлява система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в КИС (чл. 89. от ЗЗКИ). Задължителните общи условия за сигурност на КИС обхващат компютърната, комуникационната, криптографската, физическата, документалната и персоналната сигурност, сигурността при свързване на КИС, сигурността на самата информация на всякакъв електронен носител и контрамерките по TEMPEST, определени

в наредба, приета от Министерския съвет по предложение на председателя на Държавна агенция "Национална сигурност" (чл. 90., ал. 1 от ЗЗКИ).

Всяка КИС преминава през процедура по акредитиране при строго определени условия и ред, преди да бъде въведена в експлоатация. Орган по акредитиране на сигурността на национални КИС, предназначени за работа с национална класифицирана информация, в които се обработва и класифицирана информация на НАТО и на Европейския съюз, е Специализираната дирекция „Информационна сигурност“ в Държавна агенция „Национална сигурност“.

Държавната комисия по сигурността на информацията (ДКСИ) отговаря за прилагането и контрола на изпълнението на международни договори за защита и обмен на класифицирана информация. В това си качество Комисията акредитира сигурността на точките на присъствие на КИС на НАТО или Европейския съюз и взаимната свързаност с националните КИС.

3.6. Индустриална сигурност

Индустриалната сигурност е система от принципи и мерки, които се прилагат по отношение на кандидати – физически и юридически лица, при сключването или изпълнението на договор, който е свързан с достъп до КИ, с цел защитата ѝ от нерегламентиран достъп. Общите изисквания за гарантиране на индустриалната сигурност се определят от ЗЗКИ и наредба на Министерския съвет, основавайки се върху този закон (чл. 95., ал. 1 и 2).

Процедурата по предоставяне на достъп въз основа на горенаписаното може да бъде започната по два начина: от възложител или след регистриране за участие в поръчки на НАТО в базата данни на Министерството на икономиката.

Класифицираната информация се предоставя на лица след проучване за надеждност. Процедурата включва анализ на финансови и лични данни. Удостоверение за достъп се издава на икономически стабилни и надеждни кандидати – физически или юридически лица. Органът издава удостоверението в зависимост от срока на сключения договор, но за срок не по-дълъг от три години.

IV. НАТО И ЗАЩИТАТА НА ИНФОРМАЦИЯТА

Организацията на Северноатлантическия договор (НАТО) отдава сериозно значение на въпросите относно достъпа до информация и нейната сигурност. Целите, методите и стъпките за гарантиране на сигурността на класифицираната информация са разписани в редица документи, сред които:

C-M(2002)49-REV1 - Security within the North Atlantic Treaty Organization (NATO);

AC/35-D/2000-REV8 - Directive on personnel security;

AC/35-D/2001-REV3 - Directive on physical security;

AC/35-D/2003-REV5 - Directive on classified project and industrial security;

AC/35-D/2004-REV3 - Primary Directive on CIS Security;

AC/35-D/2002-REV5 - Directive on the security of NATO classified information.

Прегледът и анализът на съществуващите нормативни и стратегически документи на Алианса, свързани със защитата на информацията, показват недвусмислено сходство по отношение на направленията, по които институциите и службите за сигурност трябва да работят, за да бъдат осигурени различните видове защита. Споразуменията между страните-членки на НАТО и работата по общи стандарти и процедури е сред стъпките, които биха осигурили по-голяма синергия между държавите от Алианса.

Междувременно с това обменът на класифицирана информация с цел предотвратяване на заплахи за сигурността допринася за укрепването на доверието между съюзниците и повишаване на увереността в способностите на НАТО да защитава себе си не само във физическа среда, но в информационния домейн. При предстоящи или вече настъпили кризи споделянето на разузнавателна информация в рамките на НАТО е подход, спрямо който съюзниците проявяват все по-голяма ангажираност през последните години[4].

