



ВОДИЧ ЗА КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ

UDHËZUES PËR KLASIFIKIMIN E INFORMACIONEVE





ВОДИЧ ЗА КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ

Скопје, 2026

Дирекцијата за безбедност на класифицирани информации во координација со претставници од безбедносно-разузнавачката заедница на Република Северна Македонија

Владо Гердовски

Кире Бабаноски

DCAF Geneva Centre
for Security Sector
Governance

All rights reserved

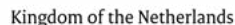
DCAF – Geneva Center for Security Sector Governance
Maison de la Paix Chemin Eugène-Rigot 2E, CH1202- Geneva, Switzerland

Сите права се задржани

ДЦАФ – Центар за управување со безбедносниот сектор – Женева – Подружница Скопје
ул. Македонија бр. 11-1/2, 1000 Скопје, Република Северна Македонија

Водичот е изготвен во рамките на **Програмата за реформа на разузнавачкиот и безбедносниот сектор во Република Северна Македонија**, спроведувана од ДЦАФ - Женевскиот центар за управување со безбедносниот сектор и финансиски поддржана од Швајцарската агенција за развој и соработка (САЦ), Министерството за надворешни работи на Холандија и Шведската агенција за меѓународен развој (Сид).

Содржината на оваа публикација не ги изразува ставовите и мислењата на донаторите или на ДЦАФ.



CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје
351.083.8(497.7)(036)
342.738(497.7)(036)

ВОДИЧ за класифицирање на информации [Електронски извор] = Udhëzues për klasifikimin e informacioneve / [urednik Vlado Ćerđovski]. - Скопје

: ДЦАФ Центар за управување со безбедносниот сектор - Женева, 2026

Начин на пристапување (URL): <https://che01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.dbki.gov.mk%2F&-data=05%7C02%7C%7Ce673581aa0cd4d89d4a808df156bea28%7Ca9f26010975473e94ae0c36afbcb9ea%7C0%7C0%7C639253225403152161%7CUknown%7CTWFpbGZsb3R8eyJFeXB0eU1hcGkiOnRydWUsIlYiOiJlLjAuMDAwMCIsImlAiOjIJAuVjoiTWFpbGlzIlldIojoyQ3D%3D%7C0%7C%7C%7Csdata=xTQ%2B%2BGLZ8YGNVLU28d%2BY6HJ%2FirrkPkMjjrsPY2n6shAserved=0>

- Текст во PDF

формат, содржи 69 стр., илустр. - Библиографија: стр. 37

ISBN 978-608-5046-08-9

а) Класифицирани информации -- Заштита -- Македонија -- Водичи
COBISS.MK-ID 69666821

ПРЕДГОВОР

Програмата за реформа на разузнавачкиот и безбедносниот сектор во Република Северна Македонија (2021-2026), спроведувана од ДЦАФ - Женевскиот центар за управување со безбедносниот сектор, има за цел да ги поддржи безбедносните, разузнавачките, правосудните и надзорните институции во зајакнувањето на нивните капацитети за добро управување, отчетност и ефективен демократски надзор. Еден од клучните сегменти на оваа поддршка е обезбедување усогласени, транспарентни и ефикасни процеси во областа на управувањето и ракувањето со класифицирани информации, со целосно почитување на принципите на владеење на правото и заштитата на човековите права и слободи.

Во рамките на спроведените активности во Програмата, беа идентификувани значајни предизвици поврзани со класификацијата на информации, вклучувајќи:

- недоследности во примената на критериумите за утврдување на степените на класификација,
- прекумерно и понекогаш неоправдано класифицирање на информации,
- отсуство на јасни механизми за контрола и верификација на класификацијата,
- различни институционални практики кои водат кон ограничена меѓуинституционална соработка и размена на информации.

За да се адресираат овие предизвици, ДЦАФ организираше неколку мултисекторски стручни дискусии со претставници од релевантните државни институции. На тие настани беше овозможена конструктивна размена на искуства и беа дефинирани основите за унапредување на усогласеноста на процесите на класифицирање, во согласност со постојната законска рамка и меѓународните стандарди. Од дискусиите произлегоа потребата од изработка на унифицирани, јасни и практично применливи насоки за класификација на информации, со цел системско зајакнување на институционалните капацитети и поттикнување оперативна ефикасност во безбедносно-разузнавачкиот сектор.

Овој Водич за класифицирање на информации е резултат на таа заедничка иницијатива. Неговите цели се:

- да понуди конкретни критериуми за разграничување на степените на класификација,
- да поддржи воспоставување интерни практики за контрола и верификација,
- да придонесе за поусогласена, рационална и одговорна примена на стандардите за класифицирање информации.

Водичот претставува практична алатка за сите ракувачи со класифицирани информации, која ќе продолжи да се унапредува низ процес на примена, обука и меѓуинституционална консултација.

ДЦАФ, заедно со безбедносно-разузнавачките институции и Дирекцијата за безбедност на класифицирани информации како носител на процесот, останува посветен на натамошната поддршка во јакнењето на безбедносниот систем заснован на владеење на правото, професионализам, интегритет и усогласени стандарди.



Порака од директорот на Дирекцијата за безбедност на класифицирани информации



Заштитата на класифицираните информации претставува еден од клучните столбови на националната безбедност и на довербата меѓу институциите. Во услови на динамични безбедносни предизвици, од исклучителна важност е сите носители и корисници на класифицирани информации да постапуваат одговорно, професионално и во согласност со важечките законски и подзаконски прописи.

Овој Водич е подготвен со цел да обезбеди јасни и практични насоки за правилно ракување, заштита и управување со класифицираните информации. Неговата

доследна примена ќе придонесе за унапредување на безбедносната култура, намалување на ризиците од неовластен пристап, како и за зајакнување на интегритетот на институционалните процеси.

Овој Водич што е пред Вас не е само документ. Тој е алатка што треба да Ве води, да Ве потсетува и да Ви помогне во секојдневното работење. Неговата вистинска вредност се гледа само тогаш кога ќе го примениме доследно и одговорно.

Секој од Вас има важна улога. Секој пристап до информација носи одговорност. Секоја одлука, дури и најмалата, може да има големо влијание. Токму затоа, внимателноста, дисциплината и професионалната етика не се избор, туку неопходност.

Дозволете ми да бидам јасен: безбедноста не трпи компромиси. Не постои „доволно добро“ кога станува збор за заштита на класифицирани информации. Постојат само правилни постапки и обврска тие секогаш да се следат.

Да ја чуваме довербата што ни е дадена.

Да ги заштитиме институциите што ни се доверени.

И да изградиме систем на кој сите ќе можеме да се потпреме.

Ви благодарам.

Фљорим Јаја

Директор на Дирекцијата за безбедност на класифицирани информации

Скопје, 2026

СОДРЖИНА

ЛИСТА НА ТАБЕЛИ	8
КОРИСТЕНИ КРАТЕНКИ	8
1. Вовед	9
2. Создавачи и изработувач на класифицирана информација	10
2.1. Создавач на класифицирана информација	10
2.2. Изработувач на класифицирана информација	12
2.3. Разграничување на улогите меѓу создавачот и изработувачот	13
2.4. Одговорност на создавачот и изработувачот на класифицирана информација	14
3. Степени на класификација на информациите	15
4. Процес на одредување степен на класификација	18
4.1. Идентификација на информацијата	18
4.2. Принципи при одредување на степен на класификација	18
4.3. Критериуми за одредување степен на класификација	19
4.3.1. Содржина на информацијата	20
4.3.2. Проценка на можната штета и последиците	21
4.4. Економска оправданост при класификација на информацијата	23
4.5. Определување на можната штета и последиците	23
4.5.1. ЗА ОГРАНИЧЕНА УПОТРЕБА	26
4.5.2. ИНТЕРНО	27
4.5.3. ДОВЕРЛИВО	28
4.5.4. СТРОГО ДОВЕРЛИВО	30
4.5.5. ДРЖАВНА ТАЈНА	31
5. Ризици од несоодветно класифицирање на информации	32
6. Совети/препораки при класифицирање информации	33
БИБЛИОГРАФИЈА	34



Листа на табели

Табела 1	Задачи на создавачот на класифицирана информација	12
Табела 2	Задачи на изработувачот на класифицирана информација	13
Табела 3	Споредба на улогите на изработувачот и создавачот	14
Табела 4	Степени на класификација на информациите и нивното значење .	16
Табела 5	Безбедносни мерки кои се применуваат за класифицирани информации и за ознаката „За ограничена употреба“	17
Табела 6	Критериуми за определување степен на класификација на информацијата	20
Табела 7	Определување на степенот на класификација на информацијата и ознаката „За ограничена употреба“ во зависност од можната штета и последиците кои би настанале од неовластено откривање	24

Користени кратенки

бр.	број
ДБКИ	Дирекција за безбедност на класифицирани информации
ЕУ	Европска Унија
ЗКИ	Закон за класифицирани информации
итн	и така натаму
ЈИЕ	Југоисточна Европа
КИС	комуникациско-информациски систем
сл.	слично
ст.	став
чл.	член
УАБ	Уредба за административна безбедност на класифицирани информации и на информации за органичена употреба



1. ВОВЕД

Заштитата на класифицираните информации претставува основен предуслов за ефикасно функционирање на органите на државната и локалната власт, заштита на безбедноста и одбраната на државата, зачувување на нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес, како и гарантирање на слободите и правата на човекот и граѓанинот.

Во услови на зголемени безбедносни предизвици и динамични ризици, правилното ракување со информациите е клучно за зачувување на стабилноста, сигурноста и довербата во институциите. Класификацијата на информациите овозможува регулиран пристап и примена на соодветни мерки за заштита, врз основа на нивната чувствителност и потенцијалната штета што би можела да произлезе од нивно неовластено откривање или употреба.

Системот за класифицирани информации во Република Северна Македонија е воспоставен врз основа на јасна правна рамка чија цел е заштита на информациите од значење за националната безбедност и други витални државни интереси. Клучниот пропис кој го уредува ова подрачје е Законот за класифицирани информации (*) (ЗКИ), „Службен весник на Република Северна Македонија“ бр. 275/2019. Законот е развиен според барањата на НАТО и усогласен со стандардите воспоставени во неговите директиви за безбедност на класифицирани информации, како и со стандардите на Европската Унија, како што е Одлуката на Советот на Европската Унија (ЕУ) од 23 септември 2013 година за безбедносните правила за заштита на класифицирани информации на ЕУ (CELEX број 32013D0488)¹, обезбедувајќи применливост на овие стандарди во националниот систем за безбедност на класифицирани информации. Со Законот се уредуваат:

- постапките, условите и критериумите за класификација на информации,
- мерките и активностите за нивна заштита и безбедност,
- правата, обврските и одговорноста на создавачите и корисниците на класифицирани информации,
- начелата за национална и меѓународна размена на класифицирани информации,
- инспекцискиот надзор над спроведувањето и другите прашања поврзани со пристапот, користењето и ракувањето со класифицирани информации.

Во функција на спроведување на Законот донесени се низа подзаконски акти (уредби) кои ги регулираат специфичните аспекти на безбедноста на класифицираните информации:

- Уредба за административна безбедност на класифицирани информации;
- Уредба за физичка безбедност на класифицирани информации;
- Уредба за безбедност на лица корисници на класифицирани информации;
- Уредба за информатичка безбедност на класифицирани информации;
- Уредба за индустриска безбедност на класифицирани информации.

Националната концепција за безбедност и одбрана на Република Северна Македонија ги утврдува трајните, виталните и важните интереси на државата, кои произлегуваат од темелните вредности утврдени со Уставот и кои се насочени кон заштита на суверенитетот, територијалниот интегритет, уставниот поредок и основните права и слободи на граѓаните.

¹ 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, <https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng>



Во таа смисла, заштитата на класифицираните информации претставува клучен механизам за поддршка на безбедносните политики и за обезбедување стабилно и континуирано функционирање на државата, во согласност со меѓународните стандарди и обврски.

Оправданоста на изработката на овој Водич произлегува од законски дадената задача на ДБКИ да предлага и спроведува мерки и активности за заштита на класифицираните информации. Дополнително на ова, Одлуката на Советот на Европската унија од 23 септември 2013 година за безбедносните правила за заштита на класифицираните информации на ЕУ (CELEX број 32013D0488), односно нејзиниот Анекс III – Управување со класифицирани информации, утврдува административни мерки за контрола на класифицираните информации на ЕУ во текот на целиот нивен оперативен циклус, со цел да се спречи или открие намерно или случајно компромитирање или губење на такви информации. Според точките 2 и 3 на Анексот, информациите се класифицираат кога бараат заштита во однос на нивната доверливост, а одговорноста за определување на степенот на класификација ја има нивниот создавач, во согласност со релевантните насоки за класификација. Токму поради потребата од такви релевантни насоки, ДБКИ го иницира и го предводеше создавањето на овој Водич кој има за цел да обезбеди јасни и практични упатства за правилно одредување, означување и заштита на класифицираните информации, во согласност со европските стандарди и националната регулатива.

Практичните цели на овој Водич се:

- да се овозможи систематска и објективна проценка на степенот на заштита што треба
- да се примени за информациите од чувствителен карактер,
- да се воспостават јасни критериуми за донесување одлуки при определување на степенот на класификација,
- да се обезбеди спроведување на соодветни мерки за заштита на класифицираните информации.

Со примена на стандардите содржани во овој Водич се обезбедува унифициран пристап кон заштитата и се минимизира ризикот од неправилно ракување со класифицираните информации.

2. СОЗДАВАЧ И ИЗРАБОТУВАЧ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЈА

2.1. Создавач на класифицирана информација

Создавач на класифицирана информација е овластен изработувач на класифицирана информација.

Создавачи на класифицирана информација може да бидат органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други физички или правни лица, што создаваат информации од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата.

За класифицирана информација со степен „ДРЖАВНА ТАЈНА“, ЗКИ прецизно ги наведува создавачите, а тие може да бидат: претседателот на Република Северна Македонија, претседателот на Собранието на Република Северна Македонија, претседателот на Владата на Република Северна Македонија, претседателот на Уставниот суд на Република Северна Македонија, претседателот на Врховниот суд на Република Северна Македонија, министрите во рамките на своите ресори, јавниот обвинител на Република Северна Македонија, началникот на Генералштабот на Армијата на Република Северна Македонија, директорот на Агенцијата за разузнавање, директорот на Агенцијата за национална безбедност, директорот на Оперативно-техничката агенција, директорот на Центарот за управување со кризи, директорот на Дирекцијата за безбедност на класифицирани информации, како и лица овластени од страна на горенаведените субјекти. Ако така е определено со закон, ратификуван меѓународен договор или друг пропис, класифицирана информација со степен „ДРЖАВНА ТАЈНА“ определуваат и лицата предвидени во тие акти.

Создавачот на информацијата или лице што тој го овластил во писмена форма го определува степенот на класификација на информацијата. Создавачот во рамките на своите работни задачи и овластувања, генерира информации чија содржина може да предизвика штета по државните или службените интереси доколку биде неовластено објавена. Создавачот ја познава суштината, контекстот и чувствителноста на информацијата и затоа има обврска при нејзиното оформување да предложи соодветен степен на класификација. Затоа, создавачот треба да има соодветно образование и детално познавање на законската и подзаконската регулатива за безбедност на класифицирани информации. Дополнително, потребно е континуирано да учествува во специјализирани обуки и да поседува практично искуство во ракување и заштита на класифицираните информации.

Создавачот мора да биде способен да ја идентификува можната штета врз безбедносните, политичките, економските или меѓународните интереси на Република Северна Македонија доколку дојде до неовластено откривање на информацијата, и врз основа на тоа да го утврди соодветниот степен на класификација. Значи, создавачот, односно лицето овластено од него, треба да ја означи класифицираната информација со најсоодветниот степен на класификација со кој се обезбедува потребната заштита на државните интереси и безбедноста.



Во случаи кога информацијата не била означена со степен на класификација, а создавачот не може да се утврди или престанал да постои, класифицирањето го врши правниот следбеник на создавачот. Доколку не може да се утврди ниту правниот следбеник, тогаш, означувањето го врши ДБКИ.

Создавачот на класифицирани информации ја носи примарната институционална и законска одговорност за правилно определување, означување и измена на степенот на класификација. Создавачот ја има завршната и одлучувачка улога во процесот на класификација и обезбедува усогласеност со ЗКИ, подзаконските акти и внатрешните процедури на институцијата.

Табела 1 Задачи на создавачот на класифицирана информација

Задача	Опис
Определување степен на класификација	Создавачот врз основа на предлогот од изработувачот и направената проценка на содржината и можните последици, го утврдува соодветниот степен на класификација. При тоа мора да го почитува принципот на пропорционалност – да не се применува повисок степен од неопходниот, ниту пак да се изостави класификација кога тоа е нужно за заштита на националните интереси.
Означување на класифицираната информација	Создавачот е должен да ја означи секоја информација со нејзиниот утврден степен на класификација и да осигура дека ознаките се јасно видливи, точни и доследни со утврдените формати и стандарди, со што се спречува неовластено користење или погрешно ракување со информацијата.
Класификација на поединечни податоци	Кога информацијата содржи податоци од различна чувствителност, создавачот мора да определи степен на класификација за секој поединечен податок или дел, со цел да се избегне прекумерна класификација на целината.
Рекласификација	Создавачот има право и обврска да го промени степенот на класификација доколку се променат околностите, степенот на ризик или чувствителноста на информацијата. Таа промена мора да биде образложена, документирана и навремено спроведена.
Декласификација	Создавачот е одговорен за спроведување на процесот на декласификација, односно да утврди дека информацијата повеќе не бара класифициран статус и дека може да стане достапна како некласифицирана. Декласификацијата се спроведува врз основа на проценка на ризиците и законскиот временски рок.
Означување временски период на важење на степенот на класификацијата на информацијата	Создавачот одредува временски рок или конкретен настан по кој информацијата може да биде рекласифицирана или декласифицирана. Така се обезбедува динамичен систем на заштита што се прилагодува на променливите безбедносни услови и важноста на информацијата.

2.2. Изработувач на класифицирана информација

Изработувач на класифицирана информација е службено лице кое, врз основа на анализата на содржината на информацијата, дава и писмено образложува предлог за определување на соодветен степен на класификација, водејќи сметка за законските критериуми, ризиците и големината на штетата што може да настане од нејзиното откривање. Предлогот за класификација на информации со одреден степен ги содржи следните елементи:

- назив на организациската единица и органот кој го предлага степенот на класификација,
- наслов и краток опис на информацијата за која се предлага степенот на класификација,
- степенот на класификација што се предлага,
- образложение за штетата што би настанала од неовластено откривање на информацијата,
- име и презиме на лицето што го изготвил предлогот и
- име и презиме на лицето што го одобрил предлогот.

И покрај тоа што изработувачот дава професионална и стручно заснована проценка, крајната одлука за определување на степенот на класификација ја донесува создавачот на информацијата, односно лицето кое раководи со органот или лице овластено од него



со самото потпишување на предлогот и на документот што се класифицира. Создавачот го утврдува финалниот степен на класификација, водејќи сметка за принципот на пропорционалност, минималната потребна класификација и заштитата на националната безбедност и државните интереси. Предлогот за класификација на информацијата се чува заедно со информацијата којашто се класифицира. Во органите во коишто се применува систем за автоматска обработка на класифицирани информации, предлогот за определување на соодветниот степен на класификација на информацијата се дава по електронски пат. Со ова се обезбедува усогласен, одговорен и хиерархиски контролиран процес на класификација на информации, со цел да се спречи прекумерна или недоволна заштита и да се гарантира безбедно и ефикасно ракување со класифицирани информации.

Изработувачот на класифицирана информација има суштинска улога во обезбедувањето на законски, доследен, точен и објективен процес на класификација. Изработувачот е првиот субјект кој врши анализа на содржината на информацијата и дава стручно заснован предлог за степенот на нејзината класификација. Работата на изработувачот претставува основа за донесување на конечната одлука од страна на создавачот на информацијата.

Табела 2 Задачи на изработувачот на класифицирана информација

Задача	Опис
Анализа на содржината на информацијата	Детална проценка на суштината, контекстот и чувствителноста на информацијата со цел да се утврди дали нејзиното откривање може да предизвика штета по националната безбедност, јавниот интерес, надворешните односи или други заштитени вредности.
Изготвување предлог за степен на класификација	Подготвување писмен предлог кој ги содржи сите задолжителни елементи: опис на информацијата, предложен степен на класификација, образложение за можната штета (обезбедување јасна и аргументирана основа за предложениот степен на класификација) и податоци за изработувачот и одобрувачот.
Примена на принципот на пропорционалност	Проценување на реалната потреба од класификација и избегнување на прекумерен (неоправдано висок степен на заштита) или недоволен (неоправдано низок степен на заштита), со цел рационално користење на ресурсите и поттикнување транспарентност.
Соработка со создавачот	Координација при донесување на конечната одлука, усогласување со безбедносните мерки и обезбедување точна евиденција за класифицираните документи.
Почитување на процедурите за заштита на информациите	Обезбедување доверливост, интегритет и контролирана достапност на информацијата во текот на нејзината изработка, дури и пред нејзината официјална класификација.

