**СЪДЪРЖАНИЕ**

***Предговор***

проф. д-р Христо Георгиев…..…………………………………………………..стр.

**ПЛЕНАРНО ЗАСЕДАНИЕ**

***От кризи към реформи: развитието на ЕС до 2019***

доц. д-р Светослав Малинов…..…………………………………………………..стр.

**ТЕМАТИЧНО НАПРАВЛЕНИЕ „Необходимите реформи в ЕС: концептуални, институционални и правни аспекти“**

***Европейският съюз между федерализма, функционализма и „свещения егоизъм“ на нациите. Варианти на политическо бъдеще на организацията***

проф. д-р Христо Георгиев*……………………………………….………………….…*стр.

**ТЕМАТИЧНО НАПРАВЛЕНИЕ „Политиките на ЕС в сигурността и отбраната пред съвременните предизвикателства“**

***Основни проблеми на политиката на сигурност в разширения европейски контекст - динамика между невоенните и военните аспекти в началото на 21 век***

д-р Георги Кръстев ………………………………………………….…………...стр.

**ТЕМАТИЧНО НАПРАВЛЕНИЕ „България в ЕС – перспективи и проблеми“**

***Гранични територии, гранични хора: българските мюсюлмани и Европейският съюз***

проф. д-р Милена Беновска-Събкова, д.и.н. и доц. д-р Илия Недин…………..стр.

**ПРЕДГОВОР**

**проф. д-р Христо Георгиев,**

**Ръководител на департамент**

**„Национлна и международна сигурност“,**

**Нов български университет**

**НЕОБХОДИМИТЕ РЕФОРМИ В ЕС: КОНЦЕПТУАЛНИ, ИНСТИТУЦИОНАЛНИ И ПРАВНИ АСПЕКТИ**

**ПОЛИТИКИТЕ НА ЕС В СИГУРНОСТТА И ОТБРАНАТА ПРЕД СЪВРЕМЕННИТЕ ПРЕДИЗВИКАТЕЛСТВА**

**Основни проблеми на политиката на сигурност в разширения европейски контекст - динамика между невоенните и военните аспекти в началото на 21 век**

*доктор Георги КРЪСТЕВ*

*секретар на Съвета по сигурността към Министерски съвет*

***Резюме:***

***Ключови думи:***

**Аналитични платформи и Big Data в структурата на кризисен мениджмънт**

*проф. Руси МАРИНОВ, д.н.*

*Нов български университет*

***Резюме:***

***Ключови думи:***

**Иран и Таджикистан - два подхода към международната правна помощ на пътя на афганистанските наркотици**

*доц. д-р Тодор КОЛАРОВ*

*Нов български университет*

***Резюме:***

***Ключови думи:***

**Въведение**

Едно от важните предизвикателства пред сигурността на съвременната държава е ефикасното и ефективно противодействие на престъпленията свързани с производството, преработката, трафикът и разпространението на наркотични вещества. Този проблем, пред който се изправят всички те, е причина за редица международни договори целящи подобряване на сътрудничеството между тях срещу тази тежка трансгранична престъпност, която генерира значителни финансови активи. Като част от тези усилия са приети и Конвенциите на ООН срещу транснационалната организирана престъпност 2000 (Конвенцията от Палермо) и взаимно допълващите се Единна конвенция по упойващите вещества от 1961 г., Конвенцията за психотропните вещества от 1971 г. и Конвенцията на ООН за борба срещу незаконния трафик на упойващи и психотропни вещества от 1988 г. (Наркотичните конвенции).

Една от държавите с незавидната глобална репутация на източник на наркотици е Афганистан[[1]](#footnote-1). Два от основните маршрута за трафик на наркотици от Афганистан към трети държави са през Иран и Таджикистан. Поради това настоящото изследване фокусира вниманието си върху правната рамка в тези две държави в сферата на международно сътрудничество по наказателни дела, като се стреми да анализа ефективността и ефикасността на правния режим там. Тази статия не обхваща всички аспекти на международното сътрудничество по наказателни дела, а избира три от тях, които са ключови – международната правна помощ, екстрадицията и конфискацията на престъпни активи.

Важно условия за ефективността на тези институти е криминализацията на определени деяния в националния правен ред, което определя компетентността на националните правораздавателни органи. Поради това внимание ще бъде отделено и на този аспект, като предпоставка за международното сътрудничество.

Международните стандарти, които служат за сравнение и оценка на ефективността и ефикасността на националната уредба на Таджикистан и Иран са горепосочените конвенции на ООН и по конкретно чл. 12 (конфискация), чл. 15 (компетентност), чл. 16 (екстрадиция), чл. 18 (взаимна правна помощ) от Конвенциите на ООН срещу транснационалната организирана престъпност и аналогичните разпоредби в Наркотичните конвенции, както и Препоръките на Работната група за финансов действие (FATF) от 2012 г.

**Някои въпроси на компетентността**

Както вече се отбеляза тук, компетентността е предпоставка за ефективност на международното сътрудничество, поради което ще се започна именно с тази подтема. Член 15 от Конвенцията от Палермо задължава страните по конвенцията да установят в своята компетентност за престъпленията предвиден в този международен договор при условията на териториалния принцип. Освен това чл. 15, параграф 3 установява задължението за упражняване на компетентност в случай, че лицето е гражданин на съответната държава и тя не го екстрадира за съдене в чужбина на това основание. И двете държави, Иран и Таджикистан, установяват това правило в националното си право. В чл. 3 и сл. и чл. 7 на иранския Наказателен кодекс са предвидени териториалния и националния принципи, за да упражни държавата своята компетентност. Наказателният кодекс на Таджикистан[[2]](#footnote-2), в чл. 14 и 15, установява териториалния принцип за водещ при упражняване на компетентност. Другите принципи имат субсидиарен характер. Подробната уредба сочи, че граждани и постоянно пребиваващи в Таджикистан попадат под националната компетентност за извършени в чужбина престъпления, само ако това е нужно, за да се избегне отрицателен спор за компетентност.

Интерес представлява и въпросът за наказателната отговорност на юридически лица (ЮЛ), която конвенциите на ООН установяват като възможност. Въпреки че този институт често е сочен от представители на системата на общото право като незаменим при ефективното противодействие на тежка организирана престъпност, финансиране на тероризъм и престъпления свързан с наркотици, в тази статия това становище не получава еднозначна подкрепа. От една страна трябва да се признае, че догматичното противопоставяне на този институт, който е чужда на континенталната правна система е контрапродуктивно, особено с оглед на възприемането му от държави, които принадлежат към тази традиция[[3]](#footnote-3). От друга страна обаче международните стандарти, включително разглежданите конвенции на ООН, не установяват такова задължение. Считам, че аналогични резултати са постижими и с въвеждането на ефективна административна и гражданска отговорност за ЮЛ.

Иран въвежда наказателна отговорност за ЮЛ, докато Таджикистан – не. Иранското законодателство предвижда, че ЮЛ може да бъде закрито, лицензът му отнет (ако има такъв) и имуществото му конфискувано[[4]](#footnote-4). Наказателният кодекс на Таджикистан не предвижда такава възможност като изрично установява наказателна отговорност само за физически лица (ФЛ)(чл. 22, ал. 1). Страната обаче предвижда изрична юридическа отговорност на ЮЛ за нарушение на законодателството противодействащо на прането на пари (чл. 18). В допълнение Кодексът на административните нарушения (чл. 31) и Гражданският кодекс (чл. 57) са приложими в редица случаи, когато е нужно да се ангажира юридическа отговорност на ЮЛ.

