ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ – ВАЖЕН АСПЕКТ ОТ ДЕЙНОСТТА ПО ЗАЩИТА НА НАЦИОНАЛНАТА СИГУРНОСТ

Емине Мехмед*[*]

България направи своя исторически избор, поемайки по пътя на демократичното развитие, който стана необратим с приемането на страната, като пълноправен член на НАТО и Европейския съюз. За реализирането на тази външнополитическа цел бяха извършени редица законодателни изменения, които трябваше да приведат българското законодателство в съответствие с международните стандарти. Част от необходимите промени касаеше и преуреждането на правния режим, свързан с достъпа и защитата на информацията. През 2002 г. Народното събрание прие Закон за защита на класифицираната информация (ЗЗКИ) обн. ДВ бр. 45/30.04.2002 г. По този начин бе реализиран един от приоритетите, заложени в Концепцията за националната сигурност на Република България, а именно със специален закон да се гарантира защитата на държавния информационен ресурс от изтичане на важна за страната политическа, икономическа, научно-техническа и друга информация. Целта на закона е защитата на класифицираната информация от нерегламентиран достъп, който би създал опасност или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика, защитата на конституционно установения ред или друг правно защитен интерес.

В условията на съвременните реалности на промени в сферата на сигурността, защитата на класифицираната информация се явява важен аспект от всестранната дейност по защита на националната сигурност, в резултат на което е подложена на различни рискове и заплахи.

ЗЗКИ регламентира обществените отношения, свързани със създаването, обработването и съхраняването на класифицирана информация, както и условията и реда за предоставяне на достъп до нея. С по-

[*] *Емине Мехмед, завършила право в БСУ. От 2012 г. е адвокат към Адвокатска колегия - гр. Бургас. Автор на статии в областта на националната сигурност.*

нятието класифицирана информация се обхващат три категории информация: държавна тайна, служебна тайна и чуждестранна класифицирана информация. В изпълнение на този закон бяха приети множество подзаконови нормативни актове, регламентиращи видовете сигурност на класифицираната информация с цел изграждане на цялостна система за нейната защита.

Сигурността на класифицираната информация е комплекс от всички нормативно установени принципи, способи и мерки, гарантиращи, че класифицираната информация няма да бъде обект на нерегламентиран достъп. Поради което, защитата на класифицираната информация е система, която следва да бъде изградена и поддържана в състояние, при което са неутрализирани или поне сведени до минимум възможните заплахи.

Установената система за защита на класифицираната информация трябва да осигури опазването на относимата към сигурността на страната информация, като отговори на предизвикателствата както в мирно време, така и в условията на кризи и конфликти и положение на война. Осигуряването на защитата на класифицираната информация от нерегламентиран достъп в ситуации, различни от нормалната за системата, е показател за стабилитета 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 и конфликти.

Разработването на ефективна методология за идентифициране и управление на риска за сигурността на класифицираната информация, би допринесло за прилагането на един по-ефективен подход за противодействие на заплахите в тази особено важна област.

Защитата на класифицираната информация, като елемент от цялостната дейност по защита националната сигурност е подложена на различни рискове и заплахи. Те условно могат да бъдат разделени на външни и вътрешни. Външните заплахи са свързани с действия на чужди специални служби, международни организации, вкл. терористични и отделни лица, насочени към осъществяване на нерегламентиран достъп до класифицирана информация, свързана основно с външ-

ната политика, отбраната, икономиката и сигурността на Република България, а също така и използването на нови информационни технологии за осъществяване на нерегламентиран достъп. Вътрешните заплахи включват възможното осъществяване на нерегламентиран достъп, в резултат на неспазване на принципа „необходимост да се знае" и непознаване на нормативната база, уреждаща защитата на класифицираната информация, вкл. чуждестранната, нарушаване на работата на автоматизираните информационни системи или мрежи, които пренасят информация, настъпването на природни бедствия и крупни промишлени аварии, и др.