2.3. Разграничување на улогите меѓу создавачот и изработувачот

Иако создавачот и изработувачот на класифицирани информации тесно соработуваат во процесот на определување на степенот на класификацијата, нивните улоги и одговорности се суштински различни.

Изработувачот е одговорен за подготовка и стручна проценка на содржината на информацијата и за изготвување на предлог за соодветен степен на класификација, заснован на анализата на можните штети, ризици и законски критериуми. Изработувачот има аналитичко-подготвувачка улога, насочена кон содржината и проценката на ризиците.

Создавачот, од друга страна, има одлучувачка и правна одговорност – го проверува предлогот на изработувачот и ја донесува финалната одлука за класификација, запазувајќи ги предвидените законски услови и критериуми. Со тоа, создавачот има контролна функција над процесот на класификација на информациите.

Табела 3 Споредба на улогите на изработувачот и создавачот

Одговорен субјект	Фаза во процесот	Опис на активност / улогата
Изработувач	Подготовка на документот	Ја подготвува содржината на документот со класифицирани информации.
	Анализа на содржината и проценка на можната штета и последиците	Врши стручна анализа на содржината на информацијата (интегритет, природа и вредност) и проценка на можната штета и последиците (чувствителност, закана, ризик).
	Изготвување на предлог за степен на класификација	Го предлага соодветниот степен на класификација, врз основа на анализата и проценката на законските критериуми.
Создавач	Преглед и оценка на предлогот	Го разгледува предлогот на изработувачот, ја оценува неговата оправданост и усогласеност со процедурите.
	Конечно одлучување за степенот на класификација	Го потврдува/верификува степенот на класификација.

2.4. Одговорност на создавачот и изработувачот на класифицирана информација

Создавачот и изработувачот на класифицирана информација сносат дисциплинска, прекршочна и кривична одговорност доколку не постапуваат во согласност со законските одредби. За нив, како и за сите други лица кои се вработени во институцијата и кои се корисници на класифицирани информации, се предвидени соодветни дисциплински мерки, прекршочни и кривични санкции во случаи на повреда на правилата за класифицирање и ракување со класифицирани информации:

- **Дисциплинска одговорност:** при повреди на службената должност за што може да им бидат изречени соодветни дисциплински мерки, во согласност со законските прописи и внатрешните акти на институцијата.
- **Прекршочна одговорност:** за воспоставување и следење на законските процедури при определување на степенот на класификација, односно доколку се класифицира информација без направена потребна проценка за можната штета и последици, како и доколку не се исполни обврската навремено да се известат корисниците на класифицирана информација за промена на степенот на класификација или за нејзина декласификација.
- **Кривична одговорност:** како и секое друго лице со пристап до класифицирани информации – доколку неовластено прибават или оддадат класифицирани информации.

Со доследно почитување на законските процедури и обврски, создавачот и изработувачот обезбедуваат процесот на класификација да биде законит, рационален и усогласен со принципите на транспарентност, отчетност и добро управување.



3. СТЕПЕНИ НА КЛАСИФИКАЦИЈА НА ИНФОРМАЦИИТЕ

Информација од интерес за Република Северна Македонија

Секоја информација изготвена од орган на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје, физичко или правно лице, како и од странски државен орган, односно странско физичко или правно лице, која се однесува на безбедноста и одбраната на државата, нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес и слободите и правата на човекот и граѓанинот.

Класифицирана информација

Информација од делокругот на работа на орган на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или други правни лица којашто се однесува на јавната безбедност, одбраната, надворешните работи или безбедносни или разузнавачки активности на државата која согласно со закон мора да се заштити од неовластен пристап и е обележана со соодветен степен на класификација согласно со овој закон. Класифицирани информации може да претставуваат и документи, технички средства, машини, опрема, односно одвоени компоненти или оружје или алати што се произведени или се во процес на производство, како и доверливите пронајдоци што се однесуваат на одбраната и се од интерес на безбедноста на државата.

ЗКИ предвидува четири степени на класификација:

1. „ДРЖАВНА ТАЈНА“
2. „СТРОГО ДОВЕРЛИВО“
3. „ДОВЕРЛИВО“
4. „ИНТЕРНО“

Со цел да се обезбеди конзистентно и усогласено ракување со класифицираните информации, степенот на класификација се утврдува врз основа на видот на интересите што се штитат и нивото на штета што би настанала доколку информацијата неовластено се открие. Следната табела ги прикажува дефинициите на степените на класификација поделени според видот на потенцијалната штета и категориите на интереси кои се предмет на заштита.

Табела 4 Степени на класификација на информациите и нивното значење

Степен на класификација	Последици од неовластено откривање	Вид на интереси што се штитат
ДРЖАВНА ТАЈНА	Загрозување и нанесување непоправливи штети	Трајните интереси на Република Северна Македонија
СТРОГО ДОВЕРЛИВО	Исклучително сериозна штета	Виталните интереси на Република Северна Македонија
ДОВЕРЛИВО	Сериозна штета	Важните интереси на Република Северна Македонија
ИНТЕРНО	Работата на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, кои се од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата	

Покрај наведените степени, постои и дополнителна ознака за информации, а тоа е „ЗА ОГРАНИЧЕНА УПОТРЕБА“.

Оваа ознака не претставува степен на класификација, но служи за заштита на информации чија неовластена достапност би можела да ја намали ефикасноста на работењето на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје.

Овие информации:

- не се слободно достапни, и
- се штитат со соодветни мерки, утврдени со подзаконски акт на Владата, а тоа е
- Уредбата за административна безбедност на класифицирани информации и на информации со ограничена употреба.

Доколку класификацијата на информацијата има за цел да сокрие пречекорување на овластување, злоупотреба на функцијата или друго незаконско или казниво дејствие, таа информација не се смета за класифицирана. Лицата кои ќе ја пријават таквата информација до надлежен орган, согласно Законот за заштита на укажувачи, уживаат законска заштита.

Со определувањето на степенот на класификација на информациите, всушност се определува соодветна заштита која се состои од збир на активности и мерки за спречување неовластен пристап и неовластено ракување.

Следната табела дава споредбен преглед на безбедносните мерки што се применуваат при ракување, чување, пренос и заштита на класифицирани информации и на информации означени „За ограничена употреба“. Таа овозможува јасно разграничување на обврските и постапките во зависност од степенот на класификација и нивото на ризик што произлегува од неовластено откривање на информациите.

Табелата се користи како насочувач при планирање и спроведување на безбедносните мерки од страна на институциите и одговорните лица, со цел да се обезбеди соодветна примена на законските и подзаконските решенија. Корисниците преку неа можат лесно да утврдат кои мерки се задолжителни, кои се препорачани и во кои случаи е потребно дополнително зајакнување на заштитата, во согласност со конкретниот контекст и проценката на ризик.





Табела 5 Безбедносни мерки кои се применуваат за класифицирани информации и за ознаката „За ограничена употреба“

	ЗА ОГРАНИЧЕНА УПОТРЕБА			ИНТЕРНО	ДОВЕРЛИВО	СТРОГО ДОВЕРЛИВО	ДРЖАВНА ТАЈНА
Принцип „Потребно е да знае“				да	да	да	да
Безбедносна проверка	не			не	да	да	да
Преглед на лица кои пристапиле до информацијата	не			не	не	да	да
Дисеминација	правни и физички лица кои се запознаени со мерките и активностите за заштита на таквите информации и имаат потпишано изјава за тоа	правни и физички лица кои се запознаени со мерките и активностите за заштита на таквите информации и имаат потпишано изјава за тоа	правни и физички лица кои се запознаени со мерките и активностите за заштита на таквите информации и имаат потпишано изјава за тоа	правни и физички лица кои имаат безбедносен сертификат најмалку еднаков со степенот на класификацијата	правни и физички лица кои имаат безбедносен сертификат најмалку еднаков со степенот на класификацијата	правни и физички лица кои имаат безбедносен сертификат најмалку еднаков со степенот на класификацијата	правни и физички лица кои имаат безбедносен сертификат најмалку еднаков со степенот на класификацијата
Репродукција, копии, преводи, издадоци	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“	се прави од страна на корисникот со строга примена на принципот „потребно е да знае“
Ракување и чување	во административни и безбедносни зони од прв и втор степен	во административни и безбедносни зони од прв и втор степен	во административни и безбедносни зони од прв и втор степен	во безбедносни зони од прв и втор степен	во безбедносни зони од прв и втор степен	во безбедносни зони од прв и втор степен	во безбедносни зони од прв и втор степен
КИС за ракување и чување	неакредитиран (на официјален-службен КИС)	неакредитиран	акредитиран	акредитиран	акредитиран	акредитиран	акредитиран
ТЕМПЕСТ мерки	не	да	да	да	да	да	да
Физичка достава	спакувани во еден непрозирен коверт	спакувани во два коверти	спакувани во два коверти	спакувани во два коверти	спакувани во два коверти	спакувани во два коверти	спакувани во два коверти
Пренесување преку електронски средства	да	да, со соодветна криптизација	да, со соодветна криптизација	да, со соодветна криптизација	да, со соодветна криптизација	да, со соодветна криптизација	да, со соодветна криптизација
Уништување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување	според листата на документарен материјал со рокови на негово чување

4. ПРОЦЕС НА ОДРЕДУВАЊЕ СТЕПЕН НА КЛАСИФИКАЦИЈА

4.1. Идентификација на информацијата

Идентификацијата на информацијата претставува првиот и клучен чекор во процесот на класифицирање на информацијата. Таа вклучува одредување на видот, карактерот и носителот на информацијата, како и прелиминарна проценка на нејзината чувствителност и значење за националната или организациската безбедност. Прецизната идентификација овозможува правилно одредување на степенот на класификација, избор на соодветни мерки за заштита и воспоставување на контроли за пристап и ракување со информациите. Во рамките на процесот на идентификација на информацијата се извршуваат следните активности:

- се идентификува видот и содржината на информацијата (документ, е-маил, аудио, видео, бази на податоци итн.),
- се утврдува функцијата на информацијата – дали е стратегиска, оперативна, административна или друг вид,
- се разгледува кој ја користи и кој треба да има пристап (оддели, службеници, соработници).

Класифицираните информации се однесуваат особено на следните области:

- јавната безбедност,
- одбраната,
- надворешните работи,
- безбедносните, разузнавачките и контраразузнавачките активности на државата, критичната инфраструктура, системи, уреди, пронајдоци, проекти и планови од значење за државата,
- научни, технолошки, економски и финансиски податоци од национален интерес.

Со правилна идентификација се обезбедува унифициран пристап кон ракувањето со информациите и се минимизира ризикот од неправилно класифицирање или неовластено ракување.

4.2. Принципи при одредување на степен на класификација

При одредување на степенот на класификација на информациите треба да се земат предвид следните принципи:

Принцип на штета

Се проценува каква и колкава штета би настанала доколку информацијата биде неовластено откриена, изменета или злоупотребена. Степенот на класификација директно се поврзува со сериозноста и обемот на можните последици по државните, институционалните или јавните интереси.

Принцип на пропорционалност

Степенот на класификација мора да биде сразмерен со нивото на штета што би можела да настане од неовластеното откривање на информацијата. Прекумерната класификација на информации со мала штетност, како и недоволната заштита на чувствителни информации, претставуваат отстапување од овој принцип.



Принцип на неопходност во класификацијата

Класификацијата на информацијата се врши само кога тоа е навистина неопходно за заштита на државните или институционалните интереси. Доколку целите на заштитата можат да се постигнат без класифицирање, само со ограничување на достапноста или со означување на информацијата со ознаката „за ограничена употреба“, класифицирањето не треба да се применува.

Временски принцип

При класифицирање се зема предвид временскиот период во кој информацијата има чувствителен карактер и бара заштита. Степенот на класификација не е траен по правило и треба да се преиспитува, со можност за намалување или укинување кога ќе престанат причините за заштита.

Принцип на одговорност

Класификацијата на информацијата ја врши исклучиво овластено лице, односно создавач, во рамките на своите законски надлежности. Тоа лице сноси целосна одговорност за законитоста, оправданоста и правилната примена на утврдениот степен на класификација.

4.3. Критериуми за одредување степен на класификација

Класифицирањето на информации претставува процес со кој се определува степенот на заштита што треба да и се обезбеди на една информација, во зависност од штетата која може да настане по државата доколку таа биде откриена, изменета, уништена или употребена без одобрение.

При определување на степенот со кој ќе биде класифицирана една информација, се проценуваат индикаторите што укажуваат на видот и сериозноста на потенцијалната штета што може да настане доколку информацијата биде откриена или употребена без овластување. Врз основа на таквата процена се определува дали информацијата ќе биде означена како „ДРЖАВНА ТАЈНА“, „СТРОГО ДОВЕРЛИВО“, „ДОВЕРЛИВО“ или „ИНТЕРНО“, односно со степен кој е соодветен на ризикот и интересите што се штитат.

Определувањето на соодветниот степен на класификација на информацијата се врши врз основа на следниве посочени критериуми од ЗКИ кои се суштински за правилна заштита на државните интереси и безбедноста:

1. содржина на информацијата, и

2. проценка на можната штета и последиците кои би произлегле од неовластениот пристап или неовластената употреба на информацијата врз државните интереси и безбедноста.

Определувањето на класификацијата се базира на комбинација од содржината на информацијата и проценката на можната штета. Тоа значи дека не секоја чувствителна информација автоматски се смета за „тајна“ – таа мора да биде и потенцијално штетна по државата доколку биде откриена. Колку е поосетлива или покритична содржината на информацијата за функционирањето и интересите на државата и колку е поголема потенцијалната штета по државните интереси и безбедноста, толку повисок треба да биде степенот на класификација.

Табела 6 Критериуми за определување степен на класификација на информацијата

Критериум	Опис	Елементи	Контролни прашања за проценка
Содржина на информацијата	Ја опфаќа точноста, значењето и потенцијалното влијание на содржината на информацијата. Се проценува дали податоците се веродостојни, дали се однесуваат на критични функции или интереси и колку нивното откривање може да влијае врз државните институции или националната безбедност.	Интегритет	Дали информацијата е точна и проверена?
		Природа	Какви податоци содржи информацијата?
		Вредност	Колкава е корисноста и важноста на информацијата?
Проценка на можната штета и последици	Проценката ги опфаќа чувствителноста на содржината, односно степенот на нејзиното значење и потенцијалната штета од неовластено откривање; можните закани кои произлегуваат од актери, настани или околности што би можеле намерно или случајно да ја искористат постоечката ранливост; како и ризикот кој се изразува преку веројатноста за појава на инцидент и интензитетот на последиците што би произлегле за институцијата или државните интереси.	Чувствителност	Каква реакција би се предизвикала доколку информацијата излезе во јавност?
		Закана	Каков настан би можел да ја искористи постоечката ранливост и да предизвика штета врз информацијата или институцијата?
		Ризик	Колкава е веројатноста информацијата да биде компрометирана и каква штета би настанала врз државните интереси?

4.3.1. Содржина на информацијата

Содржината на информацијата како критериум се однесува на интегритетот, природата и вредноста на информацијата.

Интегритет на информацијата

Интегритетот на информацијата претставува степен до кој содржината е точна, целосна и непроменета од неовластени лица. При определување на степенот на класификација, потребно е внимателно да се оцени дали информацијата е заснована на проверени и сигурни податоци, дали се заснова на кредибилен извор и дали не постои ризик од манипулација, фалсификување или погрешно претставување.

Информација со висок интегритет има значајно влијание врз донесување одлуки, креирање политики и заштита на националните интереси. Затоа, доколку е утврдено дека содржината е прецизна и сигурна, таа може да бара повисок степен на заштита. Доколку, пак, постои сомнеж во точноста, потеклото или веродостојноста на информацијата, на пример, кога податоците се непотврдени, нецелосни или потенцијално изменети, ризикот од погрешно донесени одлуки се зголемува, а потребата од висока класификација се намалува.

Природа на информацијата

Природата на информацијата се однесува на суштинската содржина – дали информацијата опфаќа оперативни податоци, лични информации, стратешки планови, технички спецификации, или било кој вид чувствителни државни или институционални податоци. При проценката на информацијата се анализира што точно содржи и на која од претходно наведените области се однесува: одбраната и безбедноста на државата, надворешната политика и меѓународните односи, разузнавачките или контраразузнавачките



активности, критичната инфраструктура или економските и технолошките интереси од стратешко значење.

Колку е покритично полето што го засега, толку ќе биде поголема веројатноста дека информацијата треба да се класифицира со повисок степен.

Вредност на информацијата

Вредноста на информацијата се однесува на степенот на нејзината корисност, уникатност и стратешка важност, односно на потенцијалот што таа го носи за поддршка на донесувањето одлуки, овозможување дејствување или влијание врз национални, институционални, политички, економски или безбедносни процеси. Колку е поголема нејзината содржинска и оперативна тежина, толку е повисока потребата за нејзино заштитено и контролирано ракување.

При оценување на вредноста, се анализира не само самиот квалитет на податоците (точност, деталност, ексклузивност), туку и нивната способност да произведат последици – позитивни или негативни – доколку бидат користени од други субјекти.

Информациите со ниска содржинска или стратешка вредност не бараат висок степен на заштита, додека информации со висока аналитичка тежина, оперативна важност или влијание врз критични процеси се сметаат за приоритетни за класифицирање.

4.3.2. Проценка на можната штета и последиците

Проценката на можната штета и последиците кои би произлегле од неовластениот пристап или неовластената употреба на информацијата врз државните интереси и безбедноста како критериум се однесува на потенцијалните негативни последици што би настанале доколку информацијата биде откриена, злоупотребена или објавена без овластување.

Проценката може да се детализира низ анализа на **чувствителноста, заканата и ризикот** по информацијата.

Чувствителност на информацијата

Чувствителноста на информацијата ја определува сериозноста на последиците што би настанале доколку информацијата биде откриена, пристапена или употребена од неовластени лица. Овој критериум ја оценува потенцијалната штета по националната безбедност, јавниот интерес или функционирањето на институциите.

Колку што е поголема можната штета, толку е повисок степенот на чувствителност и потребата од класификација.

Проценката на чувствителноста секогаш треба да биде заснована на:

- конкретни инциденти и веројатност за нивна појава,
- влијанието врз државните интереси,
- временската чувствителност (дали со тек на време ризикот опаѓа).

Создавачот на информацијата треба внимателно да ја разгледа и предвиди потенцијалната реакција и интерпретација доколку информацијата би излегла во јавност, како и непосредните, среднорочните и долгорочните последици од нејзината незаштитеност.



Закана по информацијата

При утврдување на соодветниот степен на класификација, неопходно е да се процени и природата на заканата кон информацијата. Заканата претставува секоја потенцијална акција или настан што може да искористи одредена ранливост и да предизвика штета на институцијата, нејзините процеси или на националните интереси.

Ова значи дека заканите не постојат изолирано – тие стануваат реален ризик единствено кога ќе се пресечат со постоечките ранливости во системот. Ранливостите се слабости во инфраструктурата што се штити: недоследности во дизајнот на системот, пропусти во имплементацијата на безбедносните мерки, технички недостатоци или празнини во оперативните процеси што можат да бидат злоупотребени од неовластени субјекти.

Во овој контекст, проценката на заканата опфаќа:

- типот на потенцијалниот напаѓач или извор на заканата (надворешни актери, интерни лица, технички инциденти, природни појави);
- можноста за појава на заканата и нејзината потенцијална мотивација или капацитет да предизвика штета;
- начинот на кој заканата може да ја искористи конкретната ранливост, односно дали постојните слабости овозможуваат пристап, манипулација или откривање на информацијата;
- обемот и тежината на штетата, доколку заканата се реализира и информацијата биде компромитирана.

Ризик по информацијата

Ризик по информацијата претставува комбинација на веројатноста да се случи настан што ќе доведе до нарушување на доверливоста, интегритетот или достапноста на информацијата и тежината на последиците доколку таков настан се случи. Тој произлегува од спојување на два елементи:

1. веројатност дека ќе се реализира одредена закана и
2. импакт – односно степенот на штета што би настанала доколку се реализира заканата и информацијата биде компромитирана.

Проценката на ризикот треба да ги опфати следните аспекти:

- Веројатност: колку е веројатно информацијата да биде откриена, изменета или уништена од неовластено лице;
- Импакт: какви би биле последиците врз државните интереси доколку дојде до компромитирање;
- Најкритични фази од животниот циклус на информацијата (создавање, чување, пренос, користење, уништување).

