

ПРОЦЕС НА ЗАЩИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА НА ГЕРМАНИЯ

ас. д-р Теодора ГЕЧКОВА,
Университет за национално и световно стопанство

Ass. Prof. Teodora GECHKOVA, PhD
University of National and World Economy

Резюме: Централно място в доклада заема защитата на критичната инфраструктура по примера на Германия. Германия активно разглежда въпросите по защитата на критичната инфраструктура, като се ръководи от принципа на съвместните действия от страна на държавата, обществото, бизнеса и индустриалния сектор. Като критична инфраструктура може да бъде определена всяка, която поради структурни, функционални или технически заплахи може да загуби своята позиция в рамките на цялостната система от сектори на критичната инфраструктура – резултат от взаимозависимостта на елементите.

Ключови думи: защита, критична инфраструктура, Германия.

Summary: The protection of critical infrastructure in the example of Germany takes central position in the report. Germany actively considers the issues on protection of critical infrastructure, guided by the principle of joint action by the state, society, business and industrial sector. Any infrastructure can be defined as critical if, due to structural, functional or technological threats it can lose its position within the overall system of sectors of critical infrastructure – the result of the interdependence of the elements.

Keywords: defense, critical infrastructure, Germany.

Германия представлява федерална парламентарна република (форма на държавно управление, при която начело на държавата се избира длъжностно лице, назначено с определен мандат. Водеща роля има Парламентът). В редица области на науката и техниката, страната заема водеща позиция в света. Най-големият износител и втори по големина вносител на стоки¹. Ето защо, изследването на процеса на защита на критичната инфраструктура представлява интерес за настоящата разработка.

Страната представлява „Федерация на 16 федерални провинции. Две от тях (Хамбург и Берлин), имат статут на свободни градове, а градът-провинция Берлин е обявен за федерална столица. Останалите провинции се разделят на 439 окръга, като пет от провинциите се делят и на общо 22 административни области, обединяващи няколко окръга². Страната членува в Групата на осемте (Г-8),³ Групата на двайсетте

¹ Луканов, А., Божинов, Н., Димитров, Ст., *Справочник на страните по света*, изд. „Образование и наука“, С. 2001 г., стр. 40;

² Пак там;

³ Група от 8 икономически най – големи държави в света – Великобритания, Германия, Италия, Канада, Русия, САЩ, Франция и Япония, които заедно представляват около 65 % от БВП в света;

(Г-20)⁴, НАТО (Международна организация за военно сътрудничество) и ООН (Международна организация, целяща опазване на световния мир).

Инфраструктурата, в частност критичната инфраструктура, е неразделна част от всяко едно модерно и бързо развиващо се общество. Германия се нарежда сред водещите страни в Европа в индустриално и технологично отношение, което я прави силно зависима от една добре защитена и функционираща инфраструктура. Ето защо, процесът за гарантиране сигурността на критичната инфраструктура е ключова функция на националната сигурност на страната, което е свързано с извършването на превантивни мерки, предприети от Правителството и частния сектор, и е централна, основна тема, в политиката за сигурност на страната.

Германия определя критичната инфраструктура като „организационни и физически структури и съоръжения, които имат жизнено важно значение за нормалното функциониране на икономиката и обществото, като влошаването или прекъсването на нормалното им функциониране би довело до значително нарушаване на обществената сигурност и безопасност, до траен недостиг на основни стоки и услуги или до други драматични последици.”⁵

Дейностите по гарантиране сигурността на критичната инфраструктура на страната се регламентират от Национална стратегия за защита на критичната инфраструктура на Германия. Документът определя „от една страна целите на федерално-административно ниво, които се прилагат в практиката, като се базира на политико-стратегическия подход, а от друга, представлява отправна точка за укрепване на постигнатите до момента резултати, както и по-нататъшното им развитие, с оглед появяващите се нови предизвикателства в средата за сигурност”⁶.