Обекти на сигурността на информацията са носителите, намиращи се в държавните органи и техните поделения, органите на местното самоуправление, подразделенията на Българската армия, въоръжените сили, службите за сигурност и обществен ред, юридическите и физическите лица с търговска цел, публичноправните субекти, които по законоустановения ред създават, обработват, съхраняват, предоставят за ползване и ползват информация свързана със защита на държавни и обществени интереси, както и интересите на страната, които тя се е задължила да защитава по силата на международен договор. Към тези обекти спадат:

- системата от пунктове за управление при кризи в Република България (центрове за събиране, анализ и оценка на информацията, системите за оповестяване и др.);
- системите на създаване, съхраняване, пренасяне и използване на информацията, свързана със защитата на държавния и обществения интерес, включваща в себе си автоматизираните информационни системи или мрежи, архиви и база данни, регламентите и процедурите за получаване, обработване, съхранение и пренасяне на тази информация;
- системите за свръзка и автоматизираните системи за управление на въоръжените сили и тяхното информационно осигуряване;
- предприятията на военно-промишления комплекс, съдържащи данни за научно-техническия и производствен потенциал и запасите от стратегически видове суровини и материали.

Рисковете за сигурността на класифицираната информация са реално съществуващи заплахи и вероятността от тяхното възникване и проявление. Систематизирането им и извършването на последващ

анализ и оценка са необходимите предпоставки за планиране и осъществяване на дейностите по тяхното локализиране и ограничаване.

Класифицирането на информацията, съответно прилагането по отношение на конкретна информация мерки за защита предвидени в ЗЗКИ и подзаконовите актове по неговото прилагане, е резултат от целенасочената защита на нормативно установен държавен интерес. Прилагането на мерките за защита на класифицираната информация е насочено към това да се предотвратява настъпването на нерегламентиран достъп до съответната информация. Следователно защитата на класифицираната информация следва да се разбира, като система, която трябва да бъде изградена и поддържана в състояние, при което са неутрализирани или поне сведени до минимум възможните заплахи, които я дестабилизират.

Ако нивото на риск за организацията е определено като високо, налице е остра необходимост от предприемане на мерки за коригиране на системата за сигурност на класифицираната информация. Съществуващата система може да бъде прилагана, като максимално бързо трябва да се приложи план с коригирана система от мерки за сигурност на класифицираната информация.

При средно ниво на риск е необходимо прилагане на мерки за коригиране на параметрите на системата за сигурност на класифицираната информация и трябва да бъде разработен план с коригиращи мерки, който да бъде приложен в близък период от време.

При ниско ниво на риск висшият управленски екип трябва да определи дали е необходимо прилагането на мерки за коригиране на параметрите на системата за сигурност на класифицираната информация или да реши риска да бъде приет.

Разработването на препоръки за необходимите действия за коригиране на системата от защитни механизми и процедури е заключителният етап на анализа и оценката на риска.

При разработването на препоръки за коригиране на системата от мерки, целящи минимизиране или елиминиране на идентифицираните рискове, трябва да се отчитат редица фактори като: ефективност на препоръчаните опции; съответствие на законодателните и административни норми на организационната политика; влияние върху функционалността на организацията; сигурност и надеждност и др.

Допълнителен фактор за оценка целесъобразността от прилагането на мерки за коригиране на компонентите на системата за сигурност на класифицираната информация е и факторът цена – полза. Тази оценка трябва да бъде осъществена с цел недопускане прекомерно го-

лям разход на ресурси за постигане на незначителен ефект относно редуциране на риска. 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.

Бихме могли да кажем, че физическата сигурност е сред най-уязвимите части от цялостната система за защита на класифицираната информация. В същото време физическите мерки са само един аспект от цялостната защита на класифицираната информация. В условията на извънредни ситуации твърде често възникват непредвидими, от гледна точка на физическата сигурност обстоятелства.

От практиката се налага изводът, че поради липсата най-вече на финансови средства, а не рядко и поради липса на необходимия сграден фонд, за изграждане на регистратури за класифицирана информация в съответствие с нормативно установените изисквания, мерките за физическа сигурност на класифицираната информация са значително занижени.

При наличието на подобни уязвимости в системата за физическа сигурност на класифицираната информация в условията на военно 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.

Сферата на защита на класифицираната информация, като част от цялостната дейност по защита на националната сигурност не е статично явление, а е динамичен процес, в който намират отражение развиващите се с бързи темпове икономически, политически, научно-технически и информационни процеси.