Без да претенция за изчерпателност, считам, че друг важен аспект в тази подтема е ефективността на националния режим за преследване на прането на пари. Практиката показва, че за успешното противодействие на този вид престъпление от особена важност е разделянето на предикатното престъпление от престъплението пране на пари. Таджикистан прави това в националното си законодателство (чл. 262, бележка 8 Наказателния кодекс на Таджикистан)[[5]](#footnote-5). Иранският закон против прането на пари (2008 г.) обаче изисква предикатното престъпление да е доказано в цялост преди да се докаже пране на пари[[6]](#footnote-6).

Друг аспект за ефективността на националния режим за противодействие на прането на пари е наличието на възпиращи наказания. В този смисъл считам, че глоби в не особено високи размери не могат да доведат до желания резултат. Иранският закон против прането на пари (чл. 9) предвижда възстановяване на облагата от престъплението, всички плодове от нея, и глоба в размер до ¼ от тази облага. Не се предвижда наказание лишаване от свобода. Подходът на Наказателния кодекс на Таджикистан (чл. 262) е още по-либерален, като предвижда наказание глоба от 1,500 до 2,200 USD или до 2 години лишаване от свобода и лишаване от право на упражняване на определени професии[[7]](#footnote-7).

С оглед гореизложеното, по-високи очаквания би могло да има особено към режима за противодействие на прането на пари и на двете държави, макар и в различни негови аспекти.

**Правната основа – обща характеристика**

Правната основа за реализиране на сътрудничество са международните договори и националното законодателство на държавите. Статусът на Иран и Таджикистан в процеса на присъединяване към споменатите универсални международни договори е както следва:

|  |  |  |
| --- | --- | --- |
|  | Иран | Таджикистан |
| Конвенцията от Палермо | X | 2002 |
| Протокол 1 | X | 2002 |
| Протокол 2 | X | 2002 |
| Протокол 3 | X | X |
| Наркотична конвенция от 1961 | X | 1997 |
| Наркотична конвенция от 1971 | 2000 | 1997 |
| Наркотична конвенция от 1988 | 1992 | 1996 |
| Протокол от 1972 | 2001 | X |

|  |  |
| --- | --- |
| X- подписан, но не е ратифицирана | X- не е подписана и не е ратифицирана |

Освен това, двете държави са страни и по редица многостранни и двустранни международни договори. Подходът на двете държави е различен. Таджикистан е страна по Конвенцията за правна помощ по граждански, семейни и наказателни дела на Общността на независимите държави (ОНД) от 22.01.1993 г., изменена на 7.10.2002 г., често наричан Минска (1993 г.) и Кишиневска (2002) конвенции[[8]](#footnote-8). Докато Таджикистан разчита в по-малка степен на двустранни договори, подходът на Иран е насочен именно към разгърната система от двустранни договори. Ислямската република е страна по 47 двустранни международни договора по въпросите на екстрадицията и международната правна помощ, като към юни 2015 г. още 25 са в различни стадии на подготовка (преговори, очакващи подписване или ратификация).

Важно е да се отбележи, че правният ред и на двете държави установява предимство на международните договори на страната пред националните закони. В Таджикистан това е конституционно закрепен принцип базиран на континенталната правна традиция. В Иран принципът има своите корени в ислямската правна система, и по конкретно Сура 5 от Корана, който указва „изпълнявай договорите си“.[[9]](#footnote-9) Според чл. 77 и 125 от Конституцията на Иран влезлите в сила международни договори имат директен ефект и следва да се приложат от национален съд с предимство пред националните закони.

**Правна основа на взаимната правна помощ и екстрадацията**

Националната правна рамка по въпросите на взаимната правна помощ и на двете държави установява, че такава помощ може да се основава на международен договор или взаимност. На международните договори сключени от държавите за реализирането на международна правна помощ няма да се спираме подробно, тъй като този въпрос беше засегнат по-горе. Следва да се повтори, че докато Таджикистан разчита на договорите под егидата на ООН и тези в рамките на ОНД, Иран залага на разгърната система от двустранни договори[[10]](#footnote-10).

Компетентните органи имат някои специфики. В Таджикистан въпросът е уреден в глава 48 на Наказателния кодекс на страната. Прокуратурата е компетентният орган в досъдебната фаза, а Председателят на Съдебния съвет в съдебната (чл. 470 Наказателния кодекс на Таджикистан). В Иран ситуацията е различна. В ислямската република Бюрото по международни въпроси към иранската магистратура е компетентно за всички случаи на международна правна помощ.

По принцип, този различен подход не е основание за трудности при реализиране на международната правна помощ. Потенциални предизвикателства, относно Иран, могат да възникват поради строго формализирания подход на иранските власти и невъзможността за директна комуникация между съдебните органи по повод молбите за правна помощ. Предизвикателствата по отношение на Таджикистан са свързани с факта, че Съдебният съвет няма компетеност по въпроси, които касаят Върховния съд на Таджикистан, който реализира международната правна помощ чрез собствени органи. Така системата демонстрира липса на кохерентност, което може да създаде проблеми.

Относно международните договори, които се явяват правна основа на екстрадицията, не се наблюдават отклонения от казаното за международната правна помощ която е обсъдена по-горе.

Правната основа за екстрадиция във вътрешното право на Таджикистан е в глава 49 от Наказателно-процесуалния кодекс на страната. В чл. 478 и сл. от Наказателно-процесуалния кодекс е посочено, че компетентна както за входящи, така и за изходящи молби за екстрадиция е Главната прокурора на Таджикистан. Обжалваните входящи молби за екстрадиция подлежат на съдебен контрол. Интересно е да се отбележи, че регламентацията се отнася до хипотези, при които граждани на Таджикистан са извършили престъпления на територията на Таджикистан, след което са напуснали пределите на страната (чл. 476). Това изрично ограничаване на компетентността на националните органи до хипотези на прилагане на териториалния принцип и то само по отношение на граждани на Таджикистан има потенциал да постави предизвикателства пред ефективността на реализирането на противодействието на трансгранична престъпност. Иначе националната уредба указва, че входящи молби за екстрадиция следва да се изпълнят в 30-дневен срок (чл. 481, ал. 3 от Наказателно-процесуален кодекс на Таджикистан), тоест в кратък срок. Процесуалният закон, на книга, съдържа гаранции за правата на обвиняемия и при потенциал за нарушаването им забранява екстрадиция (чл. 479 от Наказателно-процесуален кодекс на Таджикистан). Например, всички случаи на молби за екстрадиция на лица поискали политическо убежище или такива, при които може да бъдат нарушени правата на обвиняемия са основание за отказ на молбата. Наказателно-процесуалния кодекс не дава възможност за дискреционна преценка на прокуратурата при никое основание, а налага директна забрана за удовлетворяване на молбата за екстрадиция.

В Иран уредбата на екстрадицията е в Закона за екстрадицията. Чл. 9 от закона предвижда, че компетентният орган, както за входящи, така и за изходящи молби за екстрадиция е Бюрото по международни въпроси към иранската магистратура. Входящите молби се изпращат до местно компетентния съд, чието решение може да се обжалва пред висшестоящата съдебна инстанция. Законът за екстрадицията установява срокове за изпълнение на входящи молби за екстрадиция до 30 дни, когато молещата държава е съседна на Иран, и 60 дни за молби от останалите държави. Иранският закон също съдържа разпоредби гарантиращи спазване на правата на лицата, чиято екстрадиция се иска. Сочи се, че не се екстрадират лица, срещу които се води наказателно преследване по политически мотиви, при военен характер на престъплението, при дискриминация, както и когато в молещата държава се води гражданска война - докато трае войната, освен ако не се отнася за военни престъпления.

