ОСНОВНИ ПОЛОЖЕНИЯ ПРИ ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В УСЛОВИЯТА НА КРИЗИ

Автор: Асен Й. Захариев

Университет по библиотекознание и информационни технологии, доцент д-р

Резюме: *В доклада се разглеждат рискове и заплахи за сигурността на класифицираната информация в условията на кризи с различен характер. На основата на правно-нормативната уредба, регламентираща защитата на класифицираната информация, е представена система от мерки на видовете сигурност на информацията. В резултат на изводи и обобщения са изведени препоръки за ефективното им прилагане.*

Ключви думи: *кризи, риск, заплахи, класифицирана информация, видове сигурност.*

FUNDAMENTALS IN THE PROTECTION OF CLASSIFIED INFORMATION IN CRISIS CONDITIONS

Author: Asen Y. Zahariev

University of Library studies and Information technologies, Associated prof, PHD

Abstract: *The report examines risks and threats to the security of classified information in the context of crises of different nature. Based on the legal and regulatory framework, regulating the protection of classified information, a system of measures of the types of security of information is presented. As a result of conclusions and summaries, recommendations for their effective implementation have been made.*

Keywords: *crises, risk, threats, classified information, types of security*

Динамичните промени в средата на сигурност, съвременните реалности и новите предизвикателства оказват силно влияние върху състоянието на националната сигурност. Съществено влияние оказват и кризите от различен характер, които водят до нова несигурност и нови рискове.

В условията на новите реалности дейността по опазване на важната за сигурността на страната информация придобива нови измерения, изправя се пред нови заплахи и налага различни подходи и механизми за предотвратяване, овладяване и преодоляване на предизвиканите от тях неблагоприятни последици. В условия на криза изработването на адекватни политики за отговор е усложенено поради тяхната непредвидимост, непредсказуемост, неопределеност и интензивност. Динамиката на процесите и измененията на средата не могат да бъдат отчетени своевременно в правно-нормативната уредба която регламентира дейностите по защита на класифицираната информация в

условия на значителна неопределеност. Това налага да се прилагат гъвкави подходи при управлението на сигурността при отчитане на рисковете и уязвимостите на системата.

В усилията си за адекватен отговор на нарастващите рискове бяха приети различни инициативи за ефективно управление при кризи. В тази връзка на първо място бяха приети редица закони и подзаконови документи в съответствие с общностното право. За пръв път управлението при кризи е регламентирано в Закона за управление при кризи Обн. ДВ. бр.19 от 1 Март 2005г. Този закон в последствие е отменен и за уреждане на обществените отношения в тази област е приет Законът за защита при бедствия. В последвалите Национална стратегия за намаляване на риска от бедствия 2018-2030, Национална програма за намаляване на риска от бедствия 2021-2025. РМС № 865/26.11.2020, Национален план за защита при бедствия 2010. РМС № 868/01.12.2011 и други нормативни актове е поставена рамката за управление при кризи в различни области на националната сигурност но не е уреден въпросът със защитата на класифицираната информация. Тя от части е засегната в Закона за защита на класифицираната информация и Правилника за прилагане на Закона за защита на класифицираната информация. Съществен тук е въпросът как нормативната уредба в тези области кореспондира по между си, обхваща ли възможните ситуации и предоставя ли ефективна защита на информацията в различните по своя характер кризи.

Нормативната уредба в областта на информационната сфера също беше хармонизирана с общностното право като се приеха редица закони, регламентиращи обществените отношения в информационната сфера и по-конкретно в областта на защита на класифицираната информация. Основните от тях са Законът за защита на класифицираната информация, Законът за защита на личните данни, Законът за достъп до обществена информация, Правилникът за прилагане на Закона за защита на класифицираната информация. На основата на гореспоменатата нормативна уредба са приети съответно наредби и указания.

С приемането на тези закони се осъществява комплекс от мерки за гарантиране на информационната сигурност в органите на държавната власт, държавните учреждения и организации.