Германия активно разглежда въпросите по защитата на критичната инфраструктура, като се ръководи от принципа на съвместните действия от страна на държавата, обществото, бизнеса и индустриалния сектор. Казано по друг начин, държавата изпълнява ролята на модератор (ръководител), като урежда мерките за опазване на цялостната система по гарантиране сигурността на инфраструктурата. Изпълнението на дейностите от страна на бизнеса са на доброволен принцип, чрез включването им в редица правни разпоредби, което с течение на годините е довело до постигането и поддържането на изключително високо ниво по отношение на гарантиране сигурността на националната критична инфраструктура. За да се поддържа това ниво в бъдеще, с оглед непрекъснато променящите се условия в средата за сигурност, страната постоянно задълбочава подхода на доверие и конструктивно сътрудничество по пътя на цялостната защита на инфраструктурата.

Националната стратегия за защита на критичната инфраструктура идентифицира следните девет сектора, които определят състава на системата:

- сектор „Телекомуникационни и информационни технологии”;
- сектор „Енергетика”, в т.ч. доставка на електроенергия, нефт и газ;

⁴ Група от 19 страни с най – големи икономики плюс ЕС, в която участват финансови министри и управители на централни банки, с цел сътрудничество и консултация в областите на международната финансова система, глобалната икономика и други икономически сфери.

⁵ National Strategy for Critical Infrastructure Protection Germany, Berlin, 17th June 2009.

⁶ Пак там.

- сектор „Банкиране, финанси и застраховане”;
- сектор „Транспортни системи”;
- сектор „Водоснабдяване и канализация”;
- сектор „Обществено здравеопазване” – включително доставка на основни хранителни продукти;
- сектор „Аварийни и спасителни служби” – дейности по управление в извънредни ситуации;
- сектор „Правителство и публична администрация” – полиция, митници и въоръжени сили;
- сектор „Медии и културно наследство”.

Всяка инфраструктура се определя за „критична”, когато тя е „от жизненоважно значение за нормалното функциониране на съвременното общество и всяка повреда би довела до трайни смущения в общата система.”⁷

Според германското законодателство, терминът „критичност” се определя като „относителна мярка на значението на дадена инфраструктура от отношението на въздействието на нейното разрушаване или функционална недостатъчност, при осигуряване на доставките за обществото от основни стоки и услуги.”⁸

Критичността може да се отнася както за инфраструктури със символен характер, така и за такива, които съдържат различни физически елементи. Като критична инфраструктура може да бъде определена всяка, която поради структурни, функционални или технически заплахи може да загуби своята позиция в рамките на цялостната система от сектори на критичната инфраструктура – резултат от взаимозависимостта на елементите. Пример за такава взаимозависимост могат да бъдат посочени в секторите „Енергетика” и „Телекомуникационни и информационни системи”, които в зависимост от големината и гъстотата на съответните им мрежи, са от особено значение за нормалното функциониране на обществото. Едно продължително прекъсване на доставките на този вид услуги, би имало сериозно негативно влияние върху обществената сигурност и безопасност.

Една инфраструктура може да притежава символна критичност, ако нейното унищожаване би довело до чувство за загуба на националната идентичност.

По отношение на техните технически, структурни и функционални особености, секторите на критичната инфраструктура могат да бъдат класифицирани от една страна като жизненоважни (абсолютно задължителни), технически основани сектори, а от друга –като жизненоважни (абсолютно задължителни) сектори, осигуряващи социално-икономически услуги. Могат да бъдат разгледани в табл.1.

Таблица 1.

Технически базирани сектори	Сектори, осигуряващи социално-икономически услуги
Сектор „Енергетика”	Сектор „Здравеопазване”
Сектор „Телекомуникационни и информационни технологии”	Сектор „Аварийно – спасителни служби”
Сектор „Транспортни системи”	Сектор „Правителство и публична

⁷ Пак там.

⁸ Пак там.

	администрация”
Сектор „Водоснабдяване и канализация”	Сектор „Банкиране, финанси и застрахователно дело”
	Сектор „Медии и културно наследство”

Източник: Национална стратегия за защита на критичната инфраструктура на Германия

Значителна е взаимозависимостта между технически базираните сектори и такива, осигуряващи основни обществени услуги, тъй като до голяма степен, почти всички социално-икономически инфраструктури разчитат на неограничените възможности на техническите средства.

Критичната инфраструктура на Германия е изцяло базирана на технологичния прогрес, който страната реализира непрекъснато.