Следва да се отбележи, че изпълнение на молби за екстрадиция както в Иран, така и в Таджикистан следва да се реализира при скрупульозно внимание за гаранция на правата на екстрадираните лица, така че да не бъде нарушена Европейската конвенция за правата на човека. При екстрадиция в Иран следва да с е отчита и една особеност на иранската правна система, в която бой с пръчки е наказание в системата на наказателния закон на страната. В този смисъл Иран не изпълнява молби за правна помощ, ако лицето може да бъде подложено на нечовешко или унизително отношение, но горепосоченото наказание не се счита за такова. Не случайно Иран не е страна по Конвенцията на ООН за защита от изтезания, нечовешко или унизително отнасяне или наказание. Изпълнението на молби за екстрадиция на Таджикистан от страна на Русия пък е дало основание на Европейския съд за правата на човека нееднократно да установи нарушения на Русия на задълженията й по Европейската конвенция за правата на човека[[11]](#footnote-11).

**Международно сътрудничество при конфискация на престъпни активи**

Правната основа на международното сътрудничество при конфискация на престъпни актив се реализира на база на същите международни договори, които намират приложение и при взаимната правна помощ и екстрадицията.

Както в Иран, така и в Таджикистан конфискацията е наказание, но в Таджикистан тя е и мярка. Като наказание, конфискацията и в двете държави е допълнително наказани, което може да се наложи заедно с осъдителна присъда. Въпреки че това отговаря на минималните стандарти установени в международните договори на ООН, може да се постави въпроса за ефективността на такъв подход. В съвременната теория и практика все повече се налага конфискацията *in rem,* като далеч по ефективен инструмент. И двете държави възприемат, но само донякъде тази идея във вътрешното си законодателство.

В Иран конфискацията се разглежда основно като наказание. Наказанието е предвидено в Наказателния кодекс на ислямската република. Допустима е конфискация на придобитите от престъпната дейност активи и на средствата за извършване на престъплението. В Закона срещу наркотиците обаче е предвидена и конфискация на ЮЛ, които се използват при извършване на престъпления свързани с наркотици. Законът срещу наркотиците на Иран предвижда и заместваща конфискация. Иранският закон предвижда и разширена конфискация. В случай, че такава конфискация би засегнала правата на трети добросъвестни лица се прилага заместваща конфискация на паричната равностойност изискуема от извършителя на престъпното деяние. Иранската правна система допуска и гражданска конфискация[[12]](#footnote-12), по която се произнася гражданският съд, ако обвиняемият е починал или се укрива от правосъдието. Гражданския кодекс на Иран (чл. 1218), Постановление за компетентността от 1949 г. и негово тълкуване от 1982 г. установяват правилото, че лице което е изпаднало в трайно разстройство на съзнанието след извършване на престъплението е отговорно за възстановяване на причинените от престъплението вреди. Така Иран предвижда конфискация *in rem* извън наказателния процес. Тази възможност обаче изглежда ограничена, тъй като формулировката на закона предвижда конфискация в размер на причинените вреди, а не на натрупаните облаги. Последните, както е известно, могат, и обикновено са, значително по-големи.

В Таджикистан уредбата е в Наказателния кодекс на страната. И там е посочено, че конфискацията е субсидиарно наказание (чл. 47, точка и) и чл. 48, алинея 3). Наказателната конфискация не е приложима за всички престъпления, а само за изрично изброените (чл. 57, алинея 1). Таджикистан също предвижда конфискация на средствата за извършване на престъплението. Предвижда се и конфискация на облагите от престъпната дейност. Конфискуват се както директните, така и косвените облаги (чл. 57, ал. 1 и чл. 262, обяснителни бележки 3-6 от Наказателния кодекс). Формулировката на закона включва изрично и конфискация на трансформирано имуществото (чл. 57, ал. 2 от Наказателния кодекс), както и имущество прехвърлено на трети лица, включително ЮЛ (чл. 57, ал. 3 от Наказателния кодекс). Предвижда се конфискация и на паричен еквивалент, ако конфискация на реално придобитото е невъзможна (чл. 57, ал. 4 от Наказателния кодекс).

Компетентна да поиска наказанието конфискация в Иран и Таджикистан е националната прокуратура, а съдът се произнася по искането. В Иран това важи и за процедурата по изпълнение на молби за признаване и изпълнение на съдебно решение за конфискация. В Таджикистан уредбата на признаване и изпълнение на съдебни решения за конфискация е оскъдна. В Наказателно-процесуалния кодекс на Таджикистан изрично се предвижда само възможността за признаване и изпълнението на решения за конфискация на средствата на престъплението или облагите, директни и косвени, от престъпната дейност (чл. 482 от Наказателния кодекс).

Иранският закон не допуска прехвърляне на доказателствената тежест върху обвиняемия, освен в ограничени случаи на неоснователно обогатяване характерно за корупционни практики от лица с политическа експозиция. Конституцията на страната (чл. 141) и релевантни изпълнителни заповеди допускат това.

С оглед на горното не може да се твърди със сигурност дали чуждестранна молба за изпълнение на решение в Иран на граждански съд за конфискация *in rem* би била допустима за привеждане в изпълнение в ислямската република поради противоречие с *ordre public.* Уредбата в Таджикистан пък разчита в голяма степен на уредбата в международните договори, а не на уредба във вътрешното право. Изрична разгърната уредба във вътрешното право обаче би създала по-голяма сигурност и предвидимост.

**Заключение**

В заключение следва да се отбележи, че както всяка национална правна система, така и тези на Иран и Таджикистан търпят подобрения при справяне с идентифицираните предизвикателства. Очевидно някои от тези подобрения не са в законодателството, а в практиките, които не са в унисон със съвременните достижения в сферата на човешките права. Друга, например тези отнасящи се до конфискацията, макар и да покриват минимални стандарти имат потенциал да бъдат развитие до нивата на най-добрите съвременни достижения за ефективност. Накрая, съществува и група на законодателни разпоредби, които имат нужда от привеждане в унисон с общоприетите стандарти, какъвто е примерът с отнасящите се до прането на пари.

**Използвана литература:**

1. Afghanistan Opium Survey 2014 - Cultivation and Production - <http://www.unodc.org/documents/crop-monitoring/Afghanistan/Afghan-opium-survey-2014.pdf>

**Корупция и промигрантски лобизъм в Европа**

*проф. д-р Николай Радулов*

*Нов български университет*

***Резюме:***

***Ключови думи:***

**Може ли Европа да създаде единна армия като инструмент за отстояване на интересите си?**

*проф. Георги Бахчеванов, д.н.*

*Нов български университет*

***Резюме:*** *Европа трябва да притежава военна сила, за да защитава и налага своите интереси и защитава своите ценности. Военна сила с изградена структура, способна да функционира в многостранна организация за сигурност с общи оперативни процедури, ефективна система за командване и контрол, ефективна логистична поддръжка, значителни транспортни възможности и добре подготвени и способни на взаимозаменяемост въоръжени сили.*

*Основните проблеми свързани със създаването на общи въоръжени сили са: липсата на единно виждане на страните членки от такава необходимост; сложност на взаимоотношенията „НАТО и Европейски съюз”; трудното постигане на съгласие относно географските райони за действие; политиката на САЩ; разходите и др.*

***Ключови думи:*** *среда на несигурност, европейски въоръжени сили, насилие, тероризъм.*

Идеята за създаването на единна европейска армия не е нова. На практика тя се появява още преди стартирането на Европейския проект в средата на 20 век. Причините да се възобнови дебатът за общата европейска отбрана и единна европейска армия са предизвикателствата, рисковете и заплахите генерирани от съвременната среда на несигурност. На практика Европа е заобиколена от постоянно действащи въоръжени конфликти: военните действия в Украйна, анексирането на Крим, замразените конфликти в Кавказ и Приднестровието, войните в Близкия изток и Северна Африка. Към този списък можем да добавим постоянните „традиционни” симетрични и несиметрични заплахи като разпространение на оръжия за масово унищожение и средствата за тяхното доставяне, провалени държави, международен тероризъм и не на последно място кибер заплахите. Набиращите все по-голяма сила миграционни потоци и хибридните войни. Трудно е да се посочи единно европейско мислене и действие в тези предизвикателства. Събитията за пореден път показаха, че Европейския съюз няма собствена политическа тежест на международната сцена и е неспособен, да се намеси използвайки сила, където и когато е необходимо.