Мотивите за приемане на Закона за защита на класифицираната информация са свързани с изграждането на законодателна и институционална база в областта на защитата на класифицираната информация. Целта е да се да се дефинират по нов начин приоритетите и основните понятия, да се определят компетентните органи и да се регламентират техните правомощия, детайлно да се уредят процедурите и принципите

за защита на секретната информация, като се приведат в съответствие с политиката и стандартите на НАТО, както и за изпълнението на споразуменията по сигурността между Република България с НАТО и с други страни - членки и партньори.(www.aip-bg.org/documents/secr_mot.htm)

Акцентът на закона е поставен най-вече върху защитата на класифицираната информация от нерегламентирен достъп, които би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика, защитата на конституционно установения ред или друг правно защитен интерес.

Установената система за защита на класифицираната информация трябва да осигури опазването на относимата към сигурността на страната информация, като отговори на предизвикателствата не само в обичайна обстановка, но и в условията на кризи и конфликти. Осигуряването на защитата на класифицираната информация от нерегламентиран достъп в ситуации, различни от нормалната за системата, е показател за устойчивостта и универсалната приложимост на предвидените принципи, способи и мерки, а също така и на ефективното функциониране на оправомощените органи.

Управлението на риска е съвременен подход, чието приложение в сферата на сигурността позволява осъществяването на комплексно противодействие на многобройните източници на заплаха и надеждното предотвратяване на негативното им въздействие. В този контекст могат да бъдат разгледани важни проблемни области свързани със защитата на класифицираната информация в условия на кризи. В контекста на казаното до тук може да се обобщи, че установената система за защита на класифицираната информация трябва да осигури опазването на относимата към сигурността на страната информация, като отговори на предизвикателствата не само в мирно време, но и в условията на кризи и конфликти.

По своя характер и мащаб кризите могат да имат различни измерения, но интерес с оглед разглежданата проблематика представляват тези, които засягат жизненоважни интереси на обществото и пряко или косвено са свързани със заплаха и необходимост от защита на националната сигурност и обществения ред в държавата. В този смисъл "кризата" може да се разглежда като такава промяна на регионалната, националната или международна обстановка, характеризираща се с увеличена интензивност на разрушителни или агресивни процеси, при която са застрашени основни ценности, интереси и цели на обществото и се създава висока степен на заплаха за живота,

здравето и имуществото на голяма група от хора, за унищожаване на съществуващите материални и природни ресурси и за функциониране на националното стопанство.

Чрез прилагането на принципите и мерките заложени в различните видове сигурност се постига цялостна защита на класифицираната информация и се неутрализират или се свеждат до минимум възможните заплахи за сигурността на информацията независимо от условията. Отделните видове сигурност са елемент от цялостната система за защита на класифицираната информация и те се групират съгласно уязвимостта на системата.

Най- общите причини водещи до нерегламентиран достъп до класифицирана информация в нормална обстановка са:

- Нарушения от страна на изпълнителите относно класифицирането на информация;
- Разгласяване по невнимание на класифицирана информация при общуването със широк кръг лица;
- Загуба на секретни документи и изделия;
- Недостатъци в организацията на работа по защита на класифицирана информация.
- Пропуски в подготовката на служителите за работа с класифицирана информация.
- Несвоевременно вземане на мерки по ограничаване на последствията от нерегламентиран достъп.

При кризисна обстановка се създават допълнителни условия за осъществяване на нерегламентиран достъп до класифицирана информация.

Ако в обичайна обстановка за предотвратяването на изтичането на класифицирана информация е достатъчно мероприятията да се свеждат до: спазване на нормативната уредба регламентираща работата с класифицирана информация; контрол на изпълнение на изискванията за работа с класифицирана информация; контрол на регистратурите, то при кризи е необходимо да се направи анализ и оценка на риска; оценка на уязвимостите; подготовка и обучение на служителите и изготвяне на планове по видовете сигурност.