Правилната проценка на ризикот е клучна за определување на соодветниот степен на класификација, идентификување на потребните безбедносни мерки и намалување на потенцијалните последици доколку се случи одреден инцидент.



4.4. Економска оправданост при класификација на информацијата

При определување на соодветниот степен на класификација, неопходно е да се земе предвид економската оправданост за заштита на информацијата. Овој аспект се однесува на тоа дали ресурсите што треба да се вложат за нејзина заштита – финансиски средства, човечки капацитети, техничка инфраструктура и административни процедури – се пропорционални со вредноста и чувствителноста на самата информација.

Не е секоја информација еднакво значајна, па затоа не е секогаш рационално да се инвестира во скапи безбедносни мерки. Целта е да се постигне оптимален баланс помеѓу:

- вредноста, значењето и чувствителноста на информацијата и
- степенот и видот на заштита што се применува.

Во проценката на економската оправданост се разгледуваат следниве прашања:

- Дали трошокот за заштита на информацијата е сразмерен со потенцијалната штета доколку информацијата биде компромитирана?
- Постојат ли поефикасни и поекономични алтернативи што овозможуваат доволно висок степен на безбедност?

Со проценка на економската оправданост се овозможува рационално управување со ресурсите на институциите и се спречува прекумерна заштита кај информации со мала вредност и недоволна заштита кај критични информации. На овој начин се придонесува кон балансиран пристап, без притоа да се создава непотребен административен и финансиски товар.

Со внимателна проценка на економската оправданост, институциите обезбедуваат ефикасно, рационално и законски усогласено определување на степенот на класификација на информациите, при што ресурсите се користат одговорно, а државните интереси се заштитуваат соодветно.

4.5. Определување на можната штета и последиците

Табелата подолу прикажува систематизиран преглед на степените на класификација на информациите во зависност од видот и интензитетот на можната штета што би можела да настане во случај на нивно неовластено откривање, користење или злоупотреба. Таа ја поврзува природата на последиците врз државните, институционалните и јавните интереси со соодветниот степен на класификација.

При користење на табелата, најнапред се утврдува каков тип и интензитет на последици би можел да настане („ако се причини ваква штета“), потоа се споредува со дадените примери од УАБ, а на крај се определува соодветниот степен на класификација.

На овој начин се обезбедува сразмерност помеѓу тежината на последиците и степенот на заштита, се олеснува доследната примена на законските критериуми и се намалува ризикот од прекумерна или недоволна класификација на информациите.



Табела 7 Определување на степенот на класификација на информацијата и ознаката „За ограничена

Ако неовластеното откривање на информацијата...	на што?
би ја намалила ефикасноста	на работењето на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, Градот Скопје и општините во градот Скопје
би предизвикало штета	на работењето на органите
би предизвикало штета	за важните интереси на Република Северна Македонија, кои се предуслови за креирање и остварување на трајните и виталните интереси на Република Северна Македонија: - изградба и развој на сите форми на соработка со соседите, а во интерес на мирот, безбедноста и развојот на Република Северна Македонија и нејзините соседи, - сопствен придонес за зачувување и унапредување на мирот и стабилноста во Југоисточна Европа (ЈИЕ) заради зајакнување на зоната на демократијата, безбедноста и просперитетот на сите земји во регионот, - учество во изградбата на мирот и стабилноста во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите, со цел - навремено и ефикасно решавање по мирен пат, - зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународниот поредок втемелен во меѓународното право, како и политичка и економска рамноправност на државите, - обезбедување на услови и унапредување на внатрешно-политичката стабилност и можности заради еднакво право на учество кое во себе треба да содржи и општоприфатен консензус во врска со прашањата од траен, витален и важен интерес на земјата, - создавање услови за унапредување на безбедносната култура, - изградба на праведна, социјална држава со еднакви можности за сите граѓани без оглед на нивната полова, расна, верска, политичка, социјална, културна и друга припадност, - создавање услови за изградба на општество со комуникации и односи со кои ќе се развиваат заедничките вредности и култура на живеењето, особено кај младата генерација, во духот на толеранцијата, негување на демократските вредности и почитување на личниот интегритет, втемелени во европската демократска традиција, без оглед на етничката, верска или друга припадност, и - зачувување и заштита на животната средина во државата во соработка со поширокото опкружување.
би предизвикало исклучително сериозна штета	за виталните интереси на Република Северна Македонија со кои се унапредува безбедносната состојба и со кои се создаваат услови за подобар живот на граѓаните и функционирање на државата и општеството: - заштита и унапредување на мирот и безбедноста, животот, здравјето, имотот и личната безбедност на граѓаните на Република Северна Македонија, - развој на мултиетничко општество засновано врз меѓусебна доверба, заеднички напори и стремеж на сите етнички заедници за стабилност и сестран напредок на државата, - економски развој заснован врз принципите на пазарната економија, приватната сопственост, постојано унапредување на животниот стандард и квалитетот на животот, како и заштита на виталната инфраструктура и ресурси на Република Северна Македонија, - заштита и унапредување на демократските основи на правната држава - политички плурализам, парламентарна демократија, поделба на власта и демократски и фер избори, владеење на правото, доследно почитување на човековите права и слободи, како и правата и слободите на граѓаните кои припааат на сите заедници и постојано одржување и унапредување на вкупната внатрешна безбедност на општеството и државата, - политичко-одбранбена интеграција во НАТО, политичка, економска и безбедносна интеграција во Европската унија, како и во другите системи за колективна безбедност.
би предизвикало загрозување и нанесување непоправливи штети	на трајните интереси на Република Северна Македонија: - зачувување и унапредување на државниот идентитет со слободно изразување на етничкиот идентитет на сите граѓани на Република Северна Македонија, и - заштита на независноста и територијалниот интегритет.

на пример...

тогаш, информацијата
треба да се
класифицира како ...

- да ја намали ефикасноста на работењето или да влијае врз условите за унапредувањето и зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата;
- да ја намали ефикасноста на работењето на изградбата на праведна, социјална држава со еднакви можности за сите граѓани;
- да ја намали ефикасноста на работењето врз политичките, финансиските, монетарните, економските и комерцијалните преговори на државата;
- да ја намали ефикасноста на работењето во развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации;
- да ја намали ефикасноста на работењето на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат и
- да ја намали ефикасноста на работењето на активностите на државата за зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународниот поредок втемелен во меѓународното право, како и политичка и економска рамноправност на државите.

ЗА ОГРАНИЧЕНА
УПОТРЕБА

- да причини штета или да влијае врз условите за унапредувањето и зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата;
- да причини значително страдање на лица;
- да причини штета на изградбата на праведна, социјална држава со еднакви можности за сите граѓани;
- да ги уназади политичките, финансиските, монетарните, економските и комерцијалните преговори на државата;
- да го спречува развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации;
- да им причини финансиска штета или да им овозможи несоодветни достигнувања или предност на правните или физичките лица;
- да влијае негативно на зачувувањето и заштитата на животната средина;
- да ги поткопува активностите на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат;
- да ги поткопува активностите на државата за зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународниот поредок втемелен во меѓународното право, како и политичка и економска рамноправност на државите и
- да влијае негативно на меѓународните односи на државата или на односите на странска земја или меѓународна организација со Република Северна Македонија.

ИНТЕРНО

- да причини штета или да влијае врз условите за унапредувањето и зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата;
- да причини значително страдање на лица;
- да причини штета на изградбата на праведна, социјална држава со еднакви можности за сите граѓани;
- да ги уназади политичките, финансиските, монетарните, економските и комерцијалните преговори на државата;
- да го спречува развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации;
- да им причини финансиска штета или да им овозможи несоодветни достигнувања или предност на правните или физичките лица;
- да влијае негативно на зачувувањето и заштитата на животната средина;
- да ги поткопува активностите на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат;

ДОВЕРЛИВО

- да причини штета или да влијае врз условите за унапредувањето и зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата;
- да причини значително страдање на лица;
- да причини штета на изградбата на праведна, социјална држава со еднакви можности за сите граѓани;
- да ги уназади политичките, финансиските, монетарните, економските и комерцијалните преговори на државата;
- да го спречува развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации;
- да им причини финансиска штета или да им овозможи несоодветни достигнувања или предност на правните или физичките лица;
- да влијае негативно на зачувувањето и заштитата на животната средина;
- да ги поткопува активностите на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат;

СТРОГО
ДОВЕРЛИВО

- директно да го загрози територијалниот интегритет и суверенитет, како и уставниот поредок на државата;
- директно да ја загрози внатрешната стабилност на државата;
- директно да доведе до масовни човечки губитоци;
- да причини непоправливи штети на оперативната ефикасност или безбедност на државата или на ефикасноста на исклучително вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот;
- да причини непоправливи штети на основните слободи и права на човекот и граѓанинот, демократијата и владеењето на правото;
- да причини непоправливи штети на унапредувањето и развојот на економијата на државата, на заштитата на сопственоста, слободата на пазарот и претприемништвото, хуманизмот, социјалната правда и солидарноста;
- да причини непоправливи штети на заштитата и унапредувањето на животната средина на државата;
- да нанесе тешки долготрајни последици на унапредувањето и развојот на локалната самоуправа во државата и
- директно да го загрози остварувањето на целите на меѓународната политика на државата или да нанесе непоправливи штети на меѓународните односи на државата или на односите на странска земја или меѓународна организација со Република Северна Македонија.

ДРЖАВНА ТАЈНА



4.5.1. За ограничена употреба

Со ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“ се означува само онаа информација чие откривање би ја намалила ефикасноста на работењето на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, Градот Скопје и општините во градот Скопје.

Конкретните последици што би настанале со неовластено откривање на овие информации се:

1. да ја намали ефикасноста на работењето или да влијае врз условите за унапредување и зачувување на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата

Се однесува на интерни информации, процедури или анализи кои се однесуваат на безбедносни аспекти во функционирањето на државните органи, чие откривање може да доведе до попречување на ефективното работење на органите или да создаде оперативни слабости.

2. да ја намали ефикасноста на работењето на изградбата на праведна, социјална држава со еднакви можности за сите граѓани

Се однесува на информации за социјални програми, распределба на ресурси или мерки за поддршка на ранливи групи, кои ако се откријат, може да го попречат градењето на еднакви можности за сите граѓани во државата.

3. да ја намали ефикасноста на работењето врз политичките, финансиските, монетарните, економските и комерцијалните преговори на државата

Се однесува на информации за преговори со странски држави, инвеститори или институции кои често содржат чувствителни податоци за услови и стратегии. Откривањето на овие податоци може да ја ослаби преговарачката позиција на државата.

4. да ја намали ефикасноста на работењето во развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации

Се однесува на информации за оперативните аспекти на договорите или обврските од меѓународни спогодби кои се чувствителни и нивното откривање може да го наруши спроведувањето или да создаде дипломатски тензии.

5. да ја намали ефикасноста на работењето на активностите на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат

Се однесува на информации за дипломатски иницијативи, безбедносни проекти или стратегии за превенција на конфликти, кои, ако се откријат, можат да го ослабат влијанието на државата или да доведат до саботажа на активностите.

6. да ја намали ефикасноста на работењето на активностите на државата за зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународното право, како и политичка и економска рамноправност на државите

Се однесува на информации кои покажуваат отстапување од меѓународни стандарди, процедури или обврски што може да ја ослаби позицијата на државата на меѓународен план и да ја загрози довербата на партнерите.

4.5.2. Интерно

Со степен „ИНТЕРНО“ се класифицира само онаа информација чие неовластено откривање би предизвикало штета за работењето на органите.

Конкретните последици што би настанале со неовластено откривање на овие информации се:

1. да причини штета или да влијае врз условите за унапредувањето и зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност на државата

Се однесува на информации за начинот на справување со безбедносни ризици и закани и чие откривање би предизвикало слабеење и недоверба во безбедносниот систем.

2. да причини значително страдање на лица

Се однесува на информации чие откривање би можело да доведе до психолошка траума, физичко страдање, дискриминација или опасност за група лица.

3. да причини штета на изградбата на праведна, социјална држава со еднакви можности за сите граѓани

Се однесува на информации за интерни мерки, активности и практики во социјалните политики, со чие откривање може да се предизвикаат политички манипулации, да се наруши довербата во институциите и да се создаде впечаток на неправедност меѓу граѓаните.

4. да ги уназади политичките, финансиските, монетарните, економските и комерцијалните преговори на државата

Се однесува на информации за преговорите со странски инвеститори, меѓународни банки или држави кои содржат чувствителни податоци за услови, цени и стратегии. Откривањето на ваквите информации може да ја ослаби преговарачката позиција на државата.

5. да го спречува развојот или операциите утврдени во билатералните или мултилатералните договори кои државата ги склучила со странски земји или меѓународни организации

Се однесува на информации поврзани со договорите со други држави или организации чие откривање може да предизвика дипломатски тензии.

6. да им причини финансиска штета или да им овозможи несоодветни достигнувања или предност на правните или физичките лица



Се однесува на информации што би овозможиле на одредени лица или компании да стекнат финансиска предност или да избегнат обврски.

7. да влијае негативно на зачувувањето и заштитата на животната средина

Се однесува на информации за животната средина кои можат да предизвикаат паника или да се искористат за општествен притисок.

8. да ги поткопува активностите на државата на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите

Се однесува на информации за дипломатски напори, безбедносни иницијативи или стратегии за превенција на конфликти кои би можеле да бидат саботирани.

9. да ги поткопува активностите на државата за зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународното право и политичка и економска рамноправност на државите

Се однесува на информации чие откривање би можело да ја наруши репутацијата на државата.

10. да влијае негативно на меѓународните односи на државата или на односите на странска земја или меѓународна организација со Република Северна Македонија

Се однесува на информации содржани во дипломатски комуникации, чувствителни договори и сл., чие откривање би можело да предизвика дипломатски инцидент.

4.5.3. Доверливо

Со степен „ДОВЕРЛИВО“ се класифицира само онаа информација чие неовластено откривање би предизвикало сериозна штета за важните интереси на Република Северна Македонија.

Конкретните последици што би настанале со неовластено откривање на овие информации се:

1. да причини сериозна штета на мирот, демократските основи на правната држава и развојот на мултиетничкото општество

Се однесува на информации кои, ако се објават, би можеле да поттикнат општествена нестабилност, нарушување на јавниот мир или поткопување на демократските вредности.

2. да причини сериозна штета за животот, здравјето, имотот и личната безбедност или слободата на човекот и граѓанинот

Се однесува на информации чие неовластено откривање би можело да доведе до загрозување на граѓаните, нивниот имот или здравје.

3. да причини сериозна штета на оперативната ефикасност или безбедност на државата или на ефикасноста на вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани,



особено со тероризмот

Се однесува на информации кои може да ја ослабат способноста на институциите да се справат со безбедносни ризици, тероризам или организиран криминал.

4. да причини сериозна штета или да е значително во спротивност со финансиските, монетарните, економските и стопанските интереси на државата

Се однесува на информации кои, ако се откријат, би можеле да влијаат на стабилноста на пазарите, буџетот или економските политики на државата.

5. да причини сериозна штета на животната средина на државата

Се однесува на информации кои би можеле да бидат злоупотребени на начин што ќе резултира со еколошка деградација или ризици за здравјето на населението.

6. да причини сериозна штета на унапредувањето и развојот на локалната самоуправа во државата

Се однесува на информации поврзани со развојни проекти, распределба на средства или критична инфраструктура на локално ниво.

7. да причини сериозна штета или да е значително во спротивност со политичко-одбранбената интеграција на државата во НАТО, со економската и безбедносна интеграција во Европската Унија или во другите системи за колективна безбедност

Се однесува на информации чие откривање може да ја наруши довербата меѓу сојузниците и да ја загрози интеграцијата на државата во меѓународни организации.

8. да причини сериозна штета во развојот или операциите утврдени во меѓународните договори ратификувани согласно Уставот на Република Северна Македонија и меѓународните документи кои државата ги склучила со странски земји или меѓународни организации

Се однесува на информации поврзани со тековни меѓународни преговори, договори или соработки, чија компромитација би ја ослабила позицијата на државата.

9. да причини сериозна штета на меѓународните односи на државата, така што ќе предизвика формален протест или други санкции

Се однесува на информации чие откривање може да предизвика негативна дипломатска реакција (инцидент, санкција, прекин на соработка и др.).

10. да ги прекине или на друг начин значително да ги оневозможи значајните активности на државата на меѓународен план или активностите на странска земја или меѓународна организација на планот на соработка со Република Северна Македонија

Се однесува на информации кои можат да влијаат врз соработката во заеднички операции, иницијативи или програми со странски партнери.



4.5.4. Строго доверливо

Со степен „СТРОГО ДОВЕРЛИВО“ се класифицира само онаа информација чие неовластено откривање би предизвикало исклучително сериозна штета за виталните интереси на Република Северна Македонија.

Конкретните последици што би настанале со неовластено откривање на овие информации се:

1. да причини исклучително сериозна штета на независноста и територијалниот интегритет на државата

Се однесува на информации кои, ако се откријат, би можеле да создадат реална опасност за нарушување на независноста или територијалното единство на државата, преку поттикнување внатрешни и надворешни конфликти, охрабрување сепаратистички движења, итн.

2. да причини исклучително сериозна штета на државниот идентитет со слободно изразување на етничкиот идентитет на сите граѓани

Се однесува на информации што се однесуваат на етничкиот идентитет и државната политика за мултиетничко општество, чија компромитација би можела да доведе до тензии, дискриминација, нарушување на меѓуетничките односи, социјалната кохезија и чувството на припадност кон државата.

3. директно да го загрози животот или исклучително сериозно да влијае врз јавниот ред или врз личната безбедност или слобода на човекот и граѓанинот

Се однесува на информации за безбедносни мерки, справување со протести или криминални групи и сл., чие откривање би можело директно да го загрози животот или безбедноста на лица, или да предизвика сериозен јавен немир.

4. да причини исклучително сериозна штета на оперативната ефикасност или безбедност на државата или на ефикасноста на исклучително вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот

Се однесува на информации поврзани со тајни одбранбени, безбедносни или разузнавачки активности, операции, методи или агенти, чие откривање би ја намалило способноста на државата да реагира на терористички или други безбедносни закани.

5. да причини исклучително сериозна материјална штета на финансиските, монетарните, економските и стопанските интереси на државата

Се однесува на информации кои би можеле да предизвикаат финансиска нестабилност, девалвација на валутата или нарушување на пазарната доверба.

6. да причини исклучително сериозна штета на животната средина на државата

Се однесува на информации поврзани со заштитата на животната средина, чија злоупотреба може да предизвика сериозни еколошки катастрофи или здравствени последици.

7. да причини исклучително сериозна штета на унапредувањето и развојот на локалната самоуправа во државата

Се однесува на информации поврзани со локални политики, инфраструктурни проекти или финансиски планови, чија компромитација може да предизвика сериозна штета во работењето на локалната самоуправа.

8. да причини исклучително сериозна штета на остварувањето на целите на меѓународната политика или на меѓународните односи на државата или на односите на странска земја или меѓународна организација со Република Северна Македонија

Се однесува на информации чија компромитација може сериозно да го наруши угледот на државата, да предизвика дипломатски спор или да влијае негативно врз меѓународните партнерства.

4.5.5. Државна тајна

Состепен „ДРЖАВНА ТАЈНА“ се класифицира само онаа информација чие неовластено откривање би предизвикало загрозување и нанесување непоправливи штети на трајните интереси на Република Северна Македонија.

Конкретните последици што би настанале со неовластено откривање на овие информации се:

1. директно да го загрози територијалниот интегритет и суверенитет, како и уставниот поредок на државата

Се однесува на информации чие објавување би овозможило или олеснило акти кои водат до нарушување на границите, територијалниот интегритет, или до поткопување на уставните институции и основниот уставен поредок. Нивното откривање би овозможило надворешни или внатрешни актери да ги поткопаат државните институции или да предизвикаат конфликт.

2. директно да ја загрози внатрешната стабилност на државата

Се однесува на информации кои, ако се објават, би можеле да предизвикаат загрозување и сериозни нарушувања на јавниот ред и мир, појава на масовни немири, паника, недоверба, дестабилизација или колапс на витални државни функции.

3. директно да доведе до масовни човечки губитоци

Се однесува на информации кои ако се откријат би можеле да резултираат со загуба на голем број животи (како резултат на вооружен конфликт, терористички напад, човечки предизвикана катастрофа, инциденти во критична инфраструктура, итн).

4. да причини непоправливи штети на оперативната ефикасност или безбедност на државата или на ефикасноста на исклучително вредни одбранбени, безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот

Се однесува на информации за тајни операции, методологии, извори или средства на безбедносно-разузнавачките служби и одбранбените институции, што, доколку се откријат,



значајно би го нарушило нивното функционирање.