В подкрепа на горното можем да цитираме реакцията на политическите лидери на Европа по повод изказването на председателя на Еврокомисията Жан Клод Юнкер: „Европейският съюз се нуждае от собствена армия за решаване на проблема, че не е възприеман сериозно като международна сила. Европейска армия няма да бъде създадена с цел веднага да бъде използвана. Но една обща армия на европейците би предала на руснаците посланието, че ние сме готови да отстояваме ценностите на Европейския съюз. Обединяването на военните усилия на страните членки ще направи разходи по-ефективни и ще задълбочи още повече европейската интеграция. Такава армия ще ни помогне да формулираме обща външна политика и политика на сигурността“.

Идеята на Юнкер получава подкрепата както на германския канцлер Ангела Меркел, така и сред депутатите от Бундестага. Според ръководителя на комисията по външни работи в Бундестага Норберт Ретген, е дошло времето за създаване на такава армия[[13]](#footnote-13). Подобна армия би засилила влиянието на Берлин не само в Европа, но и в света. Естествено тук присъства и интересът на германското военно-промишлено лоби.

Великобритания обаче категорично отхвърля идеята. "Нашата позиция е кристално ясна - отбраната е национална, а не отговорност на Европейския съюз, и няма изгледи тази позиция да се промени, както няма изгледи за създаване на европейска армия", казва говорител на британското правителство. Джефри Ван Орден. зам.-председател на Европейските консерватори и реформисти допълва: „Безкрайните приказки за европейска армия трябва да престанат. За еврократите всяка криза се разглежда като възможност все повече да централизират целите на Европейския съюз. Амбициите на Европейския съюз в сферата на отбраната са пагубни за нашите национални интереси, за НАТО и за близките съюзнически отношения, които Великобритания има с много страни извън Европейския съюз - не на последно място САЩ, страните от Персийския залив и много страни от Общността на нациите. Юнкер живее в измислен свят. Ако нашите страни се изправят пред сериозна заплаха за сигурността си, на кого тогава ще разчитаме - на НАТО или на ЕС? Отговорът се налага от само себе си.

За да се добие вярна представа за характера и значението на идеята за създаването на единна европейска армия и за да се разбере същността и значението на общата външна политика и политиката за сигурност (ОВППС), и като част от нея политиката за сигурност и отбрана на Европейския съюз е необходимо да имаме ясна картина на предисторията. Това дава възможност да се отчете пълния потенциал на тенденциите на развитие на връзките между отделните политики на Европейския съюз и особено взаимното им влияние и обвързаност с неговата външна политика и политиката му за сигурност и отбрана. Историческата ретроспекция е наложителна и за да бъдат оценени в пълната им сила позициите и сблъсъка на интереси на държавите-членки в този процес – сблъсък, който няма да приключи скоро и в който изчаквателната позиция и пасивността не може да се очаква да бъдат печеливши. Цялата история на обединяване на Европа е поредица от неуспешни опити за директно обединяване на нейната сигурност и отбрана и решаване на тази задача индиректно и еволюционно[[14]](#footnote-14).

Началото е поставено през 1947 г., когато Великобритания и Франция подписват договора от Дюнкерк, който предвижда взаимопомощ срещу евентуално нападение от Германия. През март 1948 г. – Дюнкеркският договор става Брюкселски[[15]](#footnote-15). В него влизат Белгия, Холандия и Люксембург. На 28 септември 1948 г. е създадена Западноевропейската отбранителна организация (ЗЕОО). Организацията трябва да прилага Брюкселския договор. През април 1949 г. , САЩ и Канада заедно със страните от ЗЕОО създават НАТО с Вашингтонския договор. Договорът предвижда задължение за взаимна отбрана, ако някой от съюзниците бъде нападнат.

Първоначалните усилия за съвместни действия във външната политика и сигурността са материализирани в предложението за създаване на Европейска отбранителна общност през 1952 г. Това е началото за стартиране на амбициозен план за създаването на наднационална Пан-европейска армия, предложен от френския политик Рене Плевен. Инициативата се проваля вследствие на вето от страна на Франция. Френското Национално събрание отказва да ратифицира договора за нея.

През 1954 г. страните от ЗЕОО променят Брюкселския договор, приемат в него Западна Германия и Италия и организацията еволюира в Западноевропейски съюз (ЗЕС).

На 13 декември 2007 г. е подписан Лисабонският договор. Той постановява, че Европа ще има обща отбрана, когато държавите-членки решат това с единодушие. Политиката да сигурност и отбрана от “европейска” става “обща”, което слага край на ЗЕС. Лисабонският договор преподрежда уредбата за външни отношения, сигурността и отбраната на Европейския съюз и внася в тази уредба фундаментални промени.

Има ли правно основание идеята за създаване на Европейски въоръжени сили? Европейският съюз е политически и икономически съюз състоящ се от 28 европейски държави. Той е самостоятелно юридическо лице, притежаващо правомощия да действа независимо от съставящите го държави в рамките на предоставените му компетенции. Неговият статут е регламентиран в Договора за Европейския съюз (ДЕС) и Договора за функционирането на Европейския съюз (ДФЕС), в сила от 1 декември 2009 г. или както е по-известен като „Договора от Лисабон”. Функционирането на ЕС се осъществява от неговите органи и учреждения, някои от които са наднационални, а други — междуправителствени.[[16]](#footnote-16)

Въпреки, че Договорът от Лисабон не се отнася пряко до "Европейска армия", той регламентира Общата политика за сигурност и отбрана (ОПСО). ОПСО е неразделна част от общата външна политика и политика за сигурност (ОВППС) на Съюза. ОПСО е определена в Договора за Европейския съюз (ДЕС). Член 41 определя финансирането на ОВППС и ОПСО, като политиката е допълнително описана в членове 42—46, в глава 2, раздел 2 от дял V („Разпоредби, свързани с общата политика за сигурност и отбрана“), както и в протоколи № 1, 10 и 11 и в декларации № 13 и 14. Специфичната роля на Европейския парламент в ОВППС и ОПСО е описана в член 36 от ДЕС[[17]](#footnote-17).

Решенията относно ОПСО се вземат от Европейския съвет и Съвета на Европейския съюз (член 42 от ДЕС). Те се вземат с единодушие с някои забележими изключения относно Европейската агенция по отбрана (EАО, член 45 от ДЕС) и постоянното структурирано сътрудничество (ПСС, член 46 от ДЕС), при които се прилага гласуването с мнозинство. Предложенията за решения обикновено се правят от върховния представител на Съюза по въпросите на външните работи и политиката на сигурност, който също така изпълнява функцията на заместник-председател на Европейската комисия (заместник-председател/върховен представител).

