

# ИНДЕНТИФИКАЦИЯ И ОЦЕНКА НА РИСКА ОТ ТЕРОРИСТИЧНИ ДЕЙСТВИЯ В КРИТИЧНИ ИНФРАСТРУКТУРНИ ОБЕКТИ ОТ ЗНАЧЕНИЕ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

**подполковник д-р Данаил Петев**  
Военна академия „Г. С. Раковски“

**Абстракт:** В статията се разглеждат същността и целите на явлението тероризъм, основните причини, способстващи възникването му, и дейностите в борбата срещу него. Разкрит е процесът по управление на риска от терористични действия. Разгледани са алтернативни подходи за превенция от терористична заплаха. На базата на системния анализ и методологията за управление на риска се изследват теоретичните основи на критичността и уязвимостта на критичната инфраструктура. Представена е координацията в дейностите на институциите в борбата срещу тероризма във връзка с националната сигурност.

**Ключови думи:** тероризъм; терористична дейност; управление на риска; анализ на риска; критичната инфраструктура; организирана престъпност

## Увод

Асиметричните заплахи (особено международният тероризъм и разпространението на оръжия за масово унищожение), регионалните конфликти, киберпрестъпността и трансграничната организирана престъпност оказват съществено влияние върху средата на сигурност в глобален и регионален мащаб.

Радикализацията и тероризмът ще продължат да генерират заплахи. Регионалните конфликти и икономическите и финансовите кризи допълнително изострят тази заплаха<sup>1</sup>.

Терористичният риск<sup>2</sup> за Европа от религиозно мотивирани групировки се увеличава вследствие на благоприятната среда за разпространяване на идеите на радикални идеологии основани на исляма сред общностите в Западна Европа и на Балканите. Процесът се подпомага от създадените в Близкия изток и Северна Африка логистични бази и завръщащите се от конфликтните зони чуждестранни бойци, които притежават реален боен опит. Терористичните организации паралелно с децентрализацията на структурите и разнообразяването на способите си за действие умело експлоатират възможностите за инфилтриране на свои членове в демократичните общества и привличане на нови привърженици.

Към момента тероризмът се определя като вид обществен конфликт, явление в обществения живот. Различава се от обикновената криминална престъпност по своите цели. Целта на тероризма не се постига с резултата, получен вследствие на извършването на едно или повече престъпления. Много експерти в областта на тероризма го характеризират като „насилие с политически цели“, „насилие (...) за осъществяване на политически, религиозни и етнически стремежи“. Причини, способстващи възникване на тероризма и провеждане на терористични акции, са въоръжените конфликти и войни, недоволството от политическата система, недоволството и несъгласието с определени политически решения, сепаратизъм и контра сепаратизъм, търсенето на историческо възмездие за понесени поражения в миналото и др.

## Основна част

### ***1. Координация в дейностите на министерствата и ведомствата в борбата срещу тероризма във връзка с националната сигурност***

Анализът на средата за сигурност е съществен фактор при идентифициране и оценка на потенциалните заплахи, насочени срещу стратеги-

чески обекти и дейности от значение за националната сигурност на Република България.

Изпълнението на политиката за национална сигурност се осъществява от органите на централната и териториалната изпълнителна власт. Органите на местното самоуправление и на местната власт, както и тези на съдебната допринасят съобразно своите компетенции за реализирането на политиката за сигурност. Ефективността на системата зависи от взаимното доверие и сътрудничество между държавните институции, частния сектор, неправителствените организации и гражданите, а също така и със страните партньори за обмен на информация и съвместни действия.