5. да причини непоправливи штети на основните слободи и права на човекот и граѓанинот, демократијата и владеењето на правото

Се однесува на информации чие откривање би довело до трајно нарушување на демократските институции, владеењето на правото или правната заштита на слободите и правата на граѓаните.

6. да причини непоправливи штети на унапредувањето и развојот на економијата на државата, на заштитата на сопственоста, слободата на пазарот и претприемништвото, хуманизмот, социјалната правда и солидарноста

Се однесува на информации кои, ако се откријат, би предизвикале сериозна и долгорочна економска штета – на пример, нарушување на финансиските пазари, сериозни финансиски манипулации или загрозување на сопственичките права.

7. да причини непоправливи штети на заштитата и унапредувањето на животната средина на државата

Се однесува на информации чие објавување би довело до откривање на ранливи еко-системи или би овозможило активности кои ќе предизвикаат долгорочна штета врз животната средина и населението (паника, еколошки катастрофи, сериозни здравствени последици и др.).

8. да нанесе тешки долготрајни последици на унапредувањето и развојот на локалната самоуправа во државата

Се однесува на информации кои, ако се откријат, би го парализирале или долгорочно би го ослабиле функционирањето и развојот на локалните самоуправи, нивните финансиски механизми или критична инфраструктура на локално ниво.

9. директно да го загрози остварувањето на целите на меѓународната политика на државата или да нанесе непоправливи штети на меѓународните односи на државата или на односите на странска земја или меѓународна организација со Република Северна Македонија

Се однесува на информации кои, ако се откријат, ќе ја компромитираат довербата меѓу државите, ќе доведат до прекин на чувствителни дипломатски преговори или ќе предизвикаат долгорочни дипломатски и меѓународни повреди.

5. РИЗИЦИ ОД НЕСООДВЕТНО КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ

Одредувањето на степенот на класификација мора да биде строго сразмерно со проценетата штета од неовластен пристап или неовластена употреба. На овој начин се спречуваат две ризични појави:

- **прекумерна класификација** – прекумерната класификација настанува кога на информацијата и се доделува повисок степен на тајност од реално потребниот. Ова води кон:

- непотребно ограничување на пристапот за службени лица кои треба да ја користат информацијата во својата работа (информацијата не е достапна до лица кои имаат потреба да ја знаат),
- забавено донесување одлуки и нарушена ефикасност во институциите,
- зголемени административни и финансиски трошоци за чување, пренос и заштита на информациите,
- ризик од создавање „култура на тајност“ и намалена транспарентност на институцијата.

- **недоволна класификација** – недоволната класификација се јавува кога на информацијата и се доделува понизок степен на заштита од потребниот, што резултира со:

- зголемен ризик критичните податоци да станат достапни на неовластени лица,
- можност за сериозни безбедносни, политички или економски последици,
- нарушување на оперативните активности на државните органи,
- потенцијално поткопување на меѓународната доверба и соработка.

За да не се случи ова, класифицирањето бара правилна, внимателна и професионална процена на содржината на информацијата, потенцијалната штета од неовластено откривање и времетраењето на чувствителноста. Со соодветен баланс, институциите обезбедуваат заштита на државните интереси, а истовремено овозможуваат ефикасно и одговорно ракување со класифицираните информации.



6. ПРАКТИЧНИ ПРЕПОРАКИ ЗА КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ

Познавање на законската рамка

Секогаш имајте јасно познавање и разбирање за ЗКИ и подзаконските акти кои го регулираат класифицирањето на информациите.

Проценка на заканата и ризикот од откривање на информацијата

Размислете што би се случило ако информацијата биде откриена неовластено и како тоа би влијаело на интересите на државата или институцијата.

Примена на принципите при одредување на степените на класификација на информациите

Примена на принципите на штета, пропорционалност, нужност, временска ограниченост и одговорност, како и други утврдени добри и позитивни практики, при одредување и оправдување на соодветниот степен на класификација на информациите.

Објективност и непристрасност

Одредувањето на степенот мора да се базира на законски утврдените критериуми (содржината на информацијата и проценката на штетата и последиците), а не на лични интереси или субјективни критериуми.

Конзистентност во класификацијата

Информации со слична содржина треба да имаат сличен степен на класификација, за да се избегне конфузија, нееднаква и несоодветна заштита.

Образложување на предложениот степен на класификација

Изборот на степен треба да се образложи во предлогот од изработувачот.

Почитување на временската осетливост

Проценете дали информацијата со текот на времето губи чувствителност и дали е потребно ревидирање на степенот.

Консултација и колегијална проверка

При сомнеж или комплексни случаи, консултирајте се со релевантни експерти, колеги или надлежни органи.

Обучен и информиран персонал

Сите лица кои учествуваат во процесот потребно е да се едуцирани за критериумите, процедурите и обврските за класификација.

Безбедносна култура во постапувањето

Одредувањето степен на класификација е дел од заштитата на државата, институцијата и граѓаните – секогаш третирајте ја информацијата како потенцијално чувствителна.



БИБЛИОГРАФИЈА

2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, <https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng>.

Бакрески, О., Деаноска-Трендафилова, А. (2021). Коментар на законот за класифицирани информации, ДЦАФ, Скопје, https://www.dbki.gov.mk/files/pdf_files/Komentar_Makedonski.pdf.

Закон за класифицирани информации, „Службен весник на Република Северна Македонија“ бр. 275/2019.

Кривичен законик, „Службен весник на Република Македонија“ бр. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 и 248/2018 и „Службен весник на Република Северна Македонија“ бр. 36/2023 и 188/2023. Одлуки на Уставниот суд на Република Македонија: У. бр. 220/2000 од 30 мај 2001 година, објавена во „Службен весник на Република Македонија“ бр. 48/2001; У. бр. 210/2001 од 6 февруари 2002 година, објавена во „Службен весник на Република Македонија“ бр. 16/2002; У. бр. 206/2003 од 9 јуни 2004 година, објавена во „Службен весник на Република Македонија“ бр. 40/2004; У. бр. 228/2005 од 5 април 2006 година, објавена во „Службен весник на Република Македонија“ бр. 50/2006 и У. бр. 169/2016 од 16 ноември 2017 година, објавена во „Службен весник на Република Македонија“ бр. 170/2017.

Национална концепција за безбедност и одбрана, „Службен весник на Република Македонија“ бр. 40/2003

Уредба за административна безбедност на класифицирани информации и на информации за ограничена употреба, „Службен весник на Република Северна Македонија“ бр. 204/2023.

Уредба за безбедност на лица корисници на класифицирани информации, „Службен весник на Република Северна Македонија“ бр. 157/2022.

Уредба за индустриска безбедност на класифицирани информации, „Службен весник на Република Македонија“ бр. 16/2005.

Уредба за информатичка безбедност на класифицирани информации, „Службен весник на Република Македонија“ бр. 16/2005.

Уредба за физичка безбедност на класифицирани информации, „Службен весник на Република Северна Македонија“ бр. 175/2025.

Устав на Република Македонија, „Службен весник на Република Македонија“ бр. 52/1991, со Амандманите I и II на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 1/1992, Амандманот III на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 31/1998, Амандманите IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV, XVI, XVII и XVIII на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 91/2001, Амандманот XIX на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 84/2003, Амандманите XX, XXI, XXII, XXIII, XXIV, XXV, XXVI, XXVII, XXVIII, XXIX и XXX на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 107/2005, Амандманот XXXI на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 3/2009, Исправката на Амандманот XXXI на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 13/2009, Амандманот XXXII на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 49/2011, Амандманите XXXIII, XXXIV, XXXV и XXXVI на Уставот на Република Македонија, „Службен весник на Република Македонија“ бр. 6/2019, и Објавата, „Службен весник на Република Македонија“ бр. 36/2019.



UDHËZUES PËR KLASIFIKIMIN E INFORMACIONEVE

Shkup, 2026

Prodhuar nga:

Drejtoria për Siguri të Informacioneve të Klasifikuara në koordinim me përfaqësuesit e komunitetit të sigurisë-inteligjencës të Republikës së Maqedonisë së Veriut

Redaktor:

Vllado Gjerdovski

Konsulenti i jashtëm:

Kire Babanoski

Botues:



©DCAF, 2026

All rights reserved

DCAF – Geneva Center for Security Sector Governance
Maison de la Paix Chemin Eugène-Rigot 2E, CH1202- Geneva, Switzerland

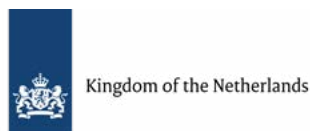
@DCAF, 2026

Të gjitha të drejtat e rezervuara

DCAF – Qendra për Menaxhim me Sektorin e Sigurisë – Gjenevë – Filiali Shkup
rr. "Maqedonia" nr. 11-1 / 2, 1000 Shkup, Republika e Maqedonisë Veriore

Udhëzuesi u përgatit në kuadër të **Programit për Reformën e Sektorit të Inteligjencës dhe Sigurisë në Republikën e Maqedonisë së Veriut**, i zbatuar nga DCAF – Qendra e Gjenevës për Menaxhim me Sektorin e Sigurisë dhe i mbështetur financiarisht nga Agjencia Zvicerane për Zhvillim dhe Bashkëpunim (SDC), Ministria e Punëve të Jashtme e Holandës dhe Agjencia Suedeze për Zhvillim Ndërkombëtar (Sida).

Përmbajtja e këtij publikimi nuk shpreh qëndrimet dhe opinionet e donatorëve ose të DCAF-së.



CIP - Katalogimi në publikim
Biblioteka Kombëtare dhe Universitare "Shën Kliment Ohridski", Shkup

PARATHËNIE

Programi për Reformë në Sektorin e Inteligjencës dhe Sigurisë në Republikën e Maqedonisë së Veriut (2021–2026), i zbatuar nga DCAF – Qendra e Gjenevës për Menaxhim me Sektorin e Sigurisë, synon të mbështesë institucionet e sigurisë, inteligjencës, drejtësisë dhe mbikëqyrjes në forcimin e kapaciteteve të tyre për qeverisje të mirë, llogaridhënie dhe mbikëqyrje efektive demokratike. Një nga segmentet kryesore të kësaj mbështetje është siguri i proceseve të harmonizuara, transparente dhe efikase në fushën e menaxhimit dhe trajtimit të informacionit të klasifikuar, duke respektuar plotësisht parimet e sundimit të ligjit dhe mbrojtjen e të drejtave dhe lirive të njeriut.

Në kuadër të aktiviteteve të zbatuara në Program, u identifikuan sfida të rëndësishme në lidhje me klasifikimin e informacionit, duke përfshirë:

- mospërputhje në zbatimin e kriterëve për përcaktimin e shkallëve të klasifikimit,
- klasifikimin e tepruar dhe ndonjëherë të pajustificuar të informacionit,
- mungesa e mekanizmave të qartë për kontrollin dhe verifikimin e klasifikimit,
- praktika të ndryshme institucionale që çojnë në bashkëpunim të kufizuar ndër-institucional dhe shkëmbim informacioni.

Për të adresuar këto sfida, DCAF organizoi disa diskutime shumë-sektoriale me ekspertë me përfaqësues nga institucionet përkatëse shtetërore. Në këto ngjarje u mundësua shkëmbimi konstruktiv i përvojave dhe u përcaktuan bazat për promovimin e harmonizimit të proceseve të klasifikimit, në përputhje me kuadrin ligjor ekzistues dhe standardet ndërkombëtare. Nga diskutimet lindi nevoja për të zhvilluar udhëzime të unifikuara, të qarta dhe praktikisht të zbatueshme për klasifikimin e informacionit, me qëllim forcimin sistematik të kapaciteteve institucionale dhe inkurajimin e efikasitetit operacional në sektorin e sigurisë dhe inteligjencës.

Ky **Udhëzues për Klasifikimin e Informacionit** është rezultat i kësaj iniciative të përbashkët. Objektivat e tij janë:

- të ofrojë kriterë specifikë për përcaktimin e shkallëve të klasifikimit,
- të mbështesë krijimin e praktikave të kontrollit të brendshëm dhe verifikimit,
- të kontribuojë në një zbatim më të harmonizuar, racional dhe të përgjegjshëm të standardeve të klasifikimit të informacionit.

Udhëzuesi është një mjet praktik për të gjithë përpunuesit e informacionit të klasifikuar, i cili do të vazhdojë të promovohet përmes një procesi aplikimi, trajnimi dhe konsultimi ndër-institucional.

DCAF, së bashku me institucionet e sigurisë-inteligjencës dhe Drejtorinë për Sigurinë e Informacioneve të Klasifikuara si bartës të procesit, mbetet e angazhuar për mbështetje të mëtejshme në forcimin e sistemit të sigurisë bazuar në sundimin e ligjit, profesionalizmin, integritetin dhe standardet e harmonizuara.

*DCAF – Qendra e Gjenevës për Menaxhim me Sektorin e Sigurisë
Shkup, 2026*

Mesazh nga Drejtori i Drejtorisë për Siguri të Informacioneve të Klasifikuara



Mbrojtja e informacionit të klasifikuar është një nga shtyllat kryesore të sigurisë kombëtare dhe të besimit midis institucioneve. Në kushtet e sfidave dinamike të sigurisë, është me rëndësi të madhe që të gjithë bartësit dhe përdoruesit e informacionit të klasifikuar të veprojnë me përgjegjësi, profesionalizëm dhe në përputhje me ligjet dhe aktet nënligjore në fuqi.

Ky udhëzues është përgatitur me qëllim që të ofrojë udhëzime të qarta dhe praktike për trajtimin, mbrojtjen dhe menaxhimin e duhur të informacionit të klasifikuar. Zbatimi i tij i vazhdueshëm do të kontribuojë në rritjen e kulturës së sigurisë, zvogëlimin e rreziqeve të qasjes së

si dhe forcimin e integritetit të proceseve institucionale.

Ky udhëzues para Ju, nuk është vetëm një dokument. Është një mjet që duhet t'ju udhëzojë, t'ju kujtojë dhe t'ju ndihmojë në punën tuaj të përditshme. Vlera e tij e vërtetë shihet vetëm kur e zbatojmë në mënyrë të vazhdueshme dhe të përgjegjshme.

Secili prej jush ka një rol të rëndësishëm për të luajtur. Çdo qasje në informacion është përgjegjësi. Çdo vendim, edhe më i vogli, mund të ketë një ndikim të madh. Kjo është arsyeja pse kujdesi, disiplina dhe etika profesionale nuk janë një zgjedhje, por një domosdoshmëri.

Më lejoni të jem i qartë: siguria nuk pranon kompromise. Nuk ka "mjaftueshëm të mira" kur bëhet fjalë për mbrojtjen e informacionit të klasifikuar. Ka vetëm procedura korrekte dhe një detyrim për t'i ndjekur gjithmonë ato.

Të ruajmë besimin që na është dhënë.

Të mbrojmë institucionet që na janë besuar.

Dhe të ndërtojmë një sistem në të cilin të gjithë mund të mbështetemi.

Ju faleminderit.

Florim Jaja

Drejtori i Drejtorisë për Siguri të Informacioneve të Klasifikuara

Shkup, 2026



PËRMBAJTJA

LISTA E TABELAVE	41
SHKURTESAT E PËRDORURA	41
1. Hyrje	42
2. Krijuesi dhe përpunuesi i informacionit të klasifikuar	43
2.1. Krijuesi i informacionit të klasifikuar	43
2.2. Përpunuesi i informacionit të klasifikuar	45
2.3. Diferencimi i roleve midis krijuesit dhe përpunuesit	46
2.4. Përgjegjësia e përpunuesit dhe krijuesit të informacionit të klasifikuar	46
3. Notat e klasifikimit të informacionit	47
4. Procesi i përcaktimit të nivelit të klasifikimit	50
4.1. Identifikimi i informacionit	50
4.2. Parimet gjatë përcaktimit të nivelit të klasifikimit	50
4.3. Kriteret për përcaktimin e shkallës së klasifikimit	51
4.3.1. Përmbajtja e informacionit	52
4.3.2. Vlerësimi i dëmeve dhe pasojave të mundshme	53
4.4. Arsyetimi ekonomik për klasifikimin e informacionit	54
4.5. Përcaktimi i dëmeve dhe pasojave të mundshme	55
4.5.1. PËR PËRDORIM TË KUFIZUAR	58
4.5.2. INTERNE	59
4.5.3. KONFIDENCIALE	60
4.5.4. RREPTËSISHT KONFIDENCIALE	61
4.5.5. SEKRET SHTETËROR	63
5. Rreziqet e klasifikimit joadekuat të informacioneve	64
6. Rekomandime praktike për klasifikimin e informacioneve	65
BIBLIOGRAFIA	66



Lista e tabelave

Tabela 1	Detyrat e krijuesit të informacionit të klasifikuar	44
Tabela 2	Detyrat e përpunuesit të informacionit të klasifikuar.	45
Tabela 3	Krahasimi i roleve të përpunuesit dhe krijuesit	46
Tabela 4	Shkallët e klasifikimit të informacionit dhe kuptimi i tyre	48
Tabela 5	Masat paraprake të sigurisë të zbatueshme për informacionin e klasifikuar dhe për etiketën “Për përdorim të kufizuar”	49
Tabela 6	Kriteret për përcaktimin e shkallës së klasifikimit të informacionit	52
Tabela 7	Përcaktimi i nivelit të klasifikimit të informacionit dhe shënimit “Për përdorim të kufizuar” në varësi të dëmit të mundshëm dhe pasojave që do të mund të lindnin nga zbulimi i paautorizuar	56

Shkurtesat e përdorura

nr.	numër
DSIK	Drejtoria për Siguri të Informacioneve të Klasifikuara
BE	Bashkimi Evropian
LIK	Ligji për informacione të klasifikuara
etj.	dhe të tjera
EJL	Evropa Juglindore
SKI	Sistemi i komunikimit dhe informimit
ngj.	të ngjashme
par.	paragrafi
neni	neni
RrSA	Rregullore për sigurinë administrative të informacioneve të klasifikuara dhe të informacioneve për përdorim të kufizuar



1. HYRJE

Mbrojtja e informacioneve të klasifikuara është një parakusht themelor për funksionimin efektiv të organeve të qeverisjes shtetërore dhe lokale, mbrojtjen e sigurisë dhe mbrojtjes së shtetit, ruajtjen e integritetit dhe sovranitetit të tij territorial, rendit kushtetues, interesit publik, si dhe garantimin e lirive dhe të drejtave të njeriut dhe qytetarit.

Mes rritjes së sfidave të sigurisë dhe rreziqeve dinamike, trajtimi i duhur i informacionit është thelbësor për ruajtjen e stabilitetit, sigurisë dhe besimit në institucione. Klasifikimi i informacioneve mundëson qasje të rregulluar dhe zbatimin e masave përkatëse të mbrojtjes, në bazë të ndjeshmërisë së tyre dhe dëmit të mundshëm që mund të shkaktohet nga zbulimi ose përdorimi i tyre i paautorizuar.

Sistemi për informacione të klasifikuara në Republikën e Maqedonisë së Veriut është vendosur mbi bazën e një kornize të qartë ligjore, që ka për qëllim mbrojtjen e informacioneve me rëndësi për sigurinë kombëtare dhe interesa të tjera jetike shtetërore. Rregullorja kryesore që rregullon këtë fushë është Ligji për informacione të klasifikuara (*) (LIK), "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut" nr. 275/2019. Ligji është hartuar sipas kërkesave të NATO-s dhe në përputhje me standardet e përcaktuara në direktivat e saj për sigurinë e informacionit të klasifikuar, si dhe me standardet e Bashkimit Evropian, siç është Vendimi i Këshillit të Bashkimit Evropian (BE) i 23 shtatorit 2013 mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së (CELEX numër 32013D0488), duke siguruar zbatueshmërinë e këtyre standardeve në sistemin kombëtar për sigurinë e informacionit të klasifikuar. Me ligjin rregullohen:

- procedurat, kushtet dhe kriteret për klasifikimin e informacionit,
- masat dhe aktivitetet për mbrojtjen dhe sigurinë e tyre,
- të drejtat, detyrimet dhe përgjegjësitë e krijuesve dhe përdoruesve të informacionit të klasifikuar,
- parimet për shkëmbimin kombëtar dhe ndërkombëtar të informacionit të klasifikuar,
- mbikëqyrjen inspektuese mbi zbatimin dhe çështje të tjera që lidhen me qasjen, përdorim in dhe trajtimin e informacionit të klasifikuar.

Në funksion të zbatimit të ligjit janë miratuar një sërë aktesh nënligjore (rregullore), të cilat rregullojnë aspektet specifike të sigurisë së informacioneve të klasifikuara:

- Rregullore për sigurinë administrative të informacioneve të klasifikuara;
- Rregullore për sigurinë fizike të informacionit të klasifikuar;
- Rregullore për sigurinë e personave përdorues të informacionit të klasifikuar;
- Rregullore për sigurinë informatike të informacionit të klasifikuar;
- Rregullore për sigurinë industriale të informacionit të klasifikuar.