Договорът от Лисабон въвежда понятието „европейска политика в областта на отбранителните способности и въоръжаването“ (член 42, параграф 3 от ДЕС), въпреки че все още предстои то да бъде определено. Той също така установява връзка между ОПСО и други политики на Съюза, като изисква EAО и Комисията да работят в сътрудничество, когато е необходимо (член 45, параграф 2 от ДЕС). Това по-специално се отнася за политиките на Съюза в областта на научните изследвания, промишлеността и космическото пространство.

Лисабонският договор предвижда ЕС да има общи цивилни и военни мисии в целия им спектър – от хуманитарна помощ и опазване на мира до налагането му със сила. Решенията за тях изискват консенсус между държавите-членки. Извън отделните мисии обаче договорът предвижда и изграждане на обща европейска отбрана “ако държавните и правителствените ръководители решат това единодушно”. Такова решение още липсва, главно заради съпротивата на Великобритания, но договорът предлага опция и при липса на консенсус – т.нар. “структурирано сътрудничество” – общата отбрана се изгражда на междуправителствена основа между желаещите държави.

Европа има потенциал да бъде респектираща военна мощ. Общият брой на личния състав от конвенционалните въоръжени сили на страните членки на Европейския съюз в момента е повече от 1,5 милиона души. Европейците разполагат с повече от 15 хиляди танка, най-малко 15 хиляди бронирани машини и бронетранспортьори, 4000 бойни самолети и кораби.

Днес базата на общата военна мощ на Европа се допълва от ядрените сили на Великобритания и Франция (членки на Съвета за сигурност на ООН). Великобритания разполага с четири ядрени подводници (NPS), с 16 балистични ракети с 200 ядрени бойни глави. Франция има 4 подводници с 64 ракети и 384 бойни глави, както и изтребители-бомбардировачи Mirage-2000h и Rafale, въоръжени с крилати ракети с ядрени бойни глави.

Европа е икономически гигант, който не разполага със собствени въоръжени сили. Тя има 500 милиона души население и е най-големият свободен и единен пазар. На нея се падат 26 процента от световния БВП при 22 процента за САЩ, 16 на сто от световната търговия при 14,1 на сто за САЩ[[18]](#footnote-18). Европа разполага с мощен военнопромишлен комплекс, които подкрепя идеята, както за увеличаване на разходите за отбрана на страните членки, така и за създаване на Европейски въоръжени сили. Европа на няколко пъти през XXI век изпреварва САЩ по отношение на продадените оръжия. Тук са част от най-големите в света военно-промишлени концерни – ЕАДС,“БАЕ Системс”, “Дасо”, “Финмеканика”, “Круп”, “Краус-Мафай-Дегман”, “Викърс”, “Ото Мелара”. Например в момента акциите на Европейския аерокосмически концерн ЕАДС (European Aeronautic Defence and Space Company - EADS) се разпределят както следва: 11.96 на сто се държат от контролираната от френското правителство компания SOGEPA (Societе de Gestion de Participations Aеronautiques), 10.69 процента са на германската GZBV, а 4.12% са собственост на испанската SEPI (Sociedad Estatal de Participaciones Industriales). Останалите 72.37 на сто са на институционални инвеститори, фондове и други частни структури[[19]](#footnote-19).

В рамките на "Общата политика в областта на европейската сигурност и отбрана", разработен през 1999 г., Европейският съюз извършва независимо и осъществява различни дейности - както цивилни и военни. ЕС поддържа международни военни и цивилни мисии в Афганистан, Босна и Херцеговина, Конго, Мали, Молдова, Либия, Нигер, Ирак, Косово, Палестинските територии, Сомалия, Южен Судан и Украйна. Повече от 13 подобри мисии на ЕС вече са приключили.

Основните проблеми свързани със създаването на общи въоръжени сили са: липсата на единно виждане на страните членки от такава необходимост, сложност на взаимоотношенията „НАТО и Европейски съюз”; трудното постигане на съгласие относно географските райони за действие; политиката на САЩ и др..

Германия, Франция, Холандия, Полша и други по-малки страни подкрепят идеята за създаване на общи въоръжени сили. Великобритания вижда създаването на армията на Европейския съюз като стъпка към по-голяма федерализация и отслабване на ролята на националните държави в Европа. За британците трансатлантическите отношения обикновено са по-важни от европейските.

Друг чувствителен въпрос също е по отношение на задълженията на държавите-членки, определен от Европейския съюз, които извършват обща отбрана в рамките на Северноатлантическия договор. В отговор на критичните гласове относно дублиращи се структури на двете организации, неоправдани финансови разходи за въоръжаване и отбрана и др., говорителя на Европейската комисия Мина Андреева казва: "Разполагаме с изследвания, които показват, че общото европейско сътрудничество в областта на отбраната може да доведе до икономии в размер до 120 млрд. евро всяка година".

Проблем е и съгласието относно географските райони за действие на едни Въоръжените сили на Европа. Като такива могат да се посочат Африка, Близкия Изток, Централна Азия, Кавказ и Балканите. Тук е асоциацията с член 6 на Северноатлантическия договор[[20]](#footnote-20), който ограничава района, който НАТО покрива, за да не би да се направи косвеният извод, че САЩ поемат по-широки задължения, като например защита на колониалните владения на новите си, по това време, Западноевропейски партньори по договора.

Според някои експерти САЩ винаги са ревнували Европа от опитите за отбранителни проекти извън НАТО. Например на среща на НАТО в Берлин (3 юни 1996 г.) се решава да създаде европейски стълб на НАТО под наблюдението на ЗЕС. Замисълът е той да се намесва там, където алиансът не желае и частично да облекчи ангажиментите на САЩ. Решението идва след войната в Босна и Херцеговина. В същото време тогавашният американски държавен секретар Мадлийн Олбрайт начертава “червените линии” на САЩ около европейския стълб, известни като “трите Д” – никакво дублиране (duplication), никаква дискриминация срещу членове на НАТО извън ЕС (discrimination – има се предвид Турция), никакво отделяне (decoupling) на Европа от САЩ.

Ситуацията в момента не е точно така. САЩ преориентират центъра на външната си политика към Азия и Тихия океан и очакват от Европа все повече да поема сама отговорности в кризи, където те не желаят да се намесват. Тук могат да се посочат Босна и Херцеговина, Украйна, Либия, Мали. Нещо повече, не минава среща на НАТО, където САЩ да не напомнят, че посрещат ¾ от разходите на алианса.

След войните на Балканите, в Ирак и в Афганистан САЩ са все по-малко склонни и готови да се ангажират в решаването на всяка ново появила се криза. Решенията в НАТО се вземат с консенсус, което означава, например че Турция може с вето до ограничи възможността на европейците да действат в свой интерес. Европа се нуждае от автономна възможност да прави, каквото е необходимо, без да бъде спъвана с вето извън Европейския съюз.

Вариантите за еволюционно изграждане на Европейски въоръжени сили се свеждат до два: „отгоре надолу” и „отдолу на горе”.

Еволюционно изграждане на Европейски въоръжени сили от горе надолу. Тук се открояват три задачи: изграждане и поддържане на постоянен европейски щаб по отбраната, постоянни европейски сили за бързо реагиране, които да са на разположение в случаи на кризи и европейска „бяла книга за отбраната“, като първообраз на европейска „отбранителна стратегия“.