В Република България задачите и отговорностите на институциите по противодействие на тероризма и овладяване на последствията от терористични актове произтичат от Закона за противодействие на тероризма (ЗПТ), нормативните документи, уреждащи тяхната дейност и взаимодействието им с други държавни и недържавни субекти. Министерствата, ведомствата и органите на местната власт изпълняват задачите си съгласно своите планове за действие, заповедите и разпорежданията на съответните ръководители.<sup>3</sup>

Стратегическите обекти и дейности, които са от значение за националната сигурност на Република България, се определят от Министерския съвет в единен списък по предложение на съответните министри или ръководители на ведомства след предварително съгласуване с председателя на Държавна агенция „Национална сигурност“ (ДАНС). Тези обекти и дейности са част от критичната инфраструктура на страната.<sup>4</sup>

На политическо ниво координацията на дейностите в борбата срещу тероризма се осъществява от Съвета по сигурността към Министерския съвет, който организира и координира дейността на министерствата и ведомствата във връзка с националната сигурност, включително борбата срещу тероризма. На експертно ниво функциите на национален координатор по противодействието на тероризма се изпълняват от Националния контра-терористичен център, разположен в ДАНС, който предоставя информация в непрекъснат денонощен режим на компетентните органи и структури, необходима за предотвратяване и пресичане на заплахи от тероризъм.<sup>5</sup>

## ***2. Процес по управление на риска на критичната инфраструктура<sup>6</sup> от терористични действия***

На основата на системния анализ и методологията за управление на риска<sup>7</sup> се изследват: теоретичните основи на критичността и уязвимостта

на критичната инфраструктура; определянето на рисковите индикатори, анализа и оценката на риска; управлението на процесите на риска и кризата с моделите на терористичните удари от използването на оръжие за масово унищожение (ОМУ) и промишлени опасни аварии (ПОА) по критичните обекти. Съгласно стратегията на тероризма най-добрата цел е най-уязвимият обект. Поради тази причина контролът на уязвимостта има съществена роля при противодействието на тероризма. Уязвимостта е слабост, която носителят на заплахата може да използва за нанасяне на вреди. Тя е функция от няколко фактора – атрактивност на обекта, осъществимост за извършване на атака и потенциалното въздействие

През април 2007 г. Съветът на Европейския съюз прие заключения относно Европейската програма за защита<sup>8</sup> на критичните инфраструктури. В тях отново изтъкна, че държавите членки носят крайната отговорност за управлението на механизмите за защита на критичните инфраструктури в рамките на техните национални граници. Същото така приветства усилията на Комисията за разработване на европейска процедура за установяване и означаване на европейски критични инфраструктури<sup>9</sup> (ЕКИ) и за оценка на необходимостта от подобряване на тяхната защита. Държавите членки и собствениците/операторите на ЕКИ<sup>10</sup> носят първична и крайна отговорност за тяхната защита.

За установяването на потенциални ЕКИ се прилагат междусекторни и секторни критерии. Междусекторните критерии са:

1. потенциален брой на загиналите или ранените;
2. икономически последици – оценява се значимостта на икономическите загуби и/или влошеното качество на продукти или услуги, включително възможните последици за околната среда;
3. обществени последици – оценяват се последиците за общественото доверие, физическото страдание и нарушаването на ежедневието, включително загубата на основни услуги.

Праговите стойности на междусекторните критерии, определени за всеки конкретен случай от компетентния министър съгласувано със заинтересуваните държави – членки на Европейския съюз (ЕС), се основават на степента на нарушаване или на унищожаване на дадената инфраструктура. Секторните критерии са определени с Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита и отчитат характеристиките на отделните сектори с ЕКИ. Съдържанието на критериите е класифицирана информация.<sup>11</sup>

В общността съществуват определен брой критични инфраструктури, чието нарушаване или унищожаване би довело до значителни трансгранични последици. Това включва трансгранични последици за повече от един сектор като резултат от взаимозависимостта между свързани помежду си инфраструктури. Подобни ЕКИ следва да бъдат установени и означени по обща процедура. Оценяването на изискванията за сигурност за подобни инфраструктури следва да се извърши съгласно минимален общ подход. Двустранните механизми на сътрудничество между държавите членки в областта на защитата на критичните инфраструктури представляват едно добре установено и ефикасно средство за защита на трансграничните критични инфраструктури. Европейската програма за защита на критичните инфраструктури следва да се основава на този вид сътрудничество. Информацията, свързана с означаването на определена инфраструктура като ЕКИ, следва да се класифицира в съответствие със съществуващото законодателство на Общността и на държавите членки.