По отношение на гарантиране сигурността на критичната инфраструктура, страната показва добри резултати не само в количествено, но и в качествено отношение. Като пример може да бъде даден процесът по гарантиране осигуряването на доставки на основни стоки и услуги – вече няколкократно бе споменато, че това е един от основните приоритети на държавната политика на страната. Това се дължи на факта, че частните транспортни дружества са правно задължени да осигуряват сигурна и надеждна мрежа от доставки. В сектор „Енергетика” доставките се извършват в съответствие със Закон за доставка на електроенергия, а контрола по качеството се извършва с помощта на периодични технически проверки и мониторингови доклади.

Подобно на сектор „Енергетика”, доставките в сектор „Телекомуникации” също са обект на правни разпоредби, като се цели предотвратяване на неоторизиран достъп и/или умишлено прекъсване на доставките. Освен това, операторите на телекомуникационни и информационни системи са длъжни да определят заплахите, които биха могли да се очакват, което изисква планирането и предприемането на различни защитни мерки.

През последните години, почти всички сфери на обществения живот на страната се характеризират с взаимосвързаност и взаимозависимост. Проблеми, които определят действията по защитата на критичната инфраструктура не само в Германия, но и в почти всички страни по света. Следователно всички аспекти на сигурността играят важна роля във всяка една конкретна област. Още в края на 1990 г., Федералното правителство си поставя като приоритетна задача защитата на критична инфраструктура, което я превръща в ключов елемент от националната сигурност на страната. В това отношение, решаването на междусекторните въпроси са от съществено значение за управлението на съответния сектор, извършвано от съответните ресорни министерства, част от системата.

В процесът на защита на критичната инфраструктура, Федералното министерство на вътрешните работи осигурява междуведомствена координация по отношение на мерките, предприемани на национално ниво.

Министерство на вътрешните работи в сътрудничество с Федералната агенция за гражданска защита и помощ при бедствия; Федералната служба за информационна сигурност; Федерална служба „Криминална полиция” и Федералния институт „Техническо осигуряване и подкрепа” разработват и прилагат различни анализи, планове и програми за изследване и оценка на заплахите, насочени срещу повишаване

устойчивостта на критичната инфраструктура. Това представлява своеобразен модел на партньорство на национално ниво, използван с цел повишаване сигурността на елементите и обектите от системата на националната критична инфраструктура.

Като цяло през годините, в страната са предприемани множество инициативи и са прилагани различни пакети от мерки, които биха могли да бъдат обобщени по следния начин:

- всеобхватни превантивни мерки биват предприети от правителството, държавните агенции, бизнеса и индустрията (в Германия индустриалния сектор играе изключително важна роля при определяне на мерките за защита на критичната инфраструктура) за справяне на т.нар. проблем У2К, който е свързан със съхранението на данни. Мерките са насочени към осигуряване на съвместимост на информационните технологии с всички компютърно базирани инфраструктури и след настъпване на новото хилядолетие. Т.нар. ИТ концепция за защита на информационната критична инфраструктура, Национален план за защита на информационната критична инфраструктура и свързания с тях План за защита на критичната инфраструктура на страната, определят всички понятия и конкретни мерки за справяне с горе посочения проблем, като набелязаните инструменти се прилагат съвместно с бизнеса и индустриалното производство;