Трите задачи са твърде амбициозни и изискват промени в договора на ЕС. Идеята не е да се премахнат националните армии, но в определен момент, извън рамките на съществуващия договор, Европейскияt съюз да притежава общи сили, където граждани от всички европейски страни да могат пряко да кандидатстват, да се обучават и да служат. Да има нещо на общо европейско разположение в случай на нужда. Това не трябва да бъде чуждестранен легион. Това трябва да е легион на Европа, под политически контрол на Европейския съюз, с европейско командване.

Европейскияt съюз вече има част от елементите на общата отбрана като например общо военно командване на цивилни и военни мисии, общ ситуационен център, общ оперативен център, който не се нарича “щаб”, защото Великобритания не е съгласна.

Европейският съюз се нуждае от нови стратегически документи, регламентиращи политическата рамка за вземане на решение в областта на общата отбрана.

Еволюционно изграждане на Европейски въоръжени сили от долу на горе „Европа пред свършен факт“[[21]](#footnote-21). През 2014 година Германия и Холандия стартират проект за създаване на европейска армия чрез сливане на части от двете национални армии. Според проекта 2100 холандски войници са под германско командване, но още не са определени германските военноморски части, които ще се контролират от холандците. Планът е да се създаде ядро на въоръжените сили на Европейския съюз. Срещу това се противопоставя Великобритания. Чешката република също е започнал преговори за участие в проекта. За пръв път в историята батальон от 600 немски войници ще премине под полско командване. На реципрочни начала полски батальон ще се командва от германците. Все още не е ясно кои точно части ще участват в размененото командване, но се предполага, че те ще са базирани по полско-германската граница и че промяната ще влезе в сила в средата на 2016 г.

В заключение, през ХХI век Европейския съюз трябва да може да използва военна сила, за да защитава и налага своите интереси и защитава своите ценности. Военна сила с изградена структура, способна да функционира в многостранна организация за сигурност с общи оперативни процедури, ефективна система за командване и контрол, ефективна логистична поддръжка, значителни транспортни възможности и добре подготвени и способни на взаимозаменяемост въоръжени сили.

Европа трябва да притежава: стратегически ресурси и най-доброто въоръжение и способности в света; широк спектър въоръжени сили с равнище на умения, които им дават възможност да изпълнят мисия от всякакъв мащаб; способност да се предоставят на международни организации широки и многовариантни възможности за планиране; Механизъм да се изработва и допринася за базисен политически консенсус по трудни въпроси.

Една съвместна европейска армия ще изпрати ясен сигнал към света, че Европа е готова и подготвена да поема отговорност за собствената си сигурност и отбрана. За да стане потенциалът реалност обаче, трябва политическа воля. Тя все още липсва. Отбраната е на книга обща политика, а на дело – национално поле на компетентност. Задължителното общо съгласие за европейски решения се постига трудно.

**Използвана литература:**

Ще има ли Европа собствени въоръжени сили? **a-specto. 31.08.2015 г. . http://a-specto.bg/eu-army/.**

Договорът от Лисабон – отражение върху политиката за сигурност и отбрана на Европейския съюз, изводи и перспективи за България. МО на Република България. Дирекция „Политика за сигурност и отбрана”. София 2009.

Ще има ли Европа армия? http://glasove.com/categories/komentari/news/shte-ima-li-evropa-armiya.

1. **Христо А. Христов. Аспекти на общата политика за сигурност и отбрана на Европейския съюз.**

## Jérôme Legrand. Обща политика за сигурност и отбрана. Европейски парламент. 11.2015. <http://www.europarl.europa.eu/atyourservice/bg/displayFtu.html?ftuId=FTU_6.1.2.html#_ftn1>.

European Aeronautic Defence and Space Company (EADS). <http://www.britannica.com/topic/European-Aeronautic-Defence-and-Space-Company>.

1. Secret Plot Exposed: EU in stealth plan to set up army by merging German and Dutch forces. An EU armed forces is being set up "by stealth" with the merger of the German and Dutch armies and navies, it has emerged. By David Maddox. <http://www.express.co.uk/news/politics/662472/EU-federal-europe-European-army-merging-German-Dutch-forces>.
2. Maddox. <http://www.express.co.uk/news/politics/662472/EU-federal-europe-European-army-merging-German-Dutch-forces>

**Основни характеристики на асиметричната война в теорията на военното изкуство и стратегиите за сигурност през ХХI век**

*ас. д-р Радослав Бонев*

*Военна академия „Г. С. Раковски“*

***Резюме:*** *Докладът представя съвременното разбиране за развитието на основните характеристики на асиметричната война през призмата на теоретичните нива във военното изкуство-стратегическо, оперативно и тактическо, обвързвайки влиянието на асиметричния характер на военните конфликти от ХХI век върху стратегиите за сигурност. Военноисторическият подход в изложението се стреми индирктно да интерполира с понятия, които днес се приемат за базисни в различни изследователски конструкции, отнасящи се до теорията на хибридната война.*

***Ключови думи:*** *асиметрия, асиметрична заплаха, асиметрична война, стратегии за сигурност.*

Според Националната отбранителна стратегия на Република България (2011 г.) *„Стратегическата среда на сигурност е сложна, динамична и с трудно предвидими измерения. Влияние върху формирането й оказват: глобализацията; кризисните явления във финансовата и икономическата сфера; разпространяването на оръжията за масово унищожение и на средства за тяхната доставка; климатичните и здравните проблеми; демографските, екологичните и енергийните проблеми;* ***асиметричните рискове и заплахи****; заплахите за информационната сигурност; страните със слаба държавност; вътрешните и регионалните конфликти; европейската и евроатлантическата интеграция; усилията на международната демократична общност за поддържане на мира и стабилността”*.[[22]](#footnote-22)

Динамиката на международните отношения през XXI век показва, че в последните години продължава да се игнорира очертаващата се тенденция за нарастване на относителния дял на въоръжени сблъсъци между неидентифицирани въоръжени групировки по етнически, религиозни, финансови, териториално-общностни и други противоречия*.*Радикалните промени, настъпили в последното десетилетие на ХХ и в началото на ХХI век, формираха съвсем нова стратегическа среда на сигурност и съотношение на военно-политическите сили в глобален и регионален мащаб. Наред с положителните тенденции съществуват и редица рискове и заплахи, най-вече такива от **асиметричен характер**. От една страна светът е по-единен, а от друга - по-разпокъсан.

След края на Студената война съществува определен риск за легитимността на трите „основни стълба” в международната правосубектност на отделни страни в конфликтни региони - *държавният модел, ненарушимостта на границите и ненамесата във вътрешните работи.* Модерните технологии намаляват значението на географската отдалеченост, увеличават разнообразието от средства и броя на субектите, способни да извършват насилие.*Показателен за това е фактът, че ако през 50-те години на XX век в света са регистрирани средногодишно по 10-12 военни конфликта, то в началото на 90-те години на миналия век техният брой нараства четирикратно.*

В резултат на тези промени възникват нови предизвикателства, рискове и заплахи за сигурността. Влизат нови „актори”, редица нови „въоръжени субекти”, като разпадащи се държавни военни сили, полувоенни формирования (обикновено финансирани от правителства), части за самоотбрана, политически и други организации, финансово-икономически и бизнес корпорации, наемници, престъпни мафиотски образувания и наркокартели, секти, терористични групи и други. В много случаи неправителствени организации подменят държавните структури или се опитват да излязат извън контрола на държавата. С отслабване на държавата недържавните формирования набират все по-голяма сила и авторитет. От 28 големи конфликта през 1991 г. в 25 от тях едната от противоборстващите страни е била от нередовни сили[[23]](#footnote-23).