Системата от мерки за **физическ**а сигурност е част от общите изисквания за сигурност на класифицираната информация.

В Закона физическата сигурност на класифицираната информация е дефинирана като система от организационни, физически и технически мерки за предотвратяване на нерегламентиран достъп до материали, документи, техника и съоръжения,

класифицирани като държавна или служебна тайна. Тази система се изгражда чрез защита на сградите, помещенията и съоръженията, в които се създава, обработва и съхранява класифицирана информация и контрола върху достъпа до тях.

Системата от мерки, способи и средства за физическа сигурност на класифицираната информация биват: общи, конкретни и специални (Чл. 8, ал.1, Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване).

Общите мерки за физическа сигурност са организационни и се изразяват в определяне и изграждане на зоните за сигурност.

Конкретните мерки са физически и технически и включват:

- определяне и изграждане на периметър;
- защитно осветление;
- алармена система против проникване;
- контрол на физическия достъп;
- защита срещу подслушване, осъществявано със или без технически средства;
- защита срещу неправомерно визуално наблюдение, осъществявано със или без технически средства;
- осъществяване на визуално наблюдение за защита на физическата сигурност на класифицираната информация със или без използване на технически средства минимум през 2 часа;
- сили за реагиране;
- пожарогасителна или пожароизвестителна система.

Специалните мерки се прилагат за осигуряване физическата сигурност на класифицирана информация, съдържаща се в материални носители, които поради своето естество или размери не могат да бъдат пренасяни (транспортирани) по общия ред, предвиден в правилника. (чл.58 от ППЗЗКИ)

В рамките на физическата сигурност на класифицираната информация специално внимание заслужават способите за предотвратяване на заплахите, а именно анализът на риска и плана за осигуряване на физическа сигурност. Целта на тези способи е насочена към създаване на ефективни методи за противодействие на заплахите за физическата сигурност чрез използване на защитни мерки.

В изпълнение на правомощието си по чл. 22, ал. 1, т. 3 от ЗЗКИ и на базата на анализа на риска служителят по сигурността на информацията разработва план за

физическа сигурност чрез физически и технически средства и следи за неговото изпълнение.

Предназначението на плана за физическа защита на класифицираната информация е да осигурява защитата на сградите, помещенията и съоръженията, в които се създава, обработва, съхранява и предоставя класифицирана информация в обичайните условия, при които съответната организационна единица осъществява своята дейност. В усложнена обстановка законът предвижда изготвянето на отделен план за защита на класифицираната информация при положение на война, военно или друго извънредно положение, задължението за чието изготвяне е предвидено за служителя по сигурността на информацията. (чл. 22, ал. 1, т.11 от ЗЗКИ). По този начин се отчита, че установените способи едва ли ще бъдат достатъчно ефективни, за да осигурят защитата при извънредни ситуации.

В заключение може да се направи извода, че физическата сигурност е сред най-уязвимите части от цялостната система за защита на класифицираната информация.

При наличието на подобни уязвимости в системата за физическа сигурност на класифицираната информация в условията на едно извънредно кризисно положение, тази информация ще бъде подложена на изключително висок риск от осъществяването на нерегламентиран достъп, нарушаване на защитата й или на риск за нейното физическо унищожаване.

Определение на понятието "документална сигурност" се съдържа в чл. 80, ал. 1 ЗЗКИ. Според цитираната разпоредба документалната сигурност се състои в система от мерки, способи и средства за защита на класифицираната информация при създаването, обработването и съхраняването на документи, както и организирането и работата на регистратури за класифицирана информация. Конкретните уредба на мерките, способите и средствата за защита, формиращи системата на документалната сигурност са детайлно регламентирани в Глава V на ППЗЗКИ.

Така установената от закона и подзаконовите актове по неговото прилагане система от мерки, способи и средства има за цел защитата на класифицираната информация от разгласяване, увреждане, злоупотреба, промяна, предоставяне, унищожаване, както и от всякакви други действия, водещи до нарушаване на защитата й или до загубване на такава информация.