Koncepti kombëtar për siguri dhe mbrojtje i Republikës së Maqedonisë së Veriut përcakton interesat e përhershme, jetike dhe të rëndësishme të shtetit, të cilat burojnë nga vlerat themelore të përcaktuara me Kushtetutë dhe janë të orientuara drejt mbrojtjes së sovranitetit, integritetit territorial, rendit kushtetues dhe të drejtave dhe lirive themelore të qytetarëve. Në këtë kuptim, mbrojtja e informacionit të klasifikuar përbën një mekanizëm kyç për mbështetjen e politikave të sigurisë dhe për sigurimin e funksionimit të qëndrueshëm dhe të pandërprerë të shtetit, në përputhje me standardet dhe detyrimet ndërkombëtare.

¹ 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, <https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng>

Arsyetimi i përgatitjes së këtij Udhëzuesi lind nga detyra e dhënë ligjërisht nga DSIK-ja për të propozuar dhe zbatuar masa dhe aktivitete për mbrojtjen e informacionit të klasifikuar. Përveç kësaj, Vendimi i Këshillit të Bashkimit Evropian i 23 shtatorit 2013 mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së (CELEX numër 32013D0488), gjegjësisht Shtojca III e tij – Menaxhimi i Informacionit të Klasifikuar, përcakton masa administrative për kontrollin e informacionit të klasifikuar të BE-së gjatë gjithë ciklit të tij operacional, me qëllim parandalimin ose zbulimin e kompromisit të qëllimshëm ose aksidental ose humbjen e këtij informacioni. Sipas pikave 2 dhe 3 të Aneksit, informacioni klasifikohet kur kërkon mbrojtje në aspektin e konfidentalitetit të tij, dhe përgjegjësia për përcaktimin e shkallës së klasifikimit i takon krijuesit të tij, në përputhje me udhëzimet përkatëse të klasifikimit. Pikërisht për shkak të nevojës për udhëzime të tilla përkatëse, DSIK-ja filloi dhe udhëhoqi krijimin e këtij Udhëzuesi i cili synon të ofrojë udhëzime të qarta dhe praktike për përcaktimin, evidentimin dhe mbrojtjen e saktë të informacionit të klasifikuar, në përputhje me standardet evropiane dhe rregulloret kombëtare. Objektivat praktike të këtij Udhëzuesi janë:

- të mundësohet një vlerësim sistematik dhe objektiv i nivelit të mbrojtjes që duhet të zbatohet për informacionet me karakter të ndjeshëm,
- të përcaktojë kriteret të qarta për vendimmarrjen gjatë përcaktimit të shkallës së klasifikimit,
- të sigurojë zbatimin e masave të duhura për mbrojtjen e informacionit të klasifikuar.

Zbatimi i standardeve të përfshira në këtë udhëzues siguron një qasje të unifikuar ndaj mbrojtjes dhe minimizon rrezikun e trajtimit jo të duhur të informacionit të klasifikuar.

2. KRIJUESI DHE PËRPUNUESI I INFORMACIONIT TË KLASIFIKUAR

2.1. Krijuesi i informacionit të klasifikuar

Krijuesi i informacionit të klasifikuar është përpunues i autorizuar i informacionit të klasifikuar.

Krijuesit e informacionit të klasifikuar mund të jenë organet e qeverisjes shtetërore dhe lokale të krijuara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe ligjin, personat juridikë të themeluar nga Republika ose komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit dhe personat e tjerë fizikë ose juridikë, të cilët krijojnë informacion me rëndësi për sigurinë publike, mbrojtjen, punët e jashtme dhe aktivitetet e sigurisë dhe inteligjencës së shtetit.

Për informacion të klasifikuar me gradën “SEKRET SHTETËROR”, LIK rendit me saktësi krijuesit, të cilët mund të jenë: Presidenti i Republikës së Maqedonisë së Veriut, Kryetari i Kuvendit të Republikës së Maqedonisë së Veriut, Kryetari i Qeverisë së Republikës së Maqedonisë së Veriut, Kryetari i Gjykatës Kushtetuese të Republikës së Maqedonisë së Veriut, Kryetari i Gjykatës Supreme të Republikës së Maqedonisë së Veriut, Ministrat brenda departamenteve të tyre, Prokurori Publik i Republikës së Maqedonisë së Veriut, Shefi i Shtabit të Përgjithshëm të Ushtrisë së Republikës së Maqedonisë së Veriut, Drejtori i Agjencisë së Inteligjencës, Drejtori i Agjencisë së Sigurisë Kombëtare, Drejtori i Agjencisë Operacionale dhe Teknike, Drejtori i Qendrës për Menaxhim të Krizave, Drejtori i Drejtorisë për Sigurinë e Informacionit të Klasifikuar, si dhe personat e autorizuar nga subjektet e mësipërme. Nëse përcaktohet kështu me ligj, me marrëveshje ndërkombëtare të ratifikuar ose me rregullore tjetër, informacioni i klasifikuar me shkallën e “SEKRETIT SHTETËROR” përcaktohet edhe nga personat e parashikuar në ato akte.



Krijuesi i informacionit ose personi që ai ka autorizuar me shkrim përcakton shkallën e klasifikimit të informacionit. Krijuesi, brenda kuadrit të detyrave dhe autorizimeve të punës së tij, gjeneron informacion, përmbajtja e të cilit mund të shkaktojë dëm për interesat shtetërore ose zyrtare nëse bëhet publikim i paautorizuar. Krijuesi e di thelbin, kontekstin dhe ndjeshmërinë e informacionit dhe për këtë arsye ka detyrimin të propozojë një shkallë të përshtatshme klasifikimi gjatë formimit të tij. Prandaj, krijuesi duhet të ketë arsim adekuat dhe njohuri të hollësishme të legjislacionit dhe akteve nënligjore për sigurinë e informacionit të klasifikuar. Përveç kësaj, është e nevojshme të marrë pjesë vazhdimisht në trajnime të specializuara dhe të ketë përvojë praktike në trajtimin dhe mbrojtjen e informacioneve të klasifikuara.

Krijuesi duhet të jetë në gjendje të identifikojë dëmin e mundshëm të sigurisë, interesave politike, ekonomike ose ndërkombëtare të Republikës së Maqedonisë së Veriut nëse ka zbulim të paautorizuar të informacionit dhe mbi atë bazë të përcaktojë shkallën e përshtatshme të klasifikimit. Pra, krijuesi, përkatësisht personi i autorizuar prej tij, duhet ta shënojë informacionin e klasifikuar me nivelin më të përshtatshëm të klasifikimit, me të cilin sigurohet mbrojtja e nevojshme e interesave shtetërore dhe e sigurisë.

Në rastet kur informacioni nuk është shënuar me nivel klasifikimi, dhe krijuesi nuk mund të përcaktohet ose ka pushuar së ekzistuari, klasifikimin e kryen pasardhësi juridik i krijuesit. Nëse nuk mund të përcaktohet as pasardhësi juridik, atëherë shënimin e bën DSIK-ja.

Krijuesi i informacioneve të klasifikuara mban përgjegjësinë primare institucionale dhe ligjore për përcaktimin, shënimin dhe ndryshimin e saktë të nivelit të klasifikimit. Krijuesi ka rolin përfundimtar dhe vendimtar në procesin e klasifikimit dhe siguron respektimin e LIK, akteve nënligjore dhe procedurave të brendshme të institucionit.

Tabela 1 Detyrat e krijuesit të informacionit të klasifikuar

Detyrë	Përshkrim
Përcaktimi i shkallës së klasifikimit	Krijuesi, në bazë të propozimit nga hartuesi dhe vlerësimit të bërë të përmbajtjes dhe pasojave të mundshme, përcakton nivelin përkatës të klasifikimit. Gjatë kësaj, duhet të respektojë parimin e proporcionalitetit - të mos zbatohet një nivel më i lartë se sa është i nevojshëm, por as të mos lihet pa klasifikim kur kjo është e domosdoshme për mbrojtjen e interesave kombëtare.
Shënimi i informacionit të klasifikuar	Krijuesi është i detyruar që çdo informacion ta shënojë me nivelin e tij të përcaktuar të klasifikimit dhe të sigurojë që shenjat të jenë qartë të dukshme, të sakta dhe në përputhje me formatet dhe standardet e përcaktuara, duke parandaluar kështu përdorimin e paautorizuar ose trajtimin e gabuar të informacionit.
Klasifikimi i të dhënave individuale	Kur informacioni përmban të dhëna me ndjeshmëri të ndryshme, krijuesi duhet të përcaktojë nivel klasifikimi për çdo të dhënë ose pjesë individuale, me qëllim që të shmangët klasifikimi i tepruar i tërësisë.
Riklasifikimi	Krijuesi ka të drejtë dhe detyrë ta ndryshojë nivelin e klasifikimit nëse ndryshojnë rrethanat, niveli i rrezikut ose ndjeshmëria e informacionit. Ky ndryshim duhet të shpjegohet, të dokumentohet dhe të zbatohet në kohën e duhur.
Deklasifikimi	Krijuesi është përgjegjës për zbatimin e procesit të deklasifikimit, përkatësisht për të përcaktuar se informacioni nuk kërkon më status të klasifikuar dhe se mund të bëhet i disponueshëm si informacion i paklasifikuar. Deklasifikimi kryhet në bazë të vlerësimit të rreziqeve dhe afatit ligjor.
Përcaktimi i periudhës së vlefshmërisë së shkallës së klasifikimit të informacionit	Krijuesi specifikon një afat kohor ose një ngjarje specifike pas së cilës informacioni mund të riklasifikohet ose deklasifikohet. Kështu sigurohet një sistem dinamik i mbrojtjes që përshtatet me ndryshimin e kushteve të sigurisë dhe rëndësinë e informacionit.

2.2. Përpunuesi i informacionit të klasifikuar

Përpunuesi i informacionit të klasifikuar është një nëpunës i cili, në bazë të analizës së përmbajtjes së informacionit, jep edhe propozim me shkrim për përcaktimin e shkallës së përshatshme të klasifikimit, duke marrë parasysh kriteret ligjore, rreziqet dhe masën e dëmit që mund të rezultojë nga zbulimi i tij. Propozimi për klasifikimin e informacionit me një shkallë të caktuar përmban elementët e mëposhtëm:

- emrin e njësisë organizative dhe organit që propozon shkallën e klasifikimit,
- titulli dhe përshkrimi i shkurtër i informacionit për të cilin propozohet shkalla e klasifikimit,
- shkallën e klasifikimit të propozuar,
- arsyetimin për dëmin që do të rezultonte nga zbulimi i paautorizuar i informacionit,
- emri dhe mbiemri i personit që ka përgatitur propozimin dhe
- emri dhe mbiemri i personit që ka miratuar propozimin.

Edhe pse përpunuesi jep një vlerësim profesional dhe të bazuar në ekspertizë, vendimi përfundimtar për përcaktimin e shkallës së klasifikimit merret nga krijuesi i informacionit, pra personi që menaxhon organin ose një person i autorizuar prej tij me vetë nënshkrimin e propozimit dhe dokumentit që është klasifikuar. Krijuesi përcakton shkallën përfundimtare të klasifikimit, duke marrë parasysh parimin e proporcionalitetit, klasifikimin minimal të kërkuar dhe mbrojtjen e sigurisë kombëtare dhe interesave shtetërore. Propozimi për klasifikimin e informacionit mbahet së bashku me informacionin që klasifikohet. Në organet ku zbatohet një sistem për përpunimin automatik të informacionit të klasifikuar, propozimi për përcaktimin e shkallës së përshatshme të klasifikimit të informacionit jepet në mënyrë elektronike.

Me këtë sigurohet një proces i pajtueshëm, i përgjegjshëm dhe i kontrolluar në mënyrë hierarkike i klasifikimit të informacionit, me qëllim parandalimin e mbrojtjes së tepërt ose të pamjaftueshme dhe garantimin e trajtimit të sigurt dhe efikas të informacionit të klasifikuar.

Përpunuesi i informacionit të klasifikuar ka një rol thelbësor në sigurimin e një procesi ligjor, të qëndrueshëm, të saktë dhe objektiv të klasifikimit. Përpunuesi është subjekti i parë që analizon përmbajtjen e informacionit dhe bën një propozim me bazë profesionale për shkallën e klasifikimit të tij. Puna e përpunuesit është baza për marrjen e vendimit përfundimtar nga krijuesi i informacionit.

Tabela 2 Detyrat e përpunuesit të informacionit të klasifikuar

Detyrë	Përshkrim
Analiza e përmbajtjes së informacionit	Vlerësimi i hollësishëm i substancës, kontekstit dhe ndjeshmërisë së informacionit për të përcaktuar nëse zbulimi i tij mund të shkaktojë dëme në sigurinë kombëtare, interesin publik, marrëdhëniet e jashtme ose vlerat e tjera të mbrojtura.
Përgatitja e një propozimi për një diplomë klasifikimi	Përgatitja e një propozimi me shkrim që përmban të gjithë elementët e detyrueshëm: përshkrimin e informacionit, shkallën e propozuar të klasifikimit, shpjegimin e dëmit të mundshëm (duke siguruar një bazë të qartë dhe të arsyetuar për shkallën e propozuar të klasifikimit) dhe të dhënat për përpunuesin dhe miratuesin.
Zbatimi i parimit të proporcionalitetit	Vlerësimi i nevojës reale për klasifikim dhe shmangia e tepruar (niveli tepër i lartë i mbrojtjes) ose i pamjaftueshëm (niveli tepër i ulët i mbrojtjes), në mënyrë që të përdoren burimet në mënyrë racionale dhe të inkurajohet transparencja.
Bashkëpunimi me krijuesin	Koordinimi gjatë marrjes së vendimit përfundimtar, harmonizimi i masave të sigurisë dhe sigurimi i të dhënave të sakta të dokumenteve të klasifikuara.
Respektimi i procedurave të mbrojtjes së informacionit	Sigurimi i konfidencialitetit, integritetit dhe disponueshmërisë së kontrolluar të informacionit gjatë përgatitjes së tij, madje edhe para klasifikimit të tij zyrtar.



2.3. Diferencimi i roleve midis krijuesit dhe përpunuesit

Megjithëse krijuesi dhe përpunuesi i informacionit të klasifikuar punojnë ngushtë së bashku në procesin e përcaktimit të shkallës së klasifikimit, rolet dhe përgjegjësitë e tyre janë thelbësisht të ndryshme.

Përpunuesi është përgjegjës për përgatitjen dhe vlerësimin me ekspertizë të përmbajtjes së informacionit dhe për përgatitjen e një propozimi për një shkallë të përshtatshme klasifikimi, bazuar në analizën e dëmeve të mundshme, rreziqeve dhe kritereve ligjore. Përpunuesi ka një rol analitik-përgatitës, të fokusuar në përmbajtjen dhe vlerësimin e rrezikut.

Nga ana tjetër, krijuesika një përgjegjësi vendimtare dhe ligjore – ai kontrollon propozimin e përpunuesit dhe merr vendimin përfundimtar për klasifikimin, duke respektuar kushtet dhe kriteret e parashikuara ligjore. Kështu, krijuesi ka një funksion kontrolli mbi procesin e klasifikimit të informacionit.

Tabela 3 Krahassimi i roleve të përpunuesit dhe krijuesit

Organi përgjegjës	Faza e procesit	Përshkrimi i aktivitetit / rolit
Përpunuesi	Përgatitja e dokumentit	Përgatit përmbajtjen e dokumentit të informacionit të klasifikuar.
	Analiza e përmbajtjes dhe vlerësimi i dëmeve dhe pasojave të mundshme	Kryen analiza ekspertësh për përmbajtjen e informacionit (integriteti, natyra dhe vlera) dhe vlerësimin e dëmeve dhe pasojave të mundshme (ndjeshmëria, kërcënimi, rreziku).
	Përgatitja e një propozimi për një diplomë klasifikimi	Propozon shkallën e përshtatshme të klasifikimit, bazuar në analizën dhe vlerësimin e kritereve ligjore.
Krijuesi	Shqyrtimi dhe vlerësimi i propozimit	Shqyrton propozimin e përpunuesit, vlerëson justifikimin dhe pajtueshmërinë e tij me procedurat.
	Vendimi përfundimtar për shkallën e klasifikimit	Konfirmon/verifikon shkallën e klasifikimit.

2.4. Përgjegjësia e përpunuesit dhe krijuesit të informacionit të klasifikuar

Krijuesi dhe përpunuesi i informacionit të klasifikuar mbajnë përgjegjësi disiplinore, kundërvajtëse dhe penale nëse nuk veprojnë në përputhje me dispozitat ligjore. Për ta, si dhe për të gjithë personat e tjerë që janë punonjës të institucionit dhe që janë përdorues të informacionit të klasifikuar, parashikohen masa të përshtatshme disiplinore, kundërvajtje dhe sanksione penale në rastet e shkeljes së rregullave për klasifikimin dhe trajtimin e informacionit të klasifikuar:

- **Përgjegjësia disiplinore:** në rast të shkeljeve të detyrës zyrtare për të cilat mund të vendosen masa të përshtatshme disiplinore, në përputhje me rregulloret ligjore dhe aktet e brendshme të institucionit.
- **Përgjegjësia për kundërvajtje:** për krijimin dhe monitorimin e procedurave ligjore në përcaktimin e shkallës së klasifikimit, përkatësisht nëse informacioni klasifikohet pa një vlerësim të nevojshëm të dëmit dhe pasojave të mundshme, si dhe nëse detyrimi për të njoftuar përdoruesit e informacionit të klasifikuar në kohën e duhur për një ndryshim në shkallën e klasifikimit ose deklasifikimit të tij nuk përmbushet.
- **Përgjegjësia penale:** si dhe çdo person tjetër me qasje në informacionin e klasifikuar – nëse ata marrin ose japin me qira informacion të klasifikuar në mënyrë të paautorizuar.

Duke respektuar në mënyrë të vazhdueshme procedurat dhe detyrimet ligjore, krijuesi dhe përpunuesi sigurojnë që procesi i klasifikimit të jetë i ligjshëm, racional dhe në përputhje me parimet e transparencës, llogaridhënies dhe qeverisjes së mirë.

3. NOTAT E KLASIFIKIMIT TË INFORMACIONIT

Informacion me interes për Republikën e Maqedonisë së Veriut

Çdo informacion i përgatitur nga një autoritet i shtetit dhe pushtetit lokal i themeluar në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe me ligj, person juridik i themeluar nga Republika ose komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit, një person fizik ose juridik, si dhe një autoritet i huaj shtetëror, përkatësisht një person i huaj fizik ose juridik, në lidhje me sigurinë dhe mbrojtjen e shtetit, integritetin dhe sovranitetin e tij territorial, rendin kushtetues, interesin publik dhe liritë dhe të drejtat e njeriut dhe qytetarit.

Informacion i klasifikuar

Informacion nga fushëveprimi i punës së një organi të qeverisjes shtetërore dhe lokale të themeluar në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe me ligj, një person juridik i themeluar nga Republika ose nga komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit ose personat e tjerë juridikë në lidhje me sigurinë publike, mbrojtjen, punët e jashtme ose aktivitetet e sigurisë ose inteligjencës së shtetit të cilat, në përputhje me ligjin, duhet të mbrohen nga qasja e paautorizuar dhe të shënohen me një shkallë të përshatshme të klasifikimit në përputhje me këtë ligj. Informacioni i klasifikuar mund të përfaqësojë gjithashtu dokumente, mjetet e teknike, makina, pajisje, pracomponentët e veçantë; armë ose mjete që prodhohen ose janë në proces prodhimi, si dhe shpikje konfidenciale që lidhen me mbrojtjen dhe janë me interes për sigurinë e shtetit.

LIK-ja parashikon katër shkallë klasifikimi:

1. "SEKRET SHTETËROR"
2. "RREPTËSISHT KONFIDENCIALE"
3. "KONFIDENCIALE"
4. "INTERNE"

Со цел да се обезбеди конзистентно и усогласено ракување со класифицираните информации, степенот на класификација се утврдува врз основа на видот на интересите што се штитат и нивото на штета што би настанала доколку информацијата неовластено се открие. Следната табела ги прикажува дефинициите на степените на класификација поделени според видот на потенцијалната штета и категориите на интереси кои се предмет на заштита.