Към тях се отнасят:

- полувоенни групи, организирани от харизматичен лидер;

- военни барони, контролиращи определени райони;

- терористични клетки, доброволци фанатици;

- организирани криминални групи;

- части и подразделения на редовни въоръжени сили и други силови ведомства.

Ето защо, според изследването „Войната на бъдещето-поглед отвъд океана” (Война будещего: взгляд из-за океана), което цитира проф. д-р Мартин ван Кревелд, ***„въоръжените конфликтиднес не представляват класическо стълкновение между две армии на бойното поле, а избухване на кръвопролитно насилие”***, поетапното осъществяване на т. нар. ***стратегии******на „принудата”, „стратегически паралич”, „разрушаването” („унищожаването”)*** и операции за ***„стремително доминиране”*** в противниковата държава или актор[[24]](#footnote-24).

Интерес представляват и възможните стратегически сценарии на Бжежински за провокиране на военен конфликт, особено три от тях:

-ожесточени атаки на иначе слаби държави, сдобили се с ОМУ;

-смъртоносни терористични атаки от страна на нелегални (неформални) организации и групировки с използване на ОМУ;

-парализиращи кибератаки срещу операционната инфраструктура на развитите общества[[25]](#footnote-25).

Друга модерна теза в днешната епоха е, че междудържавните войни отстъпват място на проникващите през всякакви граници конфликти[[26]](#footnote-26).

Съвременната стратегическа среда на сигурност и новите технологични реалности изведоха на преден план нов тип заплахи, дефинирани като асиметрични, като резултат от т. нар. „нетрадиционно насилие”[[27]](#footnote-27).

Терминът **„асиметрия”** е отно­сително нов и служи за представяне на различните видове нестандартни запла­хи и потенциални възможности.

Доц. д-р Георги Цветков твърди, че асиметрията съществува от времето на зараждането на военната наука и практика и противопоставянето между различните племенни и междудържавни общности. Асиметрия във военното дело означава *използване на различията с цел постигане на предимство над противника[[28]](#footnote-28)*. Библиографският обзор[[29]](#footnote-29) от последни­те години в теорията на международните отношения и конфликтологията показва, че „асиметрията” се очер­тава като все по-значим елемент на възможностите за анализа на: *„асиметрични заплахи”, „аси­метричен конфликт”, „асиметрична война”[[30]](#footnote-30)* в стратегическата среда на сигурност, а оттам и в стратегиите за сигурност.

Според доц. д-р Митко Хинков[[31]](#footnote-31) и проф. д-р Лариса Дериглазова[[32]](#footnote-32) най-често понятието „асиме­трия” се използва за характеризиране на отношенията между несъпоставими по мощ и статут противници. С изключение на някои военностратегически и нормативно-правни анализи (сравнително малко на брой) подчерта­ването на асиметричността е свърза­но с парадоксалния характер (използвайки корелативния модел за сравнение на проф д-р Едуард Лютвак[[33]](#footnote-33) и трансформацията в разбирането за войната от военната теория и практика, представена от проф. д-р Мартин ван Кревелд) на отно­шенията, при които по-слабият про­тивник е в състояние да нанесе сериоз­ни загуби и дори да наложи волята си над по-силния, като силният не винаги може да отстои интересите си и да подчини слабия[[34]](#footnote-34).В строго научния смисъл под „асиметрия” се разбира липсата или нарушаването на симетрията при обекти, на които е свойствено наличи­ето на подобна симетрия, или пък съче­танието на обемно-пространствени елементи, за което е характерно лип­сата на симетрия.

***Връзката на стратегиите за сигурност с аси­метрията се изгражда върху допустимото възможно противо­поставяне на симетрията, на класическото разбиране за „линейната”, „предсказуемата” стратегия, т.е. тя се представя като отсъствие на ра­венство между частите на цялото и като фактическо нарушаване структу­рата на анализирания обект, неравен­ство или несъразмерност.***

Съществуват *пет кри­тични компонента* на асиметрията, които оказват влияние на стратегическата среда на сигурност, а оттам въздействат и на стратегиите за сигурност:

*-Асиметрия на волята.* *Тя е важна, когато единият противоборстващ вижда оцеляването или жизненоважния си интерес в опасност, или е воден от силна радикална или екстремистка иде­ология, докато другият не вижда това или не се води от такава идеология;*

*-Асиметрия на средствата.* Техно­логията винаги е била предимство във военната история, особено във войните, в които се противопоставят технологични еди­ници срещу по-слабо напреднал в тази област противник. Изходът от така­ва конфронтация е ясен, особено кога­то по-слаборазвитият опонент няма времето или способността да се адап­тира към напредналите технологии. Де­мографските особености също могат да се използват като оръжие и да бъдат решаващ фактор на асиметри­ята, на противоборството на по-слабия срещу по-силния, като „компенсация” за неговото технологично изоставане в средствата за водене на военните действия;

*-Асиметрия на метода и поведени­ето.* Тази форма се проявява, когато единият от опонентите използва раз­лични морални принципи, закони, док­трини или тактически процедури, за да спечели предимство;

*-Асиметрия на Времето.* Може да се прояви, когато един от антагонис­тите вижда конфликта отвъд грани­ците на времето, в което противнико­вите операции са ограничени според продължителността на конфликта. Скоростта на реакция и очакването са също важни фактори, свързани с вре­мето;

*-Асиметрия на организацията.* Ор­ганизационната структура и нововъве­денията в нея могат да осигурят зна­чително предимство и пред техничес­ки по-силен противник[[35]](#footnote-35).

Факторите, които определят есте­ството на асиметричността на стратегическата среда на сигурност, оказвайки въздействие върху стратегиите за сигурност и военните (отбранителните) стратегии, могат да бъдат следните:

-*физическа среда* (физикогеографска и икономогеографска характеристика на стратегическата среда на сигурност);

-*участниц*и (официални и неофициални);

-*етнокултурни фактори* (включително социологически, религи­озни и психологически);

-*икономически аспекти и геодемографски фактори*;

-*регионални и глобални политически взаимоотноше­ния.*

Тези фактори въвеждат различни видове тактики, техники и процедури, които се използват в партизанска вой­на, при терористични атаки, прилага­не на оръжие за масово поразяване и други видове нелинейни начини на дей­ствие. Официалните и неофициалните участници могат да предизвикат стра­тегически ефекти, използвайки неконвенционални методи като бунтове или различни кампании срещу дадени поли­тически решения.

Началото на военната операция в Ирак през 2003 г. и неспособността на коалицията да завърши войната в съответствие с първоначалните пла­нове и да установи пълен контрол над страната след разгрома на нейната армия, както и трансформацията на военните действия в партизанска вой­на се определят от анализаторите като пример за класически „асиметри­чен конфликт”, който може да се срав­ни с войната във Виетнам. В иракския конфликт е налице очевидна диспропор­ция между силовите възможности на противниците, техния статут и стра­тегия. Още през 60-те години на мина­лия век партизанските войни, водени в условията на окупация или колониално управление, както и националноосвободителните движения, са причислени към асиметричните конфликти[[36]](#footnote-36). Днешните реалности ни карат отново да ги анализираме като специфичен модел на въоръжено противопоставяне- кризата в Украйна и конфликтите в Сирия.