Основните предизвикателства за постигане на документалната сигурност в условия на кризи са свързани с организирането на работата и отчетността на дейността на регистратурите за класифицирана информация.

Единственото отклонение от този режим се съдържа в чл. 55, ал. 3 от ППЗЗКИ и се отнася до случаите на бедствия и аварии. Само в тези две хипотези достъпът до помещенията в регистратурата, които не са определени за работа със съответните потребители от организационната единица, се осигурява от служители в регистратурата при това задължително с придружител (длъжностно лице от организационната единица), а в извънработно време и в почивни дни – от упълномощено длъжностно лице от регистратурата. Правният режим на регистратурите е изключително ограничителен. Законоустановените отклонения са малко на брой и важат само за случаи на бедствия и аварии. От установената формулировка може да се заключи, че се обхващат последиците от кризи, настъпили вследствие на човешка дейност, събития и природни явления. От характера на уредбата може да се направи извод, че тя е подчинена на правилото, че минимално необходимата защита е тази, установена в ППЗЗКИ и всяко отклонение от нея би могло да представлява нерегламентиран достъп до класифицирана информация. Именно поради това при усложнена обстановка трябва да се има предвид, че действията по опазване на съхраняваната в организационната единица класифицирана информация трябва да се реализират по предварително утвърден план. Този план трябва да бъде съобразен с анализа на риска за съответната организационна единица и дейностите който попадат в обхвата на управлението при кризи съгласно разпоредбите на Закона за защита от бедствия.

Като конкретна мярка с цел ограничаването на заплахите за документалната сигурност на класифицираната информация е необходимо служителя по сигурността на информацията да изготвя план за евакуация на документите и материалите съдържащи класифицирана информация в извънредни положения.

Съгласно чл. 83, ал. 1 от ЗЗКИ персоналната сигурност на класифицираната информация представлява система от принципи и мерки, прилагани от компетентните органи по съответния ред спрямо лицата с цел гарантиране на тяхната надеждност с оглед защитата на класифицираната информация.

За да се постигне установената цел, е необходимо да се предприемат следните дейности, попадащи в обхвата на персоналната сигурност: процедурата по проучване за надеждност, обучението за работа с класифицирана информация, прилагането на принципа “необходимост да се знае” и контролът за надеждност, упражняван по отношение на лицата, получили достъп до класифицирана информация.

Процедурата по проучване на лицата за надеждност трябва да бъде проведена за достъп до класифицирана информация, представляваща държавна тайна. Изключение е

предвидено в чл. 38, ал.2 от ЗЗКИ, за лицата с достъп до информация, класифицирана като служебна тайна.

В условия на криза без значение дали кризисоопределящите фактори са човешка дейност, събития или природни бедствия, опеделящи поведението на системата са недостигът на сили и средства, на време за реакция и на пълна информация. На тази основа може да се направи извода, че в условията на една извънредна обстановка едно лице може да реагира по начин, които не е типичен за него. Без предварителна подготовка за реагиране в условията на кризисни ситуации не може да се очаква адекватна реакция. В този контекст, като слабости в рамките на персонолната сигурност могат да се отчетат липсата на нормативно установени правила за действие в извънредни ситуации. Регламентираните задължения на лицата получили достъп до класифицирана информация са ориентирани изцяло към състоянието на нормално функциониране на системата за защита на класифицираната информация.