Тенденцията в усъвършенстването на методологията на риска се преориентира от защитното усилие на управляващия орган от положение на неблагоприятната „реакция в момента“ към „изпреварваща превенция“ на рисковата обстановка. Това е съвременен израз на овладяване на развитието на рисковия процес. Впоследствие чрез прякото управление на неговия механизъм се насочва рисковото развитие към минимизиране на въздействията и ликвидиране на риска.

Управлението на риска при терористични действия включва:

- идентификация на риска;
- оценка на риска от реализиране на терористичен акт;
- разработка на препоръки за намаляване на риска.

При идентификация на терористична заплаха следва да се определят какви функционални зони и помещения в тях изискват по-сериозен анализ, кои представляват по-малък интерес от гледна точка на терористична заплаха. Един от основните въпроси за решаване в началото на процеса по управление на риска е степента на неговата централизираност, респективно децентрализираност. „Основна цел на изучаването на риска и рисковите събития е създаване на условия за тяхното управление, което на практика е процес, съдържащ етапите на планиране, идентификация и анализ на рисковите области<sup>12</sup>, разработване на техники за въздействие върху риска, наблюдение на риска и определяне как се променя под въздействието на избраната техника и документиране на цялостната програма за управление на риска “.<sup>13</sup>

Управлението на риска от терористични действия и плановете за управление при кризи вследствие на терористични действия освен на национално ниво се изработват и действат и на общинско ниво. Структурите на министерствата и ведомствата на териториите на общините изпълняват задачите си съгласно своите плановете за управление (действие) при бедствия, заповедите и разпорежданията на съответните ръководители. Такива структури имат Министерството на вътрешните работи, Главна дирекция „Пожарна безопасност и защита на населението“, Министерството на здравеопазването (МЗ), Министерството на отбраната (МО), Министерството на земеделието и храните.<sup>14</sup>

### Заклучение

Важен фактор за управлението на риска при терористична заплаха е превенцията, чрез която се ограничават неприятните изненади, когато инцидентът внезапно настъпи и няма време за дълго обмисляне на действията или да се взимат неинформирани и импровизирани решения вследствие на недостига на време и обмисляне преди реагиране. Управлението на риска при терористични действия върху критичната инфраструктура е система от експертни дейности свързани с анализиране, ръководство и контрол на процесите на развитие. В тази връзка защитата на обектите от критичната инфраструктура трябва да отговаря на комплексните изисквания за сигурност, произтичащи от задачите, свързани с ЕС и НАТО, превръщането на Република България в комуникационен, енергиен и транспортен възел.

### БЕЛЕЖКИ

1. Заплаха – нанасяне на материални и нематериални вреди на населението (обекти на заплахата или цели) от лица, групи или организации (носител на заплахата). Анализът на заплахата изследва два ключови фактора: обекта на заплахата (целта) и носителя на заплахата. Накратко – „заплаха“ е събитие, инцидент или декларация за намерение за причиняване на нараняване, увреждане или друго враждебно действие като вземездие – бел. авт.

2. Риск – възможността да настъпи събитие, което ще повлияе върху постигане на приетите (планираните) цели на структурата (организацията). Рискът се измерва с неговото влияние и вероятност за проявление – бел. авт.

3. МИНИСТЕРСКИ СЪВЕТ. Съвет по сигурността, 2022. Закон за противодействие на тероризма. *Държавен вестник*, бр. 103 от 27 декември 2016 г. [посл. изм. и доп., бр. 32 от 26 април 2022 г.].

4. МИНИСТЕРСКИ СЪВЕТ, 2009. Постановление № 181 за определяне на стратегическите обекти и дейности, които са от значение за националната сигур-

ност. *Държавен вестник*, бр. 59 от 28 юли 2009 г. [посл. изм. и доп., бр. 70 от 20 август 2024 г.].

5. МИНИСТЕРСКИ СЪВЕТ. Съвет по сигурността, 2022. Закон за противодействие на тероризма. *Държавен вестник*, бр. 103 от 27 декември 2016 г. [посл. изм. и доп., бр. 32 от 26 април 2022 г.].