- в резултат на терористичните атака от 11 септември 2001 г. в САЩ и опустошителните наводнения от лятото на 2002 г. (през август 2002 г. проливни дъждове причиняват катастрофални наводнения в Германия, Австрия и други държави от Европейския съюз. Жертвите са почти 100 души, а икономическите загуби се оценяват на над 25млрд. евро.), Германия измества фокуса на действие, свързан с готовността на страната да гарантира националната си сигурност не само към защита на информационната сигурност, но и към всички други системи на критичната инфраструктура, като се определят и нови приоритети за справяне с потенциални заплахи. Примери за сериозни промени в стратегическо отношение могат да бъдат дадени след 11 септември 2001 г., когато в страната са въведени специални обучения за защита на персонала и действие в извънредни ситуации, които са задължителни за определени публични и частни организации. Приемат се множество международни споразумения, които да гарантират увеличаване на защитните мерки основно в транспортния сектор – по-специално въздушния (летище Франкфурт Рейн – Майн е третото по големина пътническо летище след Хийтроу и Шарл дьо Гол, то е най-голямото товарно летище в Европейския съюз, а през него годишно преминават около 52 млн. пътници и 2 млн. тона товари. Страната разполага с общо 27 цивилни летища, от които през 2012 г. са излетели около 1,2 млн. Полета, били са превозени 176 млн. пътници и 4,5 млн. тона стоки), морски и речен транспорт (страната притежава силно развит речен транспорт и има голяма флота от океански и морски кораби, както и големи пристанища на Северно и Балтийско море, които са от съществено значение и за международното корабоплаване), жп-транспорт (дължината на жп-линиите през 20102 г. достига 40 954км, които се използват от високоскоростни влакове. Статистиката сочи още, че всеки среднестатистически германец е използвал влак, средно 23 пъти през годината);

- отделно от информационните концепции за сигурност, публичния и частният сектор, заедно с организации с нестопанска цел и представители на академичното съсловие, работят съвместно по изготвянето на редица препоръки, планове и програми с практическа насоченост, с цел гарантиране устойчивостта на инфраструктурата – такива са всички практически насоки за анализ и оценка на риска и управление в извънредни ситуации, концепции за защита на хуманитарните организации, социалните сдружения, болнични заведения и др. Всички те се базират и ръководят от принципа и ролята на стратегическото планиране в процеса на защита на обектите и елементите на критичната инфраструктура на страната;

- в Германия ежегодно се провежда т.нар. LUREX, което представлява обучение за управление при кризи. В него взимат участие представители от публичния и частния сектор. На форума се разискват различни мерки и практически насочености за управление при кризи, които са разработени и предложени от правителствени и частни партньори, като се акцентира на готовността на системата за реакция при кризи на национално ниво. В резултат на съвместните учения се засилва взаимното доверие и сътрудничество между заинтересованите страни, въз основа на схващането, че процеса на управление при кризи, който е неразделна част от защитата на критичната инфраструктура, може да бъде достатъчно ефективен само чрез осъществяването на съвместни действия на всички нива на управление;

- с цел да се гарантира сигурността на критичната инфраструктура, която е напълно зависима от постоянно променящите се рискове и заплахи в обкръжаващата среда и увеличаване уязвимостта на обектите, се предприемат превантивни, изпреварващи мерки, като се използва целия потенциал, който предлагат новите технологии. Това произтича и от Национална програма „Научни изследвания за гражданската сигурност”, чието начало е поставено през 2007 г. от Федералното правителство, като част от т.нар. Hightech стратегия на Германия. В сътрудничество с академичната общност, индустриалният сектор и собствениците/операторите на обекти от критичната инфраструктура на страната разработват множество иновативни решения, гарантиращи сигурността на обществото.

Всеки един от горе изброените примери от практиката на Германия за защита на критичната инфраструктура цели да илюстрира съществуващата мрежа от партньорства между държавата и частния сектор, която ако е необходимо може да бъде доразвита и консолидирана.

Критичната инфраструктура на страната се характеризира с една много важна особеност, която е характерна не само за Германия – че от гледна точка на собствеността, по-голяма част от обектите от инфраструктурата не са държавна собственост, а се управляват и контролират от частни лица, част от тях са ги придобили съвсем наскоро. Това се отнася и за предоставянето на множество обществени услуги. В резултат на тази тенденция, отговорността за сигурността и надеждността на критичната инфраструктура все повече се поема от частния сектор, а в отделни случаи е споделена с държавата. По този начин функциите, възложени на държавата и/или на частния сектор, са насочени главно към разработване на превантивни разпоредби или механизми за защита и контрол на доставките на стоки и услуги, в случай на бедствие

или друга извънредна ситуация, когато нормалните пазарни механизми не функционират. Следователно, като изпреварваща мярка за справяне с тежки кризи и аварии, е прилагането на институционален подход, базиран на сътрудничество между държавата, бизнеса и индустриалния сектор, в рамките на установени партньорства за постигане на по – висока национална сигурност.