V. СИГУРНОСТ НА ИНФОРМАЦИЯТА И ДОСТЪП ДО ИНФОРМАЦИЯ

Съвременните процеси са обусловени от *„значението на информацията като основен ресурс за всички сфери – политика, държавно управление, икономика, образование, здравеопазване, култура.“*[5]

В тази връзка мерките и способите за защита на информацията в различна степен противоречат на най-съвременните разбирания за правото на достъп до информация. Повдигат се въпроси относно свръх-класифицирането на информация в противовес на обществените интереси за повече откритост на управлението. Наред с това, прекомерният публичен фокус върху службите за сигурност и обществен ред може да

[4] **Богданов**, П., 2020. Еволюция на стратегическите концепции на НАТО. Електронно списание на Варненския свободен университет „Черноризец Храбър“, бр. 13, 2020, с. 18-33, ISSN 1313-7514, Достъпно на: https://ejournal.vfu.bg/bg/law.html

[5] **Денчев**, С., 2019. Информация и сигурност. София: За буквите – О писменехъ. с. 25 ISBN 978-619-185-369-4 Достъпно на: https://www.unibit.bg/files/news_important/information-and-security-new-book/Information%20and%20Security.pdf

породи нереалистични очаквания от гражданите по отношение на прозрачността на техните действия.

Характерът на дейностите и задачите в сектора за сигурност изисква определено ниво на секретност. Естествено, това не изключва контролът и носенето на отговорност, както и предоставянето на информация на гражданите.

В Република България Законът за достъп до обществена информация (ЗДОИ) урежда обществените отношения, свързани с правото на достъп до обществена информация, както и с повторното използване на информация от обществения сектор. Неговите разпоредби се отнасят към видовете обществена информация (официална и служебна), реда за искане на определена информация и нейното предоставяне или отказ, както и аргумента, че класифицираната информация е основание за отказ от предоставяне на информация (чл. 37, т. 1.).

VI. РЕЗУЛТАТИ ОТ ИЗСЛЕДВАНЕТО

В резултат на извършения анализ, бихме могли да направим обобщение, което да послужи за синтез на следните изводи:

Настоящата разработка обосновава необходимостта от защитата на информацията, особено в съвременните глобални условия и наличието на множество рискове и заплахи.

Анализирани са статутът и значение на понятието „класифицирана информация“ и различните видове за нейната защита в рамките на националното законодателство на Република България.

Докладът посочва основни документи на НАТО, касаещи сигурността на информацията, което води към заключение, че съществува значително сходство в концепцията за защита на класифицираната информация на национално и съюзно ниво. Това сходство е най-видно от разграничението на видовете защита на информацията.

Повдигнат е въпросът за достъпа до информация от гражданите и връзката му със сигурността на информацията на национално и съюзно равнище. Достигнатият извод сочи, че за ефективната работа на сектора за сигурност е необходимо определено ниво на секретност, което по принцип може да противоречи на някои тълкувания за прозрачност на информацията (но не и на съществуващото законодателство).

VII. ЗАКЛЮЧЕНИЕ

На база на проведеното изследване бихме могли да заключим, че гарантирането на сигурността на информацията и в частност на класифицираната информация изисква

комплексни и широкообхватни мерки, които трябва да бъдат съобразени с актуалните рискове и заплахи, изразяващи се в опити за нерегламентиран достъп и компрометиране на информацията.

Динамичното развитие на международната среда за сигурност и обществените отношения налагат по-задълбочено проучване на връзката между сигурността на информацията и правото на гражданите на достъп до информация. Следователно, сътрудничеството между съюзниците от НАТО трябва да се фокусира и върху намирането на баланс между секретност и откритост, без това да застрашава сигурността на държавите и Алианса.