Tabela 4 Shkallët e klasifikimit të informacionit dhe kuptimi i tyre

Shkalla e klasifikimit	Pasojat nga zbulimi i paautorizuar	Lloji i interesave që mbrohen
SEKRET SHTETËROR	Rrezikimi dhe shkaktimi i dëmeve të pariparueshme	Interesat e qëndrueshme të Republikës së Maqedonisë së Veriut
RREPTËSISHT KONFIDENCIALE	Dëm jashtëzakonisht serioz	Interesat jetike të Republikës së Maqedonisë së Veriut
KONFIDENCIALE	Dëm serioz	Interesat e rëndësishme të Republikës së Maqedonisë së Veriut
INTERNE	Dëmi	Puna e organeve të qeverisjes shtetërore dhe lokale të krijuara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe me ligj, personat juridikë të themeluar nga Republika ose nga komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit, të cilat janë të rëndësishme për sigurinë publike, mbrojtjen, punët e jashtme dhe aktivitetet e sigurisë dhe inteligjencës së shtetit

Përveç gradave të listuara, ekziston një etiketë informacioni shtesë, e cila është **“për PËRDORIM TË KUFIZUAR”**.

Ky shënim nuk paraqet një shkallë klasifikimi, por shërben për të mbrojtur informacionin, disponueshmëria e paautorizuar e të cilit mund të zvogëlojë efikasitetin e funksionimit të organeve të qeverisjes shtetërore dhe lokale të krijuara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe ligjin, personat juridikë të themeluar nga Republika ose nga komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit.

Ky informacion:

- nuk janë lirisht të disponueshme, dhe
- mbrohen me masa përkatëse, të përcaktuara me akt nënligjor të Qeverisë, që është Rregullore për sigurinë administrative të informacioneve të klasifikuara dhe informacioneve me përdorim të kufizuar.

Nëse klasifikimi i informacionit ka për qëllim të fshehë tejkalimin e autorizimit, shpërdorimin e detyrës ose veprime të tjera të paligjshme ose ndëshkuese, ai informacion nuk do të konsiderohet i klasifikuar. Personat që i raportojnë këto informacione pranë një autoriteti kompetent, në përputhje me Ligjin për mbrojtjen e sinjalizuesve, gëzojnë mbrojtje ligjore.

Përcaktimi i shkallës së klasifikimit të informacionit, në fakt, përcakton mbrojtjen e duhur të përbërë nga një sërë aktivitetesh dhe masash për të parandaluar aksesin e paautorizuar dhe trajtimin e paautorizuar.

Tabela e mëposhtme ofron një pasqyrë krahasuese të masave të sigurisë të zbatuara gjatë trajtimit, ruajtjes, transferimit dhe mbrojtjes së informacionit të klasifikuar dhe informacionit të shënuar “Përpërdorim të kufizuar”. Ajo lejon një përcaktim të qartë të detyrimeve dhe procedurave në varësi të shkallës së klasifikimit dhe nivelit të rrezikut që rrjedh nga zbulimi i paautorizuar i informacionit.

Tabela përdoret si një udhëzues gjatë planifikimit dhe zbatimit të masave të sigurisë nga institucionet dhe personat përgjegjës, në mënyrë që të sigurohet zbatimi i duhur i ligjeve dhe akteve nënligjore. Përdoruesit mund të përcaktojnë lehtësisht përmes saj se cilat masa janë të detyrueshme, cilat janë të rekomanduara dhe në cilat raste nevojitet forcim i mëtejshëm i mbrojtjes, në përputhje me kontekstin specifik dhe vlerësimin e rrezikut.

Tabela 5 Masat paraprake të sigurisë të zbatueshme për informacionin e klasifikuar dhe për etiketën "Për përdorim të kufizuar"

	PËR PËRDORIM TË KUFIZUAR			INTERNE	KONFIDENCIALE	RREPTËSISHT KONFIDENCIALE	SEKRET SHITETËROR
Parimi "Duhet të dijë"	po		po	po	po	po	po
Kontrolli i sigurisë	jo		jo	jo	po	po	po
Përmbledhje e personave që i janë qasur informacionit	jo		jo	jo	jo	po	po
Shpërndarja	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim	personat juridikë dhe fizikë të cilët janë të njohur me masat dhe aktivitetet për mbrojtjen e këtij informacioni dhe kanë nënshkruar një deklaratë për këtë qëllim
Riprodhim, kopje, përkthime, ekstrakte	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"	bëhet nga përdoruesi me zbatimin e rreptë të parimit "duhet të dijë"
Trajtimi dhe ruajtja	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë	në zonat administrative dhe të sigurisë të shkallës së parë dhe të dytë
Trajtimi dhe ruajtja e SKI	i pa akredituar (në zyrtare-zyrtare SKI)	i akredituar	i akredituar	i akredituar	i akredituar	i akredituar	i akredituar
Masa TEMPEST	jo	jo	po	po	po	po	po
Dorëzim fizik	të paketuara në një zarf jo-transparent	të paketuara në dy zarfe	të paketuara në dy zarfe	të paketuara në dy zarfe	të paketuara në dy zarfe	të paketuara në dy zarfe	të paketuara në dy zarfe
Transportimi me mjete elektronike	po	po, me mbrojtje të për-shtatshme kriptografike	po, me mbrojtje të për-shtatshme kriptografike	po, me mbrojtje të për-shtatshme kriptografike	po, me mbrojtje të për-shtatshme kriptografike	po, me mbrojtje të për-shtatshme kriptografike	po, me mbrojtje të për-shtatshme kriptografike
Shkatërrimi	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij	sipas listës së materialit dokumentar me afate për ruajtjen e tij



4. PROCESI I PËRCAKTIMIT TË NIVELIT TË KLASIFIKIMIT

4.1. Identifikimi i informacionit

Identifikimi i informacionit është hapi i parë dhe kryesor në procesin e klasifikimit të informacionit. Ai përfshin përcaktimin e llojit, karakterit dhe bartësit të informacionit, si dhe një vlerësim paraprak të ndjeshmërisë dhe rëndësisë së tij për sigurinë kombëtare ose organizative. Identifikimi i saktë mundëson përcaktimin e duhur të shkallës së klasifikimit, përzgjedhjen e masave të duhura të mbrojtjes dhe vendosjen e kontrolleve për qasjen dhe trajtimin e informacionit.

Në kuadër të procesit të identifikimit të informacionit, kryhen aktivitetet e mëposhtme:

- identifikohet lloji dhe përmbajtja e informacionit (dokument, e-mail, audio, video, baza të të dhënave, etj.),
- përcaktohet funksioni i informacionit – nëse është strategjik, operativ, administrativ ose i ndonjë lloji tjetër,
- vlerësohet se kush e përdor dhe kush duhet të ketë qasje (departamente, zyrtarë, bashkëpunëtorë).

Informacionet e klasifikuara lidhen veçanërisht me fushat e mëposhtme:

- sigurinë publike,
- mbrojtjen,
- punë të jashtme,
- aktivitetet e sigurisë, inteligjencës dhe kundërzbulimit të shtetit,
- infrastruktura kritike, sistemet, pajisjet, shpikjet, projektet dhe planet me rëndësi për shtetin,
- të dhëna shkencore, teknologjike, ekonomike dhe financiare me interes kombëtar.

Me identifikim të saktë sigurohet një qasje e unifikuar në trajtimin e informacionit dhe minimizohet rreziku i klasifikimit të pasaktë ose i trajtimit të paautorizuar.

4.2. Parimet gjatë përcaktimit të nivelit të klasifikimit

Gjatë përcaktimit të nivelit të klasifikimit të informacionit duhet të merren parasysh parimet e mëposhtme:

Parimi i dëmit

Vlerësohet se çfarë dëmi do të ndodhte nëse informacioni zbulohet, modifikohej ose keqpërdorej në mënyrë të paautorizuar. Niveli i klasifikimit lidhet drejtpërdrejt me seriozitetin dhe shtrirjen e pasojave të mundshme ndaj interesave shtetërore, institucionale ose publike.

Parimi i proporcionalitetit

Niveli i klasifikimit duhet të jetë në përpjesëtim me nivelin e dëmit që mund të shkaktohet nga zbulimi i paautorizuar i informacionit. Klasifikimi i tepruar i informacionit me dëme të ulëta, si dhe mbrojtja e pamjaftueshme e informacionit të ndjeshëm, përbëjnë shkelje të këtij parimi

Parimi i domosdoshmërisë në klasifikim

Klasifikimi i informacionit kryhet vetëm kur është vërtet i nevojshëm për mbrojtjen e interesave shtetërore ose institucionale. Nëse objektivat e mbrojtjes mund të arrihen pa klasifikim, vetëm duke kufizuar disponueshmërinë ose duke shënuar informacionin me emërtimin “për përdorim të kufizuar”, klasifikimi nuk duhet të zbatohet.

Parimi kohor

Klasifikimi merr parasysh periudhën kohore në të cilën informacioni është i ndjeshëm dhe kërkon mbrojtje. Shkalla e klasifikimit nuk është e përhershme si rregull dhe duhet të rishqyrtohet, me mundësinë e zvogëlimit ose shfuqizimit kur pushojnë arsyet e mbrojtjes.

Parimi i përgjegjësisë

Klasifikimi i informacionit kryhet ekskluzivisht nga një person i autorizuar, përkatësisht krijuesi, brenda kompetencave të tij ligjore. Ai person mban përgjegjësi të plotë për ligjshmërinë, justifikimin dhe zbatimin e duhur të shkallës së përcaktuar të klasifikimit.

4.3. Kriteret për përcaktimin e shkallës së klasifikimit

Klasifikimi i informacionit është një proces që përcakton shkallën e mbrojtjes që duhet t'i jepet një informacioni, në varësi të dëmit që mund të ndodhë për shtetin nëse zbulohet, modifikohet, shkatërrohet ose përdoret pa leje.

Gjatë përcaktimit të shkallës në të cilën do të klasifikohet një informacion, vlerësohen treguesit që tregojnë llojin dhe ashpërsinë e dëmit të mundshëm që mund të ndodhë nëse informacioni zbulohet ose përdoret pa autorizim. Bazuar në një vlerësim të tillë, përcaktohet nëse informacioni do të shënohet si “SEKRET SHTETËROR”, “RREPTËSISHT KONFIDENCIAL”, “KONFIDENCIAL” ose “i BRENDSHËM”, pra me një shkallë që është e përshtatshme për rrezikun dhe interesat që mbrohen.

Përcaktimi i shkallës së përshtatshme të klasifikimit të informacionit bëhet në bazë të kriterëve të specifikuar më poshtë nga LIK, të cilat janë thelbësore për mbrojtjen e duhur të interesave dhe sigurisë shtetërore:

1. përmbajtja e informacionit, dhe

2. vlerësimi i dëmeve dhe pasojave të mundshme që mund të rezultojnë nga qasja e paautorizuar ose përdorimi i paautorizuar i informacionit mbi interesat dhe sigurinë shtetërore.

Përcaktimi i klasifikimit bazohet në një kombinim të përmbajtjes së informacionit dhe vlerësimit të dëmit të mundshëm. Kjo do të thotë se jo të gjitha informacionet e ndjeshme konsiderohen automatikisht “sekrete” – ato gjithashtu duhet të jenë potencialisht të dëmshme për shtetin nëse zbulohen. Sa më e ndjeshme ose kritike të jetë përmbajtja e informacionit në lidhje me funksionimin dhe interesat e shtetit dhe sa më i madh të jetë dëmi i mundshëm ndaj interesave dhe sigurisë shtetërore, aq më e lartë duhet të jetë shkalla e klasifikimit.



Tabela 6 Kriteret për përcaktimin e shkallës së klasifikimit të informacionit

Kriteri	Përshkrim	Elementet	Pyetje për vlerësimin e kontrollit
Përmbajtja e informacionit	Mbulon saktësinë, rëndësinë dhe ndikimin e mundshëm të përmbajtjes së informacionit. Vlerësohet nëse të dhënat janë të besueshme, nëse lidhen me funksione ose interesa kritike dhe sa mund të ndikojë zbulimi i tyre mbi institucionet shtetërore ose sigurinë kombëtare.	Integritet	A është informacioni i saktë dhe i verifikuar?
		Natyra	Çfarë të dhëna përmban informacioni?
		Vlera	Sa i dobishëm dhe i rëndësishëm është informacioni?
Vlerësimi i dëmeve dhe pasojave të mundshme	Vlerësimi përfshin ndjeshmërinë e përmbajtjes, gjegjësisht shkallën e rëndësisë së saj dhe dëmin e mundshëm nga zbulimi i paautorizuar; kërcënimet e mundshme që vijnë nga aktorë, ngjarje ose rrethana që mund të shfrytëzojnë qëllimisht ose aksidentalisht një cenueshmëri ekzistuese; si dhe rrezikun e shprehur përmes gjasave të ndodhjes së një incidenti dhe intensitetit të pasojave që mund të lindin për institucionin ose interesat shtetërore.	Ndjeshmëria	Cili do të ishte reagimi nëse informacioni do të bëhej publik?
		Kërcënim	Çfarë ngjarje mund ta shfrytëzojë cenueshmërinë ekzistuese dhe të shkaktojë dëm ndaj informacionit ose institucionit?
		Rrezik	Sa ka gjasa që informacioni të komprometohet dhe çfarë dëmi do t'i shkaktonte interesave shtetërore?

4.3.1. Përmbajtja e informacionit

Përmbajtja e informacionit si kriter i referohet integritetit, natyrës dhe vlerës së informacionit.

Integriteti i informacionit

Integriteti i informacionit është shkalla në të cilën përmbajtja është e saktë, e plotë dhe e pandryshuar nga persona të paautorizuar. Gjatë përcaktimit të shkallës së klasifikimit, është e nevojshme të vlerësohet me kujdes nëse informacioni bazohet në të dhëna të verifikuara dhe të besueshme, nëse bazohet në një burim të besueshëm dhe nëse nuk ka rrezik manipulimi, falsifikimi ose keqinterpretimi.

Informacioni me integritet të lartë ka një ndikim të rëndësishëm në vendimmarrje, politikëbërje dhe mbrojtjen e interesave kombëtare. Prandaj, nëse zbulohet se përmbajtja është e saktë dhe e besueshme, mund të kërkojë një shkallë më të lartë të mbrojtjes. Megjithatë, nëse ka dyshime në lidhje me saktësinë, origjinën ose besueshmërinë e informacionit, për shembull, kur të dhënat janë të pakonfirmuara, të paplota ose potencialisht të ndryshuara, rreziku i vendimeve të pasakta rritet dhe nevoja për klasifikim të lartë zvogëlohet.

Natyra e informacionit

Natyra e informacionit i referohet përmbajtjes thelbësore – nëse informacioni përfshin të dhëna operationale, informacione personale, plane strategjike, specifitime teknike, ose ndonjë lloj të dhënash të ndjeshme shtetërore ose institucionale. Gjatë vlerësimit të informacionit, analizohet se çfarë përmban saktësisht dhe cilës nga fushat e përmendura më parë i referohet: mbrojtja dhe siguria e shtetit, politika e jashtme dhe marrëdhëniet ndërkombëtare, aktivitetet e inteligjencës ose kundërzbulimit, infrastruktura kritike ose interesat ekonomike dhe teknologjike me rëndësi strategjike.

Sa më kritike të jetë fusha që ka të bëjë me të, aq më shumë ka të ngjarë që informacioni të klasifikohet në një shkallë më të lartë.

Vlera e informacionit

Vlera e informacionit i referohet shkallës së dobisë, veçantisë dhe rëndësisë strategjike të tij, domethënë potencialit që ai sjell për të mbështetur vendimmarrjen, për të mundësuar veprimin ose për të ndikuar në proceset kombëtare, institucionale, politike, ekonomike ose të sigurisë. Sa më e lartë të jetë përmbajtja dhe pesha e saj operacionale, aq më e lartë është nevoja për trajtimin e saj të mbrojtur dhe të kontrolluar.

Gjatë vlerësimit të vlerës, analizohet jo vetëm cilësia e vetë të dhënave (saktësia, detajet, ekskluziviteti), por edhe aftësia e saj për të prodhuar pasoja - pozitive ose negative - nëse përdoret nga subjektet e tjera.

Informacioni me përmbajtje të ulët ose vlerë strategjike nuk kërkon një shkallë të lartë mbrojtje, ndërsa informacioni me peshë të lartë analitike, rëndësi operacionale ose ndikim në proceset kritike konsiderohet si përparësi për klasifikim.

4.3.2. Vlerësimi i dëmeve dhe pasojave të mundshme

Vlerësimi i dëmeve dhe pasojave të mundshme që mund të rezultojnë nga qasja e paautorizuar ose përdorimi i paautorizuar i informacionit mbi interesat dhe sigurinë shtetërore si kriter i referohet pasojave të mundshme negative që mund të lindin nëse informacioni zbulohet, keqpërdoret ose publikohet pa autorizim.

Vlerësimi mund të detajohet përmes **ndjeshmërisë, kërcënimit** dhe analizës së **rrezikut** të informacionit.

Ndjeshmëria e informacionit

Ndjeshmëria e informacionit përcakton ashpërsinë e pasojave që do të ndodhnin nëse informacioni zbulohet, aksesohet ose përdoret nga persona të paautorizuar. Ky kriter vlerëson dëmtimin e mundshëm të sigurisë kombëtare, interesit publik ose funksionimit të institucioneve.

Sa më i madh të jetë dëmi i mundshëm, aq më e lartë është shkalla e ndjeshmërisë dhe nevoja për klasifikim.

Vlerësimi i ndjeshmërisë duhet të bazohet gjithmonë në:

- incidente specifike dhe gjasat e ndodhjes së tyre,
- ndikimin në interesat shtetërore,
- ndjeshmërinë kohore (nëse rreziku zvogëlohet me kalimin e kohës).

Krijuesi i informacionit duhet të shqyrtojë me kujdes dhe të parashikojë reagimin dhe interpretimin e mundshëm nëse informacioni do të bëhej publik, si dhe pasojat e menjëhershme, afatmesme dhe afatgjata të mosmbrojtjes së tij.

Kërcënim për informacionin

Gjatë përcaktimit të shkallës së përshtatshme të klasifikimit, është gjithashtu e nevojshme të vlerësohet natyra e kërcënimit ndaj informacionit. Kërcënim është çdo veprim ose ngjarje e mundshme që mund të shfrytëzojë një cenueshmëri të veçantë dhe të shkaktojë dëm për një



institucion, proceset e tij ose interesat kombëtare.

Kjo do të thotë se kërcënimet nuk ekzistojnë të izoluar - ato bëhen një rrezik real vetëm kur kryqëzohen me dobësitë ekzistuese në sistem. Vulnerabilitetet janë dobësi në infrastrukturën që mbrohet: mospërputhje në dizajnin e sistemit, mangësi në zbatimin e masave të sigurisë, të meta teknike ose boshllëqe në proceset operative që mund të keqpërdoren nga subjekte të paautorizuara.

Në këtë kontekst, vlerësimi i kërcënimit përfshin:

- llojin e sulmuesit të mundshëm ose burimin e kërcënimit (aktorë të jashtëm, të brendshëm, incidente teknike, fenomene natyrore);
- mundësinë e kërcënimit dhe motivimin ose aftësinë e tij të mundshme për të shkaktuar dëm;
- mënyrën në të cilën kërcënimi mund të shfrytëzojë cenueshmërinë specifike, përkatësisht nëse dobësitë ekzistuese lejojnë hyrjen, manipulimin ose zbulimin e informacionit;
- fushëveprimin dhe ashpërsinë e dëmit, nëse kërcënimi realizohet dhe informacioni komprometohet.

Rrezik për informacionin

Rreziku për informacionin është një kombinim i gjasave që një ngjarje të ndodhë duke çuar në një shkelje të konfidencialitetit, integritetit ose disponueshmërisë së informacionit dhe ashpërsisë së pasojave nëse ndodh një ngjarje e tillë. Ai rezulton nga bashkimi i dy elementeve:

1. probabiliteti që një kërcënim i veçantë do të realizohet dhe
2. ndikimi - përkatësisht, shkalla e dëmit që do të ndodhte nëse kërcënimi realizohet dhe informacioni komprometohet.

Vlerësimi i rrezikut duhet të mbulojë aspektet e mëposhtme:

- Probabiliteti: sa ka gjasa që informacioni të zbulohet, ndryshohet ose shkatërrohet nga një person i paautorizuar;
- Ndikimi: cilat do të ishin pasojat mbi interesat shtetërore nëse komprometohen;
- Fazat më kritike të ciklit jetësor të informacionit (krijimi, ruajtja, transferimi, përdorimi, shkatërrimi).

Vlerësimi i duhur i rrezikut është thelbësor për përcaktimin e shkallës së përshtatshme të klasifikimit, identifikimin e masave të nevojshme të sigurisë dhe zvogëlimin e pasojave të mundshme nëse ndodh një incident i veçantë.