6. Критична инфраструктура – елемент, система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни последици за Република България в резултат на невъзможността да се запазят тези функции.

7. Управление на риска – процес, при който се изследва, анализира и проследява развитието на съществуващите рискове с цел да се намали негативният ефект от евентуалното им настъпване или да се предостави възможност за възползване от тяхното настъпване.

8. Защита – всички дейности, целящи гарантиране на нормалното функциониране, непрекъснатостта и целостта на критичните инфраструктури с цел възпиране, намаляване, смекчаване или неутрализиране на заплахите, рисковете или уязвимостта им.

9. Европейска критична инфраструктура – критична инфраструктура, разположена на територията на Република България, чието повреждане или разрушаване би оказало съществено негативно влияние върху поне още една държава, членка на ЕС. Значимостта на това негативно въздействие се оценява чрез взаимосвързани критерии, които включват последици, загуби или щети, произтичащи от междусекторни зависимости, свързани с безопасността и сигурността на инфраструктурата на енергетиката, на транспорта или на други видове инфраструктура.

10. Собственици/оператори на европейски критични инфраструктури са физически лица, юридически лица или организации, които отговарят за инвестирането във или за нормалното функциониране, непрекъснатостта и целостта на определен елемент, система или част от тях, означени като ЕКИ.

11. МИНИСТЕРСКИ СЪВЕТ. Съвет по сигурността, 2022. Закон за противодействие на тероризма. *Държавен вестник*, бр. 103 от 27 декември 2016 г. [посл. изм. и доп., бр. 32 от 26 април 2022 г.].

12. Анализ на риска – отчитане на съответните сценарии за действие при различни потенциални заплахи с цел да се извърши оценка на уязвимостта и на евентуалните негативни последици от нарушаването или унищожаването на дадена критична инфраструктура.

13. МИНИСТЕРСКИ СЪВЕТ, 2012. Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях. *Държавен вестник*, бр. 81 от 23 октомври 2012 г. [посл. изм. и доп., бр. 27 от 5 април 2016 г.].

14. МИНИСТЕРСКИ СЪВЕТ, 2023. Национален план за противодействие на тероризма. (Решение № 564 от 24.08.2023 г.) Портал за обществени консултации. [Онлайн]. Достъпно на: <https://www.strategy.bg>.

15. МИНИСТЕРСКИ СЪВЕТ, 2011. Постановление № 18 за установяването и означаването на европейски критични инфраструктури в Република България и мерки за тяхната защита. *Държавен вестник*, бр. 11 от 4 февруари 2011 г.

16. НАРОДНО СЪБРАНИЕ, 2018. Актуализирана Стратегия за национална сигурност на Република България. *Държавен вестник*, бр. 26 от 23.03.2018 г.

17. СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪЮЗ [официален сайт], 2008. Директива 2008/114/ЕО на Съвета от 8 декември 2008 година относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита. EUR lex. [Онлайн] Достъпно на: <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32008L0114>.

## IDENTIFICATION AND ASSESSMENT OF THE RISK OF TERRORIST ACTIVITIES IN CRITICAL INFRASTRUCTURE OBJECTS OF NATIONAL SECURITY SIGNIFICANCE

**Abstract:** The article examines the essence and goals of the phenomenon of terrorism, the main reasons contributing to its emergence and the activities in the fight against it. The process of managing the risk of terrorism is revealed. Alternative approaches to terrorist threat prevention are explored. On the basis of system analysis and risk management methodology, the theoretical foundations of criticality and vulnerability of critical infrastructure are explored. The coordination in the activities of the ministries and departments in the fight against terrorism in relation to national security is presented.

**Keywords:** terrorism; terrorist activity; risk management; risk analysis; critical infrastructure; organized crime

**Lieutenant Colonel Dr. Danail Petev, Assoc. Prof.**

ORCID iD: 0000-0002-6495-2268

Emergency Management Department

Command and Staff Faculty

Rakovski National Defence College

82, Evlogi i Hristo Georgievi Blvd.

1504 Sofia, Bulgaria

E-mail: d.petev@rncd.bg