БЛАГОДАРНОСТИ

Тази публикация е разработена и финансирана по научноизследователски проект по договор № КП-06-М65/6 от 16.12.2022 г. на тема: „Публичност и прозрачност на информацията. Изследване и развитие на процедурите, свързани с нарушаване на правата за достъп до информация на гражданите“ на Фонд „Научни изследвания“ към Министерство на образованието и науката на Република България.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. **Ангелов**, Г., **Иванова**, М., 2023. Архитектурен подход за описание на процесите в комуникационно-информационни системи на организационно-управленски структури. Статия в списание ОБРАЗОВАНИЕ, НАУЧНИ ИЗСЛЕДВАНИЯ И ИНОВАЦИИ, Научно списание година I, книжка 3, 2023, с. 36-42., ISSN 2815-4630 Достъпно на: https://e-journal.unibit.bg/razshireno-tyrsene/publikacii-po-rubriki/5-nacionalna-sigurnost/20-ivanova-angelov

2. **Богданов**, П., 2020. Еволюция на стратегическите концепции на НАТО. Електронно списание на Варненския свободен университет „Черноризец Храбър“, бр. 13, 2020, с. 18-33, ISSN 1313-7514, Достъпно на: https://ejournal.vfu.bg/bg/law.html

3. **Денчев**, С., 2019. Информация и сигурност. София: За буквите – О писменехь. ISBN 978-619-185-369-4 Достъпно на: https://www.unibit.bg/files/news_important/information-and-security-new-book/Information%20and%20Security.pdf

4. **Закон** за защита на класифицираната информация, Обн. Дв. Бр. 45 от 30 април 2002 г., последна попр. изм. Дв. Бр. 13 от 13 февруари 2024 г. – Достъпно на: https://lex.bg/laws/ldoc/2135448577

5. **Йорданова**, С. Анализ на актуалната глобална политико-икономическа информационна среда. – В: Обществото на знанието и хуманизмът на XXI век. София: За буквите – О писменехь, 2021, с. 511 – 520, ISSN 2683-0094

6. **Йорданова**, С. Теоретични основи на разузнаването, дипломацията и анализа (Фрагментарен поглед). София: За буквите – О писменехь, 2023, с. 235. ISBN: 978-619-185-614-5

7. **Йотова**, Р., **Йорданова**, С., 2022. Потреблението на информацията като основен ресурс в системата на информационното общество. В: Образованието в глобалния свят на новите технологии. Втори конгрес на Университетите от Югоизточна Европа и Азия – интелигентна дестинация за култура, туризъм, младеж, изкуствен интелект и блокчейн технологии. София: За буквите – О писменехь, 2022, с. 233-240. ISBN: 978-619-185-551-3

8. **Казаков**, К., 2019. Стратегическо управление на информационните услуги в сигурността. Софттрейд, С. 2019, ISBN 978-954-334-220-4 COBISS.BG-ID 1289504996

9. **Наредба** за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване, Приета с ПМС № 52 от 4.03.2003 г., обн., ДВ, бр. 22 от 11.03.2003 г., в сила от 11.03.2003 г. – Достъпно на: https://www.dksi.bg/media/1620/naredba_za_sistemata_ot_merki_sposobi_i_sredstva_za_fiziceskata_sigurnost_na_klasificiranata_informa.pdf

10. **Петева**, И., 2008. Информационни аспекти на връзката „достъпност-сигурност“ на обществено значимата информация. В: Годишник на секция „Информатика”. СУБ, т.1. София, Изд. На Сю/за на учените в България, 2008 с.24-28. Достъпно на: http://old.usb-bg.org/Bg/Annual_Informatics/2008/SUB-Informatics-2008-1-024-028.pdf

11. **Петева**, И., **Денчев**, С., **Целков**, В., 2020. Сигурност на информационните ресурси. София: За буквите – О писменехь. ISBN:978619185-432-5

12. **Правилник** за прилагане на Закона за защита на класифицираната информация, Приет с ПМС № 276 от 2.12.2002 г., обн., ДВ, бр. 115 от 10.12.2002 г., в сила от 10.12.2002 г., последно изм. и доп., бр. 68 от 22.08.2017 г., бр. 79 от 8.09.2020 г., в сила от 8.09.2020 г. – Достъпно на: https://www.dksi.bg/media/6596/pravilnik_za_prilagane_na_zakona_za_zashtita_na_klasificiranata_informaciq.pdf