Обектите на критичната инфраструктура на Германия са изложени на множество рискове и заплахи, което изисква непрекъснати анализи и оценки на техния интензитет и избор на мерки за тяхното неутрализиране.

Според Националната стратегия за защита на критичната инфраструктура на страната, заплахите могат да бъдат обобщени в следния табличен вид:

Таблица 2

Природни явления Човешки грешки	Технически повреди/	Тероризъм/организирана престъпност
Екстремни климатични явления	Системни грешки	Тероризъм
Горски пожари	Небрежност	Саботаж
Земетресения	Аварии и катастрофи	Други престъпни форми
Епидемии и пандемии	Грешки в организацията на работа – недостатъци в процеса на управление на риска, недостатъчна координация и сътрудничество и др.	Граждански войни
Космически събития – енергийни бури, метеоритни дъждове и др.		

Тези събития или инциденти, резултат от множество фактори, причиняват огромни човешки, финансови и материални щети и/или водят до загуба на общественото доверие в политическото ръководство на страната, като могат да унищожат цели обекти или дори сектори от критичната инфраструктура, представляващи изключително важно значение за обществото. Секторите се характеризират със силна зависимост и взаимозависимост по между си, което може да доведе до т.нар. „ефект на доминото” – нарушаване в дейността на обект или сектор, поради реализирана заплаха, оказва влияние и на останалите елементи

След 11 септември 2001 г., борбата с тероризма става основна цел на държавата за постигане и поддържане на ефективната защита на националната сигурност. Приемат се редица законодателни промени в тази посока, не само в страната, но и на ниво Европейски съюз. Значението и измерението на тази заплаха се увеличават драстично през последните години.

В процеса на защита на критичната инфраструктура, освен заплахите от тероризъм, трябва да се обърне внимание и на заплахите, произтичащи от екстремалните климатични промени, които се характеризират с не по-малка мащабност, честота на повторенията (ако през изминалия век природните бедствия се наблюдаваха през няколко години, дори десетилетия, то днес те са ежедневие) и размер на загубите, били те човешки или икономически. В Германия сериозни щети върху обекти от критичната инфраструктура биха могли да бъдат причинени от силни бури или тежки наводнения, извод до който се стига в Стратегията за защита на критичната

инфраструктура на страната. Глобалните климатични промени и последствията от тях, които все по-често се усещат, в бъдеще ще ангажират все по-силно световната общественост.

Следователно, вниманието на държавата и обществото, по отношение на гарантирането на сигурността на критичната инфраструктура, трябва да бъде насочено от една страна към заплахата от терористични нападения, а от друга – към заплахите от природни бедствия. Разбира се, не трябва да се пренебрегват и останалите заплахи, като тези от системни грешки, човешки грешки, пожари и др., които биха нанесли не по-малки щети върху системата.

От подобно значение са рисковете и заплахите за информационната инфраструктура. В исторически план, първоначално се ангажира със защитата на тази система, по-късно с останалите сектори – факт, който беше дискутиран в изследването. Престъпни деяния, техническа неизправност или човешка грешка са само малка част от заплахите, които определят сигурността и нормалното функциониране на инфраструктурата.

Независимо от естеството и причините за възникване на заплахите, високо индустриализираните общества, каквото е и немското, разчитат на нормалното функциониране на множество сложни технологии, които се управляват и контролират от различни организационни структури. Всяко общество в хода на своето технологично развитие ще бъде все по-чувствително към смущенията във функционирането на тази инфраструктура. Това изисква разработването и прилагането на високи стандарти на сигурност и безопасност на доставките. Тази силна обществена зависимост от нормалното функциониране на доставките на стоки и услуги в немската практика се нарича „парадокс на уязвимостта” – колкото повече податливостта на обществото към повреди в процеса на доставка намалява, толкова по-сериозно ще бъде въздействието на един, действително разрушителен инцидент. Този парадокс непрекъснато се засилва, поради растящата зависимост на почти всички сектори от националното стопанство от гарантиране доставките на електроенергия, телекомуникационни и информационни продукти и др. Ето защо, държавната политика на страната е особено силна в тази област.