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 война, военно или друго извънредно положение, е необходимо да бъдат изменени и допълнени нормативно установените правила на отделните видове сигурност в съответствие с идентифицираните проблемни области.

Динамиката на процесите в средата за сигурност налага непрекъснато актуализиране и отчитане 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. Служителят по

сигурността на информацията следва да разработи специален план за действие в условията на война, военно или друго извънредно положение. Този план трябва да бъде съобразен с анализа на риска за съответната организационна единица. Целесъобразно е разработването на инструкция за работа в зоните за сигурност и инструкция за работа на дежурните по отношение на охраната на тези зони при война, военно или друго извънредно положение.

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 война, военно или друго извънредно положение.

- Увеличаването или намаляването на уязвимостите на националната система за защита на класифицираната информация в условия на война, военно или друго извънредно положение до голяма степен зависи от идентифициране на рисковете за отделните видове сигурност на класифицираната информация при изграждането на отделните им елементи.
- Идентифицирането на рисковете и уязвимостите в областта на защитата на класифицираната информация изисква в процеса на анализ на риска да бъдат моделирани всички възможни ситуации, които биха възникнали при различни извънредни ситуации, и които биха довели до нерегламентиран достъп до класифицирана информация.
- При война, военно или друго извънредно положение системата от организационни, технически и физически мерки за предотвратяване на нерегламентиран достъп до материали и документи, съдържащи класифицирана информация може да включва и повишаване нивото на сигурност на нейното пренасяне, чрез куриери оборудвани със специални автомобили за пренасяне на информацията, изграждане на регистратури в изнесените защитени пунктове за управление на всички равнища на държавното управление.
- В областта на индустриалната сигурност, с цел намаляване уязвимостите на националната система за защита на класифицираната информация, се налага необходимостта още в условия на стабилна среда да бъдат проучвани специализирани фирми и търговски дружества, имащи предмет на дейност оборудване

на техника за действия при бедствия, крупни промишлени и производствени аварии в области от национално значение, да бъдат проучвани в областта на индустриалната сигурност.

- Информационната сигурност заема важно място за оптималното протичане на процеса на управление при кризи от военен характер. В този контекст нараства ролята на изградената в Република България единна информационна среда за пренос на класифицирана информация между структурите на държавната администрация в страната.

***Използвана литература*:**

1. Бахчеванов, Г., и кол., Управление при кризи и конфликти, изд. „Софтрейд”, С., 2005 г.
2. Гочев, А. и колектив, Ранно сигнализиране и предотвратяване на конфликти. С., 1997 г.
3. Задължителни указания относно служителя по сигурността на информацията, Решение на ДКСИ №3/25.02.2003 г.
4. Задължителни указания относно съдържанието на учебната програма за провеждане на обучение в областта на защитата на класифицираната информация, Решение на ДКСИ №46/26.08.2003 г.
5. Закон за защита на класифицираната информация, Обн. ДВ. бр.45/30. 04. 2002 г., изм. ДВ. бр. 16 от 26. 02. 2010 г.
6. Закон за защита при бедствия, Обн. ДВ. бр.102 /19. 12. 2006 г., изм. ДВ. бр.93 от 24 11.2009 г.
7. Закон за министерството на вътрешните работи, Обн., ДВ, бр. 17 от 24.02. 2006 г., изм. ДВ. бр.93 от 24.11. 2009 г.
8. Манев, М., Процедури за управление на кризи, С., Военен журнал, кн. 5, 2001 г.
9. Маркова, Ц., Доклад за цялостната дейност по състоянието на защита на класифицираната информация в Република България през 2006 г.
10. Найденов, Б., Дж. Хайденрих. Национална сигурност и военна доктрина, С., 1999 г.
11. 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.22/11.03.2003 г.
12. Павлов, Г., „Управление при кризи – проблеми и перспективи”, сп., Икономически алтернативи, бр.4/2006 г.