Прилагането на правилата за проучване на лицето за надеждност и обучение за работа с класифицирана информация, ще бъде невъзможно поради липсата на време. В подобна ситуация нарушаването на установените правила за защита на класифицираната информация може да е единственото средство за преодоляване на кризата. За така извършено нарушение на установените правила не следва да се носи наказателна и административнонаказателна отговорност. Това обстоятелство налага необходимостта от нормативна регламентация за осъществяване на последващ контрол по отношение на лица имали достъп до класифицирана информация в условията на една извънредна кризисна обстановка. Ако в условията на криза достъп до класифицирана информация е предоставен на лице, което не отговаря на регламентираните условия, то това лице трябва да бъде включено в кръга на лицата, които подлежат на контрол за надеждност. Това се налага с цел идентифициране на признаци за по-нататъшно разпространение на информация от лицето и съответно предприемане на мерки за поемане на отговорност за тези последващи действия, независимо че информацията е станала известна на лицето в условията на една извънредна обстановка.

Определението за Комуникационна и информационна система се съдържа в параграф 1 т. 19 от допълнителните разпоредби на Закона за защита на класифицираната информация. Според разпоредбата на закона Комуникационна и информационна система (КИС) е съвкупност от технически (включително комуникационни средства, устройства за защита на границата, криптографски средства и среда за разпространение на сигналав границите на системата) и програмни средства, методи, процедури и

персонал, организирани за осъществяване на една или няколко функциите по създаване, обработване, ползване, съхраняване и обмен на класифицирана информация в електронна форма. (§1, т. 19 от ЗЗКИ).

Преднамерените заплахи могат да се групират на външни и вътрешни. Към външните се отнасят: терористи - реалното им присъствие са компютърните вируси; компютърни престъпници; корпоративни нарушители; хакери и др. Към вътрешните се отнасят грешките поради некомпетентност и невнимание на потребителите, операторите, системните администратори и други лица, обслужващи информационните системи. Понякога такива грешки се явяват като заплахи (неправилно въведени данни, грешка в програмата, която би могла да доведе до срив в системата), понякога създават слаби места, от които биха могли да се възползват определени сили. Най добрата защита на КИС в обичайна и извънредна обстановка е прилагането на стандартите за сигурност, определяне на уязвимостите на системите, строг контрол по прилагане на разпоредбите, обучение на персонала и

Изградената система за защита на класифицираната информация в Република България има превантивна роля. Тя гарантира нейната защита от нерегламентиран достъп, недопускане нанасянето на вреди в областта на националната сигурност, посредством ясно формулирани и нормативно определени правила, способи и процедури при създаването, съхраняването и предоставянето на достъп до нея.

В обобщение като основни източници на рискове и заплахи за сигурността на класифицираната информация се очертават:

- опитите за осъществяване на нерегламентиран достъп до класифицирана информация;

- нарушаване на нормативно установения ред за създаване, обработка, съхраняване, предоставяне и ползване на класифицирана информация;

- поддържане в неактуално състояние на нормативната база в областта на сигурността на класифицираната информация;

- целенасочените информационно-технически въздействия спрямо информация свързана със защитени държавни или обществени интереси;

- противозаконна дейност, спрямо държавните информационни и телекомуникационни системи, както и действия на отделни лица и групи насочени към несанкциониран достъп до класифицирана информация;

- крупни промишлени аварии и природни бедствия;

- повишен разузнавателен интерес към нашата страна свързан с членството ни в НАТО и ЕС;

Така очертаните рискове за сигурността на класифицираната информация не претендира за изчерпателност. Сферата на защита на класифицираната информация, като част от цялостната дейност по защита на националната сигурност е динамичен процес, в които намират отражение развиващите се с бързи темпове икономически, политически, научно-технически и информационни процеси.

На основата на анализ на отделните видове сигурност на класифицираната информация и на мерките включени в техния обхват се налагат няколко основни извода, които трябва да бъдат взети под внимание при планирането на действия в условията на кризисна обстановка. Основната цел е защита на класифицираната информация от нерегламентиран достъп, поради което няма значение дали кризата е в резултат на човешка дейност или е резултат на настъпили природни явления.

С цел оптимизиране на установената система за защита на класифицираната информация и привеждането и в състояние, което в максимална степен да гарантира опазването на държавните интереси в условия на кризи, е необходимо да бъдат актуализирани нормативно установените правила на отделните видове сигурност в съответствие с идентифицираните проблемни области.