4.4. Arsyetimi ekonomik për klasifikimin e informacionit

Gjatë përcaktimit të shkallës së përshtatshme të klasifikimit, është e nevojshme të merret parasysh justifikimi ekonomik për mbrojtjen e informacionit. Ky aspekt ka të bëjë me atë nëse burimet që duhet të investohen për mbrojtjen e saj - mjete financiare, kapacitete njerëzore, infrastrukturë teknike dhe procedura administrative - janë në përpjesëtim me vlerën dhe ndjeshmërinë e vetë informacionit.

Jo të gjitha informacionet janë njësoj të rëndësishme, kështu që nuk është gjithmonë racionale të investohet në masa të shtrenjta sigurie. Qëllimi është të arrihet një ekuilibër optimal midis:



vlerës, rëndësisë dhe ndjeshmërisë së informacionit dhe shkallës dhe llojit të mbrojtjes që zbatohet.

Në vlerësimin e justifikimit ekonomik shqyrtohen çështjet e mëposhtme:

- A është kostoja e mbrojtjes së informacionit në përpjesëtim me dëmin e mundshëm nëse informacioni komprometohet?
- A ka alternativa më efikase dhe me kosto efektive që lejojnë një shkallë mjaft të lartë sigurie?

Vlerësimi i justifikimit ekonomik mundëson menaxhimin racional të burimeve të institucioneve dhe parandalon mbrojtjen e tepruar të informacionit me vlerë të ulët dhe mbrojtjen e pamjaftueshme të informacionit kritik. Në këtë mënyrë, kontribuohet në një qasje të balancuar, pa krijuar barrë të panevojshme administrative dhe financiare.

Me vlerësimin e kujdesshëm të justifikimit ekonomik, institucionet sigurojnë një përcaktim efikas, racional dhe të harmonizuar ligjërish të shkallës së klasifikimit të informacionit, ku burimet përdoren me përgjegjësi dhe interesat shtetërore mbrohen në mënyrë adekuate.

4.5. Përcaktimi i dëmeve dhe pasojave të mundshme

Tabela e mëposhtme tregon një pasqyrë sistematike të shkallëve të klasifikimit të informacionit në varësi të llojit dhe intensitetit të dëmit të mundshëm që mund të ndodhë në rast të zbulimit, përdorimit ose keqpërdorimit të tyre të paautorizuar. Tabela lidh natyrën e pasojave mbi interesat shtetërore, institucionale dhe publike me shkallën e përshtatshme të klasifikimit.

Gjatë përdorimit të tabelës, së pari përcaktohet lloji dhe intensiteti i pasojave ("nëse shkaktohet një dëm i tillë"), pastaj krahasohen me shembujt e dhënë nga RrSA, dhe në fund përcaktohet shkalla e përshtatshme e klasifikimit.

Në këtë mënyrë sigurohet proporcionaliteti midis ashpërsisë së pasojave dhe shkallës së mbrojtjes, lehtësohet zbatimi i qëndrueshëm i kriterëve ligjore dhe zvogëlohet rreziku i klasifikimit të tepërt ose të pamjaftueshëm të informacionit.



Tabela 7 Përcaktimi i nivelit të klasifikimit të informacionit dhe shënimit "Për përdorim të kufizuar" në varësi të dëmit të mundshëm dhe pasojave që do të mund të lindnin nga zbulimi i paautorizuar

Nëse zbulimi i paautorizuar i informacionit...	në çfarë?
do të zvogëlonte efikasitetin	në funksionimin e organeve të pushtetit shtetëror dhe lokal të themeluara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe me ligj, personave juridikë të themeluar nga Republika ose nga komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit
do të shkaktonte dëme	mbi punën e organeve
do të shkaktonte dëme serioze	për interesat e rëndësishme të Republikës së Maqedonisë së Veriut, të cilat janë parakushte për krijimin dhe realizimin e interesave të përhershme dhe jetike të Republikës së Maqedonisë së Veriut: - ndërtimi dhe zhvillimi i të gjitha formave të bashkëpunimit me fqinjët, dhe në interes të paqes, sigurisë dhe zhvillimit të Republikës së Maqedonisë së Veriut dhe fqinjëve të saj, - kontributin e vet në ruajtjen dhe promovimin e paqes dhe stabilitetit në Evropën Juglindore (EJL) me qëllim të forcimit të zonës së demokracisë, sigurisë dhe prosperitetit të të gjitha vendeve në rajon, - të marrë pjesë në ndërtimin e paqes dhe stabilitetit në rajon, Evropë dhe botë, si dhe në parandalimin dhe ndërtimin e instrumenteve për paralajmërim të hershëm të tensioneve dhe krizave, me qëllim zgjidhjen paqësore në kohë dhe në mënyrë efikase, - ruajtjen dhe përparimin e rendit ndërkombëtar të bazuar në drejtësi, respekt të ndërsjellë të rendit ndërkombëtar të themeluar në të drejtën ndërkombëtare, si dhe në barazinë politike dhe ekonomike të shteteve, - sigurimi i kushteve dhe promovimi i stabilitetit të brendshëm politik dhe mundësive për hir të një të drejte të barabartë për pjesëmarrje, e cila duhet të përfshijë gjithashtu një konsensus të pranuar përgjithësisht për çështje me interes të qëndrueshëm, jetësor dhe të rëndësishëm të vendit, - krijimin e kushteve për promovimin e kulturës së sigurisë, - ndërtimin e një shteti të drejtë dhe social me mundësi të barabarta për të gjithë qytetarët pavarësisht nga përkatësia e tyre gjinore, racore, fetare, politike, sociale, kulturore dhe të tjera, - krijimin e kushteve për ndërtimin e një shoqërie me komunikime dhe marrëdhënie që do të zhvillojnë vlera të përbashkëta dhe kulturë jetese, veçanërisht midis brezit të ri, në frymën e tolerancës, duke nxitur vlerat demokratike dhe respektin për integritetin personal, të bazuara në traditën demokratike evropiane, pavarësisht nga përkatësia etnike, fetare ose tjetër, dhe - ruajtjen dhe mbrojtjen e mjedisit jetësor në vend në bashkëpunim me mjedisin më të gjerë.
do të shkaktonte dëme jashtëzakonisht serioze	për interesat jetike të Republikës së Maqedonisë së Veriut që promovojnë situatën e sigurisë dhe krijojnë kushte për jetë më të mirë të qytetarëve dhe funksionimin e shtetit dhe shoqërisë: - mbrojtjen dhe promovimin e paqes dhe sigurisë, jetës, shëndetit, pronës dhe sigurisë personale të qytetarëve të Republikës së Maqedonisë së Veriut, - zhvillimin e një shoqërie multietnike të bazuar në besimin e ndërsjellë, përpjekjet e përbashkëta dhe synimin e të gjitha bashkësive etnike për stabilitet dhe përparim gjithëpërfshirës të shtetit, - zhvillim ekonomik të bazuar në parimet e ekonomisë së tregut, pronës private, përmirësimi i vazhdueshëm i standardit të jetesës dhe cilësisë së jetës, si dhe mbrojtja e infrastrukturës dhe burimeve jetësore të Republikës së Maqedonisë së Veriut, - mbrojtje dhe promovim të themeleve demokratike të sundimit të ligjit - pluralizmi politik, demokracia parlamentare, ndarja e pushteteve dhe zgjedhjet demokratike dhe të ndershme, sundimi i ligjit, respektimi i vazhdueshëm i të drejtave dhe lirive të njeriut, si dhe të drejtat dhe liritë e qytetarëve që u përkasin të gjitha komuniteteve dhe mbajtja dhe promovimi i vazhdueshëm i sigurisë së përgjithshme të brendshme të shoqërisë dhe shtetit, - integrim politik-mbrojtës në NATO, integrim politik, ekonomik dhe i sigurisë në Bashkimin Evropian, si dhe në sistemet e tjera të sigurisë kolektive.
do të shkaktonte rrezikim dhe dëme të pariparueshme	ndaj interesave të përhershme të Republikës së Maqedonisë së Veriut: - ruajtjen dhe promovimin e identitetit shtetëror duke shprehur lirisht identitetin etnik të të gjithë qytetarëve të Republikës së Maqedonisë së Veriut, dhe - mbrojtjen e pavarësisë dhe integritetit territorial.

- të ulë efikasitetin e punës ose të ndikojë në kushtet për përmirësimin dhe ruajtjen e stabilitetit të brendshëm politik, sigurisë dhe efikasitetit operativ të shtetit;

- të ulë efikasitetin e punës në ndërtimin e një shteti të drejtë dhe social me mundësi të barabarta për të gjithë qytetarët;

- të ulë efikasitetin e punës në negociatat politike, financiare, monetare, ekonomike dhe tregtare të shtetit;

- të ulë efikasitetin e punës në zhvillimin ose operacionet e përcaktuara në marrëveshjet bilaterale ose multilaterale që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare;

- të ulë efikasitetin e punës në aktivitetet e shtetit në drejtim të ruajtjes dhe përparimit të paqes, stabilitetit, sigurisë dhe të gjitha formave të bashkëpunimit me fqinjët, në rajon, Evropë dhe botë, si dhe në parandalimin dhe ndërtimin e instrumenteve për paralajmërim të hershëm të tensioneve dhe krizave, me qëllim zgjidhjen e tyre në kohë dhe në mënyrë efikase përmes rrugëve paqësore dhe

- të ulë efikasitetin e punës në aktivitetet e shtetit për ruajtjen dhe përparimin e rendit ndërkombëtar të bazuar në drejtësi, respekt të ndërsjellë të rendit ndërkombëtar të themeluar në të drejtën ndërkombëtare, si dhe në barazinë politike dhe ekonomike të shteteve.

PËR PËRDORIM TË
KUFIZUAR

- të shkaktojë dëme ose të ndikojë në kushtet për përmirësimin dhe ruajtjen e stabilitetit të brendshëm politik, sigurisë dhe efikasitetit operativ të shtetit;

- t'u shkaktojë vuajtje të konsiderueshme personave;

- të shkaktojë dëm në ndërtimin e një shteti të drejtë dhe social me mundësi të barabarta për të gjithë qytetarët;

- të pengojë përparimin e negociatave politike, financiare, monetare, ekonomike dhe tregtare të shtetit;

- të parandalojë zhvillimin ose operacionet e përcaktuara në marrëveshjet bilaterale ose multilaterale që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare;

- të shkaktojë dëme financiare ose të lejojë arritje ose avantazhe të papërshtatshme për personat juridikë ose fizikë;

- të ndikojnë negativisht në ruajtjen dhe mbrojtjen e mjedisit;

- të rënojnë aktivitetet e shtetit në drejtim të ruajtjes dhe përparimit të paqes, stabilitetit, sigurisë dhe të gjitha formave të bashkëpunimit me fqinjët, në rajon, Evropë dhe botë, si dhe në parandalimin dhe ndërtimin e instrumenteve për paralajmërim të hershëm të tensioneve dhe krizave, me qëllim zgjidhjen e tyre në kohë dhe në mënyrë efikase përmes rrugëve paqësore;

- të rënojnë efikasitetin e punës në aktivitetet e shtetit për ruajtjen dhe përparimin e rendit ndërkombëtar të bazuar në drejtësi, respekt të ndërsjellë të rendit ndërkombëtar të themeluar në të drejtën ndërkombëtare, si dhe në barazinë politike dhe ekonomike të shteteve dhe

- të ndikojnë negativisht në marrëdhëniet ndërkombëtare të shtetit ose në marrëdhëniet e një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut.

INTERNE

- të dëmtojë rëndë paqen, themelet demokratike të sundimit të ligjit dhe zhvillimin e një shoqërie multietnike;

- të shkaktojë dëm serioz për jetën, shëndetin, pronën dhe sigurinë personale ose lirinë e njeriut dhe qytetarit;

- të shkaktojë dëm serioz në efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit;

- të shkaktojë dëme serioze ose të jetë në kundërshtim të konsiderueshëm me interesat financiare, monetare, ekonomike dhe tregtare të shtetit;

- të shkaktojë dëme serioze për mjedisin jetësor të vendit;

- të shkaktojë dëme serioze në nxitjen dhe zhvillimin e vetëqeverisjes lokale në vend;

- të shkaktojë dëme serioze ose të shkelë ndjeshëm integritimin e mbrojtjes politike të vendit në NATO, integritimin ekonomik dhe të sigurisë në Bashkimin Evropian ose në sisteme të tjera të sigurisë kolektive;

- të shkaktojë dëme serioze në zhvillimin ose operacionet e përcaktuara në marrëveshjet ndërkombëtare të ratifikuara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe dokumentet ndërkombëtare që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare;

- të shkaktojë dëme serioze në marrëdhëniet ndërkombëtare të shtetit, në mënyrë që të shkaktojë një protestë formale ose sanksione të tjera dhe

- të ndërpresë ose në mënyrë tjetër të pengojë ndjeshëm aktivitetet e rëndësishme të shtetit në planin ndërkombëtar ose aktivitetet e një vendi të huaj apo të një organizate ndërkombëtare në planin e bashkëpunimit me Republikën e Maqedonisë së Veriut.

KONFIDENCIALE

- të shkaktojë dëme jashtëzakonisht serioze për pavarësinë dhe integritetin territorial të shtetit;

- të shkaktojë dëme jashtëzakonisht serioze në identitetin shtetëror duke shprehur lirisht identitetin etnik të të gjithë qytetarëve;

- të rrezikojë drejtpërdrejt jetën ose të ndikojë jashtëzakonisht seriozisht në rendin publik ose sigurinë ose lirinë personale të personit dhe qytetarit;

- të shkaktojë dëm jashtëzakonisht serioz në efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve jashtëzakonisht të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit;

- të shkaktojë dëme materiale jashtëzakonisht të rënda për interesat financiare, monetare, ekonomike dhe tregtare të vendit;

- të shkaktojë dëme jashtëzakonisht serioze për mjedisin jetësor të vendit;

- të shkaktojë dëme jashtëzakonisht serioze në nxitjen dhe zhvillimin e vetëqeverisjes lokale në vend dhe

- të shkaktojnë dëme jashtëzakonisht serioze në arritjen e objektivave të politikës ndërkombëtare ose marrëdhënieve ndërkombëtare të shtetit ose marrëdhënieve të një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut.

RREPËTËSISHT
KONFIDENCIALE

- të rrezikojë drejtpërdrejt integritetin territorial dhe sovranitetin, si dhe rendin kushtetues të shtetit;

- të rrezikojë drejtpërdrejt stabilitetin e brendshëm të shtetit;

- të çojë drejtpërdrejt në humbje masive njerëzore;

- të shkaktojë dëme të pa riparueshme serioze mbi efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve jashtëzakonisht të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit;

- të shkaktojë dëme të riparueshme në liritë dhe të drejtat themelore të njeriut dhe qytetarit, demokracisë dhe shtetit të së drejtës;

- të shkaktojë dëme të riparueshme në nxitjen dhe zhvillimin e ekonomisë së vendit, mbrojtjen e pronës, lirinë e tregut dhe sipërmarrjen, humanizmin, drejtësinë sociale dhe solidaritetin;

- të shkaktojë dëme të riparueshme për mbrojtjen dhe promovimin e mjedisit jetësor të shtetit;

- të shkaktojë pasoja të rënda afatgjata në nxitjen dhe zhvillimin e vetëqeverisjes lokale në shtet dhe

- të rrezikojnë drejtpërdrejt arritjen e objektivave të politikës ndërkombëtare të vendit ose të shkaktojnë dëme të riparueshme në marrëdhëniet ndërkombëtare të vendit ose në marrëdhëniet e një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut.

SEKRET
SHTETËROR

4.5.1. Për përdorim të kufizuar

Me shënimin “PËR PËRDORIM TË KUFIZUAR” shënohet vetëm ajo informacion, zbulimi i së cilës do të ulte efikasitetin e punës së organeve të pushtetit shtetëror dhe lokal të themeluara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe me ligj, si dhe të personave juridikë të themeluar nga Republika ose nga komunat, Qyteti i Shkupit dhe komunat në Qytetin e Shkupit.

Pasojat specifike që do të rezultonin nga zbulimi i paautorizuar i këtyre informacioneve janë:

1. të ulë efikasitetin e punës ose të ndikojë në kushtet për përmirësimin dhe ruajtjen e stabilitetit të brendshëm politik, sigurisë dhe efikasitetit operativ të shtetit

I referohet informacionit të brendshëm, procedurave ose analizave në lidhje me aspektet e sigurisë në funksionimin e organeve shtetërore, zbulimi i të cilave mund të çojë në pengimin e funksionimit efektiv të organeve ose krijimin e dobësive operationale.

2. të ulë efikasitetin e punës në ndërtimin e një shteti të drejtë dhe social me mundësi të barabarta për të gjithë qytetarët

I referohet informacionit mbi programet sociale, shpërndarjen e burimeve ose masave për të mbështetur grupet në nevojë, të cilat, nëse zbulohen, mund të pengojnë ndërtimin e mundësive të barabarta për të gjithë qytetarët në shtet.

3. të ulë efikasitetin e punës në negociatat politike, financiare, monetare, ekonomike dhe tregtare të shtetit

I referohet informacionit në lidhje me negociatat me vendet e huaja, investitorët ose institucionet që shpesh përmbajnë të dhëna të ndjeshme mbi kushtet dhe strategjitë. Zbulimi i këtyre të dhënave mund të dobësojë pozicionin negociues të shtetit.

4. të ulë efikasitetin e punës në zhvillimin ose operationet e përcaktuara në marrëveshjet bilaterale ose multilaterale që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare

I referohet informacionit mbi aspektet operationale të marrëveshjeve ose detyrimeve të marrëveshjeve ndërkombëtare që janë të ndjeshme dhe zbulimi i tyre mund të dëmtojë zbatimin ose të krijojë tensione diplomatike.

5. të ulë efikasitetin e punës në aktivitetet e shtetit në drejtim të ruajtjes dhe përparimit të paqes, stabilitetit, sigurisë dhe të gjitha formave të bashkëpunimit me fqinjët, në rajon, Evropë dhe botë, si dhe në parandalimin dhe ndërtimin e instrumenteve për paralajmërim të hershëm të tensioneve dhe krizave, me qëllim zgjidhjen e tyre në kohë dhe në mënyrë efikase përmes rrugëve paqësore

I referohet informacionit mbi nismat diplomatike, projektet e sigurisë ose strategjitë e parandalimit të konflikteve, të cilat, nëse zbulohen, mund të dobësojnë ndikimin e shtetit ose të çojnë në sabotim të aktiviteteve.

6. të ulë efikasitetin e punës në aktivitetet e shtetit për ruajtjen dhe përparimin e rendit ndërkombëtar të bazuar në drejtësi, respekt të ndërsjellë të rendit ndërkombëtar, si dhe në barazinë politike dhe ekonomike të shteteve

I referohet informacionit që tregon një devijim nga standardet, procedurat ose detyrimet ndërkombëtare që mund të dobësojnë pozicionin e shtetit ndërkombëtarisht dhe të kërcënojnë besimin e partnerëve.

4.5.2. Interne

Me nivelin "INTERN" klasifikohet vetëm ai informacion, zbulimi i paautorizuar i së cilit do të shkaktonte dëm në funksionimin e organeve.

Pasojat specifike që do të rezultonin nga zbulimi i paautorizuar i këtyre informacioneve janë:

1. të shkaktojë dëme ose të ndikojë në kushtet për përmirësimin dhe ruajtjen e stabilitetit të brendshëm politik, sigurisë dhe efikasitetit operativ të shtetit

I referohet informacionit se si të merren me rreziqet dhe kërcënimet e sigurisë dhe zbulimi i të cilave do të shkaktonte dobësim dhe mosbesim në sistemin e sigurisë.

2. t'u shkaktojë vuajtje të konsiderueshme personave

I referohet informacionit, zbulimi i të cilit mund të çojë në trauma psikologjike, vuajtje fizike, diskriminim ose rrezik për një grup personash.

3. të shkaktojë dëm në ndërtimin e një shteti të drejtë dhe social me mundësi të barabarta për të gjithë qytetarët

I referohet informacionit mbi masat, aktivitetet dhe praktikën e brendshme në politikat sociale, zbulimi i të cilave mund të provokojë manipulime politike, të minojë besimin në institucione dhe të krijojë përshtypjen e padrejtësisë midis qytetarëve.

4. të pengojë përparimin e negociatave politike, financiare, monetare, ekonomike dhe tregtare të shtetit

I referohet informacionit mbi negociatat me investitorët e huaj, bankat ndërkombëtare ose vendet që përmbajnë të dhëna të ndjeshme mbi kushtet, çmimet dhe strategjitë. Zbulimi i informacioneve të tilla mund të dobësojë pozicionin negociues të shtetit.

5. të parandalojë zhvillimin ose operacionet e përcaktuara në marrëveshjet bilaterale ose multilaterale që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare

I referohet informacionit në lidhje me marrëveshjet me shtete ose organizata të tjera, zbulimi i të cilave mund të shkaktojë tensione diplomatike.