13. Правилник за прилагане на ЗЗКИ. Обн., ДВ, бр. 115/10.12.2002 г., изм. ДВ. бр. 5/ 19.01.2010 г.
14. Правилник за прилагане на ЗМВР. Обн., ДВ, бр. 47/09.06.2006 г., изм. ДВ. бр. 5/ 19.01.2010 г.
15. Ралчев, Г., Трифонов, Т., Търкаланов, Ю., Преходът, фондация „Национална и международна сигурност", С., 2005 г.
16. Решение на Съвета от 23 септември 2013 година относно правилата за сигурност за защита на класифицирана информация на ЕС (2013/488/ЕС).
17. Семерджиев, Ц., Информационна война, Софттрейд, С., 2000 г.
18. Илиева Д. Само новите High Tech ли са новите технологии в образователния процес? – В: Нови информационни технологии в образователния процес. Доклади и съобщения от Осмия научен семинар на УниБИТ, проведен в Камчия на 15-18.06.2013, (под печат);
19. Илиева Д. Ядро концепта „власть" и его приядерная зона со смысловым концептом „*господство*" сквозь призму болгарских паремий. – В: Международная научная конференция „Слово. Текст. Время – XII Фразеология в идиолекте и системе славянских языков. К 200-летию со дня рождения Т.Г. Шевченко. Щецин, Польша, 14-17 ноября 2013 (в печати)
20. Илиева Д. И. За същността на концепта.// 70 години българска академична лексикография. Доклади от VI национална конференция с международно участие по лексикография и лексикология, с. 527- 535, С., 2013, ИБЕ – БАН, Акад. Издателство „Проф. Марин Дринов", ISBN 978-954-322-578-1, 653с.
21. Илиева Д.И. Истина про правду и истину (сквозь призму болгарской и русской языковой личности). – В: Ростов на Дон. Южно-Российские научные чтения – 2013. Южный федеральный университет. Факультет филологии и журналистики. Язык как система и деятельность – 4. Материалы Международной научной конференции. с. 128 – 132, Изд-во Foundation, Ростов-на-Дону, 2013, ISBN 978-5-4376-0091-7.

РЕЗЮМЕ

В условиях современных реальностей перемен в сфере безопасности, защита классифицированной информации является важным аспектом всесторонней деятельности по защите национальной безопасности, в результате чего защита подвержена на разные риски и угрозы. Акцент ставится на безопасность классифицированной информации, которая комплексно состоит из нормативноустановленных принципов, способов и мер, гарантирующих, чтобы классифицирванная информация не стала бы объектом нерегламентированного доступа. Вследствие этого, защита классифицированной информации есть система, котороя должна быть построена и поддерживана в таком состоянии, при котором возможные угрозы могли быть нейтрализованы или доведены до минимума.

Созданная система для защиты классифицированной информации должна обеспечить охрану соответствующей к безопасности страны информации, ответив на вызовы как и в мирное время, так и в условиях кризиса и конфликтов и во время войны.

Обеспечение защиты классифицированной информации от нерегламентированного доступа в ситуациях, отличающихся от нормальной для системы, есть индикатор устойчивости и универсальной применимости прогнозированных принципов, способов и мер, а также и индикатор эффективного функционирования органов.

Разрабатывание эффективной методологии для идентифицирования риска и им управления и для безопасности классифицированной информации, способствовало бы применять более эффективный способ в борьбе с угрозами в этой важнейшей области.

SUMMARY

In the present-day reality of changes in the field of security, the protection of classified information is an important aspect of the versatile activity of ensuring national security, as a result of which it is exposed to various risks and threats. The accent is placed on the security of classified information, which is a complex of all statutory principles, means and measures that guarantee that classified information will not be the object of unauthorised access. Therefore, the protection of classified information is a system, which should be established and maintained in a condition where the possible threats are neutralised or at least limited to their minimum.

The established system of protection of classified information must ensure the safeguarding of the information related to national security, while addressing the challenges both in peaceful times and in times of crises, conflicts and wars.

Ensuring the protection of classified information from unauthorised access in situations other than those, which are customary for the system, is an indicator of the stability and the universal applicability of the envisaged principles, means and measures and of the efficient functioning of the responsible authorities.

The design of an efficient methodology to identify and manage the risk related to classified information security will contribute to the application of a more efficient approach to counteract the threats in this field of particular importance.