Динамиката на процесите в средата за сигурност налага непрекъснат мониторинг на конкретните заплахи и уязвимости на системата. В този аспект от гледна точка на физическата сигурност на класифицираната информация е необходимо периодично отчитане на конкретните заплахи произтичащи от местоположението, ресурсите и функцията на организационната единица.

В обхвата на персоналната сигурност на касифицираната информация могат да бъдат направени следните изменения и допълнения на съществуващите правила:

- в първоначалното и текущото обучение на лицата за работа с класифицирана информация да се включи инструктаж за действия в условия на извънредни обстоятелства. Този инструктаж следва да се разработи от служителя по сигурността на информацията на базата на утвърден план за защита на класифицираната информация в условия на кризи;

Предизвикателствата в рамките на **документалната сигурност** са отчетени до известна степен в действащото законодателство, като са предвидени специални правила за достъп до помещенията на регистратурата в условия на бедствия и аварии. Необходимо е обаче тази идея да бъде доведена до определен практически резултат, като

се предвидят и последващи правила за реакция при такива ситуации. В тази връзка трябва да се предвиди задължение на служителя по сигурността на информацията да планира дейностите, които да се предприемат в организационната единица при наличие на криза. В рамките на този план план служителя по сигурността на информацията следва да разработи инструкция за евакуация на документите и материалите съдържащи класифицирана информация в условията на извънредни обстоятелства.

Мерките за противодействие на рисковете за сигурността на класифицираната информация в условия на кризи следва да са насочени към:

- усъвършенстване на нормативната уредба в областта на защитата на класифицираната информация, налага се необходимостта от по-пълно и по-конкретно регламентиране дейностите на длъжностните лица работещи с класифицирана информация в условия на кризи;

- идентифициране, анализ, оценка и прогнозиране на източниците на заплаха за защитатта на класифицираната информация;

- засилване на текущия контрол върху дейността на регистратурите получаващи, обработващи и съхраняващи класифицирана информация;

- провеждане на специално обучение на служителите по сигурността на информацията и завеждащите регистратури за действия в условия на кризи, чрез разиграване на различни кризисни сценарии за управление при кризи;

- стриктен контрол за изпълнение изискванията на системата от организационни и технически мерки в областта на физическата сигурност за предотвратяване на нерегламентиран достъп до материали, документи, техника и съоръжения класифицирани като държавна и служебна тайна;

- унифициране на дейностите по анализ на риска;

- повишаване на теоретичната и практическата подготовка на служителите работещи с класифицирана информация;

- централизъм и плановост на координацията и взаимодействието на органите отговарящи за защитата на класифицираната информация в условия на кризи;

В заключение на основата на направените оценки и изводи относно видовете защита на класифицираната информация може да се каже ще се запази тенденцията на негативното влияние на някои специфични рискове върху националната ситема за защита на класифицираната информация. Осигуряването на защитата на класифицираната информация и комуникационно-информационните системи от неправомерен достъп, използване, разкриване и разрушаване се постига чрез

прилагането на политики за сигурност, постоянна оценка и анализ на рисковете и заплахите свързани със сигурноста на информацията и прилагането на своевременни и адекватни мерки за тяхното противодействие.

ЛИТЕРАТУРА:

1. Закон за защита при бедствия, Обн. ДВ. бр.102 от 19 Декември 2006г., изм. и доп. ДВ. бр.60 от 7 Юли 2020г.

2. Закон за защита на класифицираната информация, Обн. ДВ. Бр.45/30.04.2022г., изм. ДВбр.17/2602.2019г.

3. Правилник за прилагане на Закона за защита на класифицираната информация, обн. ДВ. Бр. 115/10.12.2002г. им. И доп. ДВ. Бр. 79/08.09.2020г.

4 Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване, обн. ДВ, бр.22 /03.2003г

5. www.aip-bg.org/documents/secr_mot.htm