Разбира се, не съществува инфраструктура в света, която да бъде напълно защитена. В отговор на постоянно променящата се среда за сигурност, Германия обръща внимание на т.нар. „култура на риска”, която се основава преди всичко на:

- поддържане на открита комуникация между държавата, бизнеса и обществото, по отношение на различните видове риск за критичната инфраструктура на страната, като се взема под внимание чувствителността на определена информация;

- сътрудничество между всички заинтересовани страни в процеса на предотвратяване и управление на кризи;

- по-голяма ангажираност от страна на операторите на обекти от инфраструктурата, по отношение на превенцията и управлението на инциденти;

- възможност за по-голяма самозащитеност и самопомощ на физическите лица или институциите, засегнати от прекъсване и компрометиране на услугите, предоставяни от инфраструктурата – такава нова визия за риска, по отношение на критичната

инфраструктура, би могла да направи обществото по-силно в момент на справяне с нарастващите уязвимости.

Както вече беше споменато, защитата на критичната инфраструктура в Германия се регулира от Национална стратегия, която съдържа няколко основни стратегически цели:

- изграждане на взаимно доверие при сътрудничество на всички нива на управление;

- гарантиране на пропорционалност на взетите решения и използваните ресурси, с цел повишаване нивото на защита;

За да се гарантира сигурността на критичната инфраструктура, е необходимо да се разработят т.нар. стратегически подцели, които ще бъдат определени и изпълнявани с помощта на редица планове, програми и концепции. В областта на информационните технологии, сигурността се гарантира от Национален план за защита на информационната инфраструктура.

Необходимо е усилията на държавата в областта на защитата на критичната инфраструктура да бъдат подкрепени от подходящи мерки и дейности, координирани с всички заинтересовани страни, така че да се постигне:

- ниво на превенция – всички съществуващи и очаквани рискове да бъдат предварително идентифицирани;

- отговорност – всички дейности, предприети от различните институции и организации, по време на бедствие или авария трябва да бъдат максимално ефективни, с цел незабавното възстановяване на повредената инфраструктура, ако това е възможно. Отговорността за предприетите действия и настъпилите резултати се поема от съответните нива на управление;

- устойчивост – при всеки един възникнал инцидент в обект от критичната инфраструктура на страната, се взема поука, която се привежда в стандартите за безопасност, които се разработват от заинтересованите страни в съответствие с международните стандарти. Мерките за повишаване на устойчивостта се свеждат до: превенция, изпълнение, отговорност, анализ и оценка.

Последователното прилагане на горе посочените стратегически цели ще гарантира във висока степен устойчивостта на обектите, както и засилване на немските компетенции в областта на сигурността, които страната използва, в процеса на обмен на опит на международно ниво.

Основна предпоставка за успешното изпълнение на поставените стратегически цели са добре функциониращите механизми за сътрудничество със и между публичните власти на различните нива на управление, със и между операторите на обекти от системата, които в по-голямата си част са частноправни предприятия, извършващи дейността си в частния сектор на икономиката, както и съответните асоциации в ролята им на мултипликатори. Не е за пренебрегване ролята на академичната общност в процеса на защита на инфраструктурата, която със своите научни разработки подпомага усилията за повишаване устойчивостта на системата. Работи в рамките на национална програма „Научни изследвания за гражданска сигурност”, която е иницирана от Федералното правителство, а се ръководи и

контролира от Федералното министерство на образованието и научните изследвания.

Ето защо, за да се гарантира сигурността на критичната инфраструктура, се изисква наличието на интензивно сътрудничество, координация на действията и обмен на информация между отделните партньори и участници в процеса, които биват:

- Федерална администрация – федералните министерства и техните специализирани агенции;
- Федералните провинции и техните органи на управление;
- общините и местната изпълнителна власт;
- операторите на инфраструктурни обекти;
- агенция „аварийна безопасност“;
- съответните промишлени асоциации;
- научноизследователски учреждения;
- отбранителната промишленост;
- обществеността като цяло – в тази категория се отнасят както населението, така и всички печатни и електронни медии;
- международни институции;
- в случай на необходимост и други институции.