6. të shkaktojë dëme financiare ose të lejojë arritje ose avantazhe të papërshtatshme për personat juridikë ose fizikë

I referohet informacionit që do të lejonte individë ose kompani të caktuara të fitonin një avantazh financiar ose të shmangnin detyrimet.

7. të ndikojnë negativisht në ruajtjen dhe mbrojtjen e mjedisit

I referohet informacionit mjedisor që mund të shkaktojë panik ose të përdoret për presion shoqëror.



8. të rrënojnë aktivitetet e shtetit në drejtim të ruajtjes dhe përparimit të paqes, stabilitetit, sigurisë dhe të gjitha formave të bashkëpunimit me fqinjët, në rajon, Evropë dhe botë, si dhe në parandalimin dhe ndërtimin e instrumenteve për paralajmërim të hershëm të tensioneve dhe krizave

I referohet informacionit në lidhje me përpjekjet diplomatike, iniciativat e sigurisë ose strategjitë e parandalimit të konflikteve që mund të sabotohen.

9. të rrënojnë efikasitetin e punës në aktivitetet e shtetit për ruajtjen dhe përparimin e rendit ndërkombëtar të bazuar në drejtësi, respekt të ndërsjellë të së drejtës ndërkombëtare, si dhe në barazinë politike dhe ekonomike të shteteve

I referohet informacionit, zbulimi i të cilit mund të dëmtojë reputacionin e shtetit.

10. të ndikojnë negativisht në marrëdhëniet ndërkombëtare të shtetit ose në marrëdhëniet e një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut

I referohet informacionit të përfshirë në komunikimet diplomatike, marrëveshjet e ndjeshme, etj., zbulimi i të cilave mund të shkaktojë një incident diplomatik.

4.5.3. Konfidenciale

Me nivelin "KONFIDENCIAL" klasifikohet vetëm ai informacion, zbulimi i paautorizuar i së cilit do të shkaktojë dëm serioz për interesat e rëndësishme të Republikës së Maqedonisë së Veriut.

Pasojat specifike që do të rezultojnë nga zbulimi i paautorizuar i këtyre informacioneve janë:

1. të dëmtojë rëndë paqen, themelet demokratike të sundimit të ligjit dhe zhvillimin e një shoqërie multietnike

Ai i referohet informacionit që, nëse publikohet, mund të nxisë paqëndrueshmërinë sociale, të prishë paqen publike ose të minojë vlerat demokratike.

2. të shkaktojë dëm serioz për jetën, shëndetin, pronën dhe sigurinë personale ose lirinë e njeriut dhe qytetarit

I referohet informacionit, zbulimi i paautorizuar i të cilit mund të çojë në rrezikimin e qytetarëve, pronës ose shëndetit të tyre.

3. të shkaktojë dëm serioz në efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit

I referohet informacionit që mund të dobësojë aftësinë e institucioneve për t'u marrë me rreziqet e sigurisë, terrorizmin ose krimin e organizuar.

4. të shkaktojë dëme serioze ose të jetë në kundërshtim të konsiderueshëm me interesat financiare, monetare, ekonomike dhe tregtare të shtetit

I referohet informacionit që, nëse zbulohet, mund të ndikojë në stabilitetin e tregjeve,

buxhetit ose politikave ekonomike të vendit.

5. të shkaktojë dëme serioze për mjedisin jetësor të vendit

I referohet informacionit që mund të keqpërdoret në një mënyrë që do të rezultonte në degradimin e mjedisit ose rreziqe për shëndetin e popullatës.

6. të shkaktojë dëme serioze në nxitjen dhe zhvillimin e vetëqeverisjes lokale në vend

I referohet informacionit në lidhje me projektet e zhvillimit, shpërndarjen e fondeve ose infrastrukturën kritike në nivel lokal.

7. të shkaktojë dëme serioze ose të shkelë ndjeshëm integrimin e mbrojtjes politike të vendit në NATO, integrimin ekonomik dhe të sigurisë në Bashkimin Evropian ose në sisteme të tjera të sigurisë kolektive

I referohet informacionit, zbulimi i të cilit mund të minojë besimin midis aleatëve dhe të kërcënojë integrimin e vendit në organizatat ndërkombëtare.

8. të shkaktojë dëme serioze në zhvillimin ose operacionet e përcaktuara në marrëveshjet ndërkombëtare të ratifikuara në përputhje me Kushtetutën e Republikës së Maqedonisë së Veriut dhe dokumentet ndërkombëtare që shteti ka lidhur me vende të huaja ose organizata ndërkombëtare

I referohet informacionit në lidhje me negociatat, marrëveshjet ose bashkëpunimin ndërkombëtar në vazhdim, kompromisi i të cilit do të dobësonte pozicionin e shtetit.

9. të shkaktojë dëme serioze në marrëdhëniet ndërkombëtare të shtetit, në mënyrë që të shkaktojë një protestë formale ose sanksione të tjera

I referohet informacionit, zbulimi i të cilit mund të provokojë një reagim negativ diplomatik (incident, sanksion, ndërprerje të bashkëpunimit, etj.).

10. të ndërpresë ose në mënyrë tjetër të pengojë ndjeshëm aktivitetet e rëndësishme të shtetit në planin ndërkombëtar ose aktivitetet e një vendi të huaj apo të një organizate ndërkombëtare në planin e bashkëpunimit me Republikën e Maqedonisë së Veriut

I referohet informacionit që mund të ndikojë në bashkëpunimin në operacionet, nismat ose programet e përbashkëta me partnerët e huaj.

4.5.4. Rreptësisht konfidenciale

Me nivelin "REPTËSISHT KONFIDENCIAL" klasifikohet vetëm ai informacion, zbulimi i paautorizuar i së cilit do të shkaktoje dëm jashtëzakonisht serioz për interesat e rëndësishme të Republikës së Maqedonisë së Veriut.

Pasojat specifike që do të rezultojnë nga zbulimi i paautorizuar i këtyre informacioneve janë:

1. të shkaktojë dëme jashtëzakonisht serioze për pavarësinë dhe integritetin territorial të shtetit

I referohet informacionit që, nëse zbulohet, mund të krijojë një rrezik real të cenimit të



pavarësisë ose unitetit territorial të shtetit, duke nxitur konflikte të brendshme dhe të jashtme, duke inkurajuar lëvizjet separatiste, etj.

2. të shkaktojë dëme jashtëzakonisht serioze në identitetin shtetëror duke shprehur lirisht identitetin etnik të të gjithë qytetarëve

I referohet informacionit në lidhje me identitetin etnik dhe politikën shtetërore për një shoqëri multietnike, kompromisi i të cilit mund të çojë në tensione, diskriminim, përçarje të marrëdhënieve ndëretnike, kohezion social dhe një ndjenjë të përkatësisë në shtet.

3. të rrezikojë drejtpërdrejt jetën ose të ndikojë jashtëzakonisht seriozisht në rendin publik ose sigurinë ose lirinë personale të personit dhe qytetarit

I referohet informacionit në lidhje me masat e sigurisë, që kanë të bëjnë me protestat ose grupet kriminale, etj., zbulimi i të cilave mund të rrezikojë drejtpërdrejt jetën ose sigurinë e personave, ose të shkaktojë trazira të rënda publike.

4. të shkaktojë dëm jashtëzakonisht serioz në efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve jashtëzakonisht të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit

I referohet informacionit në lidhje me aktivitetet e fshehta të mbrojtjes, sigurisë ose inteligjencës, operacionet, metodat ose agjentët, zbulimi i të cilave do të zvogëlonte aftësinë e shtetit për t'iu përgjigjur kërcënimeve terroriste ose kërcënimeve të tjera të sigurisë.

5. të shkaktojë dëme materiale jashtëzakonisht të rënda për interesat financiare, monedhë, ekonomike dhe tregtare të vendit

I referohet informacionit që mund të shkaktojë paqëndrueshmëri financiare, zhvlerësim të monedhës ose përçarje të besimit të tregut.

6. të shkaktojë dëme jashtëzakonisht serioze për mjedisin jetësor të vendit

I referohet informacionit në lidhje me mbrojtjen e mjedisit, keqpërdorimi i të cilit mund të shkaktojë fatkeqësi të rënda mjedisore ose pasoja shëndetësore.

7. të shkaktojë dëme jashtëzakonisht serioze në nxitjen dhe zhvillimin e vetëqeverisjes lokale në shtet

I referohet informacionit në lidhje me politikat lokale, projektet e infrastrukturës ose planet financiare, kompromisi i të cilave mund të shkaktojë dëme serioze në funksionimin e vetëqeverisjes lokale.

8. të shkaktojnë dëme jashtëzakonisht serioze në arritjen e objektivave të politikës ndërkombëtare ose marrëdhënieve ndërkombëtare të shtetit ose marrëdhënieve të një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut

I referohet informacionit, kompromisi i të cilit mund të dëmtojë seriozisht reputacionin e shtetit, të shkaktojë një mosmarrëveshje diplomatike ose të ndikojë negativisht në partneritetet ndërkombëtare.

4.5.5. Sekret shtetëror

Me shkallën “SEKRET SHTETËROR” klasifikohet vetëm ai informacion, zbulimi i paautorizuar i të cilit do të shkaktonte rrezik dhe dëm të pariparueshëm për interesat e qëndrueshme të Republikës së Maqedonisë së Veriut.

Pasojat specifike që do të rezultonin nga zbulimi i paautorizuar i këtyre informacioneve janë:

1. të rrezikojë drejtpërdrejt integritetin territorial dhe sovranitetin, si dhe rendin kushtetues të shtetit

I referohet informacionit, publikimi i të cilit do të mundësonte ose lehtësonte veprime që çojnë në shkelje të kufijve, integritetit territorial, ose në dëmtimin e institucioneve kushtetuese dhe rendit themelor kushtetues. Zbulimi i tyre do të lejonte aktorët e jashtëm ose të brendshëm të minojnë institucionet shtetërore ose të shkaktojnë konflikt.

2. të rrezikojë drejtpërdrejt stabilitetin e brendshëm të shtetit

I referohet informacionit që, nëse publikohet, mund të shkaktojë rrezikim dhe prishje serioze të rendit dhe paqes publike, shfaqjen e trazirave masive, panikut, mosbesimit, destabilizimit ose prishjes së funksioneve jetike të shtetit.

3. të çojë drejtpërdrejt në humbje masive njerëzore

I referohet informacionit që, nëse zbulohet, mund të rezultojë në humbjen e një numri të madh jetësh (si rezultat i konfliktit të armatosur, sulmit terrorist, fatkeqësisë së shkaktuar nga njeriu, incidenteve në infrastrukturën kritike, etj.).

4. të shkaktojë dëme të pa riparueshme serioze mbi efikasitetin operacional ose sigurinë e shtetit, ose në efikasitetin e operacioneve jashtëzakonisht të vlefshme të mbrojtjes, të sigurisë ose të inteligjencës, apo në operacionet e ndërmarra për përballimin e kërcënimeve jokonvencionale, veçanërisht terrorizmit

I referohet informacionit në lidhje me operacionet e fshehta, metodologjitë, burimet ose asetet e shërbimeve të inteligjencës së sigurisë dhe institucioneve të mbrojtjes, të cilat, nëse zbulohen, do të dëmtonin ndjeshëm funksionimin e tyre.

5. të shkaktojë dëme të pariparueshme në liritë dhe të drejtat themelore të njeriut dhe qytetarit, demokracisë dhe shtetit të së drejtës

I referohet informacionit, zbulimi i të cilit do të çonte në shkelje të përhershme të institucioneve demokratike, sundimit të ligjit ose mbrojtjes ligjore të lirive dhe të drejtave të qytetarëve.

6. të shkaktojë dëme të pariparueshme në nxitjen dhe zhvillimin e ekonomisë së vendit, mbrojtjen e pronës, lirinë e tregut dhe sipërmarrjen, humanizmin, drejtësinë sociale dhe solidaritetin

I referohet informacionit që, nëse zbulohet, do të shkaktonte dëme serioze dhe afatgjata ekonomike – për shembull, prishje të tregjeve financiare, manipulim të rëndë financiar ose rrezikim të të drejtave të pronësisë.



7. të shkaktojë dëme të pariparueshme për mbrojtjen dhe promovimin e mjedisit jetësor të shtetit

I referohet informacionit, publikimi i të cilit do të çonte në zbulimin e ekosistemeve të cenueshme ose do të mundësonte aktivitete që do të shkaktonin dëme afatgjata në mjedis dhe popullatë (panik, fatkeqësi mjedisore, pasoja të rënda shëndetësore, etj.).

8. të shkaktojë pasoja të rënda afatgjata në nxitjen dhe zhvillimin e vetëqeverisjes lokale në shtet

I referohet informacionit që, nëse zbulohet, do të paralizonte ose në planin afatgjatë do të dobësonte funksionimin dhe zhvillimin e vetëqeverisjeve lokale, mekanizmat e tyre financiarë ose infrastrukturën kritike në nivel lokal.

9. të rrezikojnë drejtpërdrejt arritjen e objektivave të politikës ndërkombëtare të vendit ose të shkaktojnë dëme të pariparueshme në marrëdhëniet ndërkombëtare të vendit ose në marrëdhëniet e një vendi të huaj ose organizate ndërkombëtare me Republikën e Maqedonisë së Veriut

I referohet informacionit që, nëse zbulohet, do të kompromentonte besimin midis shteteve, do të çonte në ndërprerjen e negociatave të ndjeshme diplomatike ose do të shkaktohte dëme afatgjata diplomatike dhe ndërkombëtare.

5. RREZIQET E KLASIFIKIMIT JOADEKUAT TË INFORMACIONEVE

Përcaktimi i shkallës së klasifikimit duhet të jetë rreptësisht proporcional me dëmin e vlerësuar nga qasja e paautorizuar ose përdorimi i paautorizuar. Në këtë mënyrë, parandalohen dy fenomene të rrezikshme:

klasifikimi i tepruar – Klasifikimi i tepruar ndodh kur informacionit i jepet një nivel më i lartë i fshehtësisë sesa ai që është realisht i nevojshëm. Kjo çon në:

- kufizim të panevojshëm të qasjes për zyrtarët që duhet të përdorin informacionin në punën e tyre (informacioni nuk është i disponueshëm për personat që duhet ta dinë),
- vendimmarrje të ngadaltë dhe efikasitet të rrënuar në institucione,
- rritjen e kostove administrative dhe financiare për ruajtjen, transferimin dhe mbrojtjen e informacionit,
- rrezik për krijimin e një “kulture të fshehtësisë” dhe uljen e transparencës së institucionit.

klasifikimi i pamjaftueshëm – klasifikimi i pamjaftueshëm ndodh kur informacionit i jepet një nivel më i ulët i mbrojtjes sesa është e nevojshme, duke rezultuar në:

- rritje të rrezikut që të dhënat kritike të vihen në dispozicion të personave të paautorizuar,
- mundësi për pasoja serioze të sigurisë, politike ose ekonomike,
- ndërprerjen e veprimtarisë operacionale të autoriteteve shtetërore,
- minimin e mundshëm të besimit dhe bashkëpunimit ndërkombëtar.

Për të mos ndodhur kjo, klasifikimi kërkon një vlerësim të duhur, të kujdesshëm dhe profesional të përmbajtjes së informacionit, dëmit të mundshëm të zbulimit të paautorizuar dhe kohëzgjatjes së ndjeshmërisë. Me një ekuilibër të duhur, institucionet sigurojnë mbrojtjen e interesave shtetërore, ndërkohë që mundësojnë trajtim efikas dhe të përgjegjshëm të informacioneve të klasifikuara.

6. REKOMANDIME PRAKTIKE PËR KLASIFIKIMIN E INFORMACIONEVE

Njohuri mbi kuadrin ligjor

Gjithmonë kini njohuri dhe kuptoni qartë LK-në dhe aktet nënligjore që rregullojnë klasifikimin e informacioneve.

Vlerësimi i kërcënimit dhe rrezikut nga zbulimi i informacioneve

Konsideroni se çfarë do të ndodhte nëse informacioni do të zbulohet në mënyrë të paautorizuar dhe se si do të ndikonte në interesat e shtetit ose institucionit.

Zbatimi i parimeve gjatë përcaktimit të shkallëve të klasifikimit të informacionit

Zbatimi i parimeve të dëmtimit, proporcionalitetit, domosdoshmërisë, kufizimit kohor dhe përgjegjësisë, si dhe praktikave të tjera të mira dhe pozitive të vendosura, në përcaktimin dhe justifikimin e shkallës së përshtatshme të klasifikimit të informacionit.

Objektiviteti dhe paanshmëria

Përcaktimi i nivelit duhet të bazohet në kriteret e përcaktuara me ligj (përmbajtja e informacionit dhe vlerësimi i dëmit dhe pasojave), dhe jo në interesa personale apo kritere subjektive.

Qëndrueshmëria në klasifikim

Informacioni me përmbajtje të ngjashme duhet të ketë një shkallë të ngjashme klasifikimi, për të shmangur konfuzionin, mbrojtjen e pabarabartë dhe të papërshtatshme.

Arsyetimi i nivelit të propozuar të klasifikimit

Zgjedhja e nivelit duhet të arsyetohet në propozimin e hartuesit.

Respektimi i ndjeshmërisë kohore

Vlerësoni nëse informacioni me kalimin e kohës e humb ndjeshmërinë dhe nëse është nevojitet rishikimi i nivelit.

Konsultim dhe verifikim kolegjal

Nëse dyshoni ose keni raste komplekse, konsultohuni me ekspertë, kolegë ose autoritete kompetente përkatëse.

Staf i trajnuar dhe i informuar

Të gjithë personat pjesëmarrës në proces duhet të edukohen për kriteret, procedurat dhe detyrimet për klasifikim.

Kultura e sigurisë në veprim/përdorim

Përcaktimi i nivelit të klasifikimit është pjesë e mbrojtjes së shtetit, institucionit dhe qytet arëve - gjithmonë trajtojeni informacionin si potencialisht të ndjeshëm.



BIBLIOGRAFIA

2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, <https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng>.

Bakreski, O., Deanoska-Trendafillova, A. (2021). Koment mbi Ligjin për informata të klasifikuara, DCAF, Shkup, https://www.dbki.gov.mk/files/pdf_files/Komentar_Makedonski.pdf.

Ligji për informata të klasifikuara, "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut", nr. 275/2019.

Kodi penal "Gazeta Zyrtare e Maqedonisë" nr. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 dhe 248/2018 dhe "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut" nr. 36/2023 dhe 188/2023. Vendimet e Gjykatës Kushtetuese të Republikës së Maqedonisë: U. nr. "Gazeta Zyrtare të Republikës së Maqedonisë" nr. 48/2001; U. nr. 210/2001 të 6 shkurtit 2002, botuar në "Gazeta Zyrtare të Republikës së Maqedonisë" nr. 16/2002; U. nr. 206/2003 të datës 9 qershor 2004, botuar në "Gazeta Zyrtare të Republikës së Maqedonisë" nr. 40/2004; U. nr. 228/2005 të datës 5 prill 2006, botuar në "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 50/2006 dhe U. nr. 169/2016 të 16 nëntorit 2017, botuar në "Gazeta Zyrtare të Republikës së Maqedonisë" nr. 170/2017.

Koncepti nacional për siguri dhe mbrojtje, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 40/2003

Rregullorja për sigurinë administrative të informacioneve të klasifikuara dhe të informacioneve për përdorim të kufizuar, "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut" nr. 204/2023.

Rregullorja për sigurinë e personave që përdorin informata të klasifikuara, "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut", nr. 157/2022.

Rregullorja për Sigurinë Industriale të Informacionit të Klasifikuar, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 16/2005.

Rregullorja për Sigurinë e Informacionit të Informacionit të Klasifikuar, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 16/2005.

Rregullorja për sigurinë fizike të informatave të klasifikuara, "Gazeta Zyrtare e Republikës së Maqedonisë së Veriut", nr. 175/2025.

Kushtetuta e Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 52/1991, me amendamentet I dhe II të Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 1/1992, Amendamenti III i Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 31/1998, Amendamenti IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV, XVI, XVII dhe XVIII të Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 91/2001, Amendamenti XIX i Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 84/2003, Amendamentet XX, XXI, XXII, XXIII, XXIV, XXV, XXVI, XXVII, XXVIII, XXIX dhe XXX të Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 107/2005, Amendamenti XXXI i Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë"

nr. 3/2009, Korrigjimi i Amendamentit XXXI të Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 13/2009, Amendamenti XXXII i Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 49/2011, Amendamentet XXXIII, XXXIV, XXXV dhe XXXVI të Kushtetutës së Republikës së Maqedonisë, "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 6/2019, dhe botimi "Gazeta Zyrtare e Republikës së Maqedonisë" nr. 36/2019.