Многократно вече бе споменато, че ефективността на защитата на критичната инфраструктура се определя от наличието на партньорство между горе изброените заинтересовани страни, което включва обмен на информация, разработване на концепции и програми, координирани със съответните оператори на обекти. Федералната администрация е ангажирана с процеса на съгласуваност при разработването на рамкови програми, в съответствие с изискванията за гарантиране на националната сигурност, приети на държавно ниво.

В случай, че бъдат идентифицирани пропуски по отношение на сигурността на секторите, поради появата на нови рискове и заплахи или не отразяването на съществуващи такива, които не бъдат отстранени на доброволен принцип или ако правните разпоредби не предлагат адекватни решения, Федералното правителство си запазва правото, в рамките на неговата компетентност, да предприема инициативи за изменение на съществуващото законодателство. Пропуските се отстраняват от операторите и/или собствениците на обекти от състава на критичната инфраструктура.

В националната стратегия за защита на критичната инфраструктура на Германия е записано, че Федералното и местните правителства са длъжни да предприемат действия по гарантиране сигурността на системата, в съответствие с техните области на отговорност, които биват:

- определяне на общи цели на защитата;
- анализ на заплахите, уязвимостите и управленските способности;
- оценка на очакваните заплахи;
- определяне на защитни цели, като се вземат под внимание съществуващите защитни мерки, анализ на съществуващата нормативна уредба, идентифициране на допълнителни мерки, допринасящи за постигането на целите;
- ако и когато е необходимо, промени в националното законодателство.

Тези работни пакети се изпълняват главно от публичния сектор със съдействието

на съответните оператори на обекти. Отговорността за координацията на действията, на национално ниво, се поема от Федералното министерство на вътрешните работи.

За гарантиране изпълнението на Стратегията за защита на националната критична инфраструктура е необходим богат набор от инструменти, които биват:

- програми и планове – Национален план за защита на информационната критична инфраструктура, както и свързаните с неговото изпълнение програми и концепции;
- конкретни препоръки за действие;
- Национална концепция за защита на критичната инфраструктура, която дава основни насоки за физическата защита на обектите;
- ръководство за управление при кризи;
- различни програми за защита на секторите и/или подсекторите;
- редица стандарти, норми и правила – стандарти за гарантиране на информационната сигурност; разпоредби относно гарантиране осигуряването на доставки на газ, питейна вода и др.

През годините страната членува в различни международни съюзи, които имат отношение към защитата на критичната инфраструктура. Основните ѝ стратегически партньори в този процес са:

- съседните ѝ държави – Франция, Белгия, Австрия, Чехия, Полша, Дания и Холандия;
- Европейският съюз и съответно страните членки в него;
- страните-членки на Г-8 – съюз, в който страната членува, почти от неговото създаване. Тук са представени осемте най-развити икономически държави в света;
- страните-членки на Г-20 – Германия стартира членството си през 1999 г. като негов домакин. Това е организация за сътрудничество и консултации по въпроси, свързани с международната финансова система;
- НАТО – международна организация за военно сътрудничество, в която Германия членува от 1955 г., първоначално само като Западна Германия.

В рамките на международното си сътрудничество, страната подкрепя всички усилия и мерки, които са насочени към идентифициране и намаляване на уязвимостта на обектите на критичната инфраструктура, особено на тези, които имат трансгранично значение. Разширяването на съществуващите и подкрепа на нови двустранни партньорства за обмен на информация и най-добри практики, са от особено значение при гарантиране сигурността на транснационалните критични инфраструктури.

Използвана литература:

1. Луканов, А., Божинов, Н., Димитров, Ст., *Справочник на страните по света, изд. „Образование и наука“, С. 2001 г., стр. 40;*
2. *Съобщение на Комисията „Защита на критичната инфраструктура в борбата с тероризма“ от 20 октомври 2004 г. (COM (2004) 702 final);*
3. *Critical Infrastructure Protection (CI) - Status and Perspectives - Workshop on CIP, Frankfurt 2003;*
4. www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_english.pdf - *National Strategy for Critical Infrastructure Protection (CIP Strategy) Germany;*
5. *National Strategy for Critical Infrastructure Protection Germany, Berlin, 17th June 2009;*