Ако се изведат на преден план съвпа­дащите елементи на споменатите слу­чаи, може да се определят и някои ос­новни черти на асиметричните кон­фликти, които имат своето въздействие върху стратегиите за сигурност/стратегическите концепции на държавата/съюза в практиката на съюзната (коалиционната) стратегия за ангажиране във военни действия:

-непредсказумост на резулта­та при очевидно несъразмерни силови възможности и статути на противо­стоящите страни;

-използване от стра­на на слабия участник на стратегия, изградена върху търсене „слабостите на силния”;

-използване от слабата страна на забранени средства за воде­не на военни действия;

-конкретна тактика на „не­преки” военни действия, прилагана от слабата страна;

-неспособност на силния за адаптация към спецификата на театъра на военните действия и др.[[37]](#footnote-37)

Например тероризмът в началото на XXI век представлява вариант на асиметрични бойни действия, тъй като изразява логиката на борбата на „слабите” срещу „силните”.

*Следователно, тероризмът като средство за борба на „слабите” е заменил партизанската война, която в продължителен период от време изпълнява тази функци,*т.е., разликата между конвенционалната партизанската война и терористичните стратегии е в съзнателното използване на *парадоксалните предимства на стратегическата асиметрия.*

През втората половина на ХХ век в теорията на международните отношения и теорията на военната стратегия, както и в практиката на международнта политика, съществува стремеж за съобразяване със спецификата на асиметричните конфликти. В началото на ХХI век част от водещите държави се опитват да адаптират стратегиите за сигурност и отбранителните политики, отчитайки обособилата се реална възможност за възникването на асиметричност при осигуряване на национлната им сигурност. В тази посока се очертават следните по-характерни тендинции, които са *специфичен аргумент* за влияние върху стратегиите за сигурност, националните военни (отбранителни) стратегии и доктрините за организацията и използването на видовете въоръжени сили:

-осъществяване на превантивни действия срещу асиметрични против­никови формирования и оптимално из­ползване на данните от разузнаването и агентурните мрежи;

-подготвяне на въоръжените сили за водене на бойни действия със срав­нително малки по численост контин­генти от специално подготвени воен­ни части;

-осъществяване на превантивни действия срещу асиметрични против­никови формирования и оптимално из­ползване на данните от разузнаването и агентурните мрежи;

-ограничаване мащабите на военни­те операции и преминаване към нево­енни средства за натиск срещу по-слаб противник;

-осъществяване на мерки за осигу­ряване на постоянен контакт с мест­ното население, за чийто защитник се обявява по-слабият противник, както и оказване на военна и материална по­мощ на собствените привърженици в местното общество.

Определението асиметрична война има различни значения на всяко ниво, защото:

*-на стратегическо ниво* (стратегия за сигурност, национална военна /отбранителна стратегия) във фоку­са на определението е вероятно да се включват сигурност и влияние на съответната нация;

*-на оперативно ниво* (доктрини за организация, бойно използване и осигуряване на видовете въоръжени сили) може да се съсредоточи върху косвените подхо­ди за планиране и провеждане на кам­пании и операции;

*-на тактическо ниво*(действия на тактическите формирования от видовете въоръжени сили) фокусът е ве­роятно върху асиметрични приложения на тактики, техники и процедури (ТТП), които могат да бъдат прила­гани по различен начин в операция на асиметрична война в сравнение с кон­венционална операция[[38]](#footnote-38).

Нова опасност от глобален мащаб са възникващите многочислени вътрешнодържавни въоръжени конфликти, провокирани вследствие на политически, религиозни и етнически противоречия между техните граждани. Нерядко такива конфликти придобиват затегнат характер и прерастват в масов тероризъм, във въстанически движения, в граждански войни.

Използването на паравоенни формирования се налага като неизменен компонент на по-голяма част от асиметричните конфликти. Тези формирования като неформални сили, които не са подчинени на командването на редовните въоръжени сили, имат изградена структура и мрежова организация.

**Кои са най-важните идеи, които определят особеностите и основните характеристики на съвременната асиметрична война?** Това са:

-асиметричната заплаха;

-информационната технология, която коренно промени природата на войната;

-разбиването на цикъла на вземането на решение на противника, което определя победителя в бойните действия;

-цифровите комуникации, които променят начина на организация на военната сила.

Взети заедно, тези идеи не подсилват просто традиционните способи за водене на войната, а коренно преобразяват нейната природа. Те по-скоро преобръщат основните предпоставки за планирането и воденето на войни. Тук отново се връщаме към понятието *„асиметрична заплаха”* като ключово при определяне на съдържанието на асиметричната война. За същността на „асиметричните заплахи” има доста определения, като едно от тях е, *„че асиметричната заплаха представлява мислене, организация и действие, различни от тези на противника, с цел да се увеличат съответните предимства, да се използват слабостите на противника, да се запази инициативата или да се спечели по-голяма свобода на действие”[[39]](#footnote-39)*. Заслужава внимание формулировката, че „асиметричните заплахи” и „опасности” обикновено се представят като *асиметрия между усилията, които са нужни за осъществяване на разрушително въздействие, последиците от оказаното деструктивно въздействие и усилията, които са необходими то да бъде предотвратено, а ако се случи, последиците от него да бъдат неутрализирани.* Тези усилия, за да бъдат сравнявани, следва да бъдат измервани с една и съща мерна единица”[[40]](#footnote-40). Основното в определенията за асиметричните заплахи е наличието на термина „асиметрия”, който беше описан подробно.

Необходимо е да приемем, че основателно се подчертава *съществуващата връзка* между стратегия/стратегическата концепция за сигурност на държавата/съюза и концепцията за т.нар. „асиметрична война”[[41]](#footnote-41). Именно от нея се ръководят водещите държави, съюзи (коалиции), разработвайки стратегии за сигурност, стратегически концепции, военни (отбранителни) стратегии, стратегии за борба с тероризма, както и плановете за организационно развитие на видовете въоръжени сили. При това не се обръща достатъчно внимание на факта, че модерната асиметрична война все повече се доближава до т.нар. **„бунтовнически войни”** (или „метежни войни”) – термин, въведен от руския военен теоретик -полковник проф. Евгений Меснер. Според Меснер *„В света се води война, която ни заплашва с по-тежки бедствия, отколкото нахлуването на източните племена в Римската империя: защото някогашните варвари са рушели Рим и културата му, но в същото време са възприели и много неща от него, докато днешните само унищожават и то с такава фанатична упоритост, с каквато навремето културният Рим сравнил със земята съперника си Картаген”[[42]](#footnote-42)*. Анализирайки локалните конфликти и регионалните войни след края на Студената война, забелязваме, че начинът на воюване се съпровожда с нанасянето на асиметрични удари от страна на различни организации, терористични саботажни групи, или отделни индивиди, като подбудите им трудно се поддават на точна класификация – сред тях са политически мотивираното желание на една от странитe (обикновено по-слабата във военно и/или социално-икономическо отношение) да „отмъсти на окупатора”, „освобождаването на страната”, „осъществяването на политическо-социален преврат” и т.н. Наличието на подобна смес от различни идеологии, принципен протест и безпринципна възможност за разрушаване, няма как да не определим като „метеж” (или „бунт”). Евгений Меснер подчертава, че: *„именно този термин започнах да използвам в трудовете си, издадени след Втората световна война[[43]](#footnote-43). Тази война приключи през 1945, но метежът продължи. През годините той се разширяваше, придобивайки такава сила и всеобхватност, че в крайна сметка се превърна в нова специфична форма на военни действия, която лично аз определям като „метежна” или „бунтовническа” война”[[44]](#footnote-44)*.

По-късно тезите на Меснер са развити от американския полковник Джон Бойд (1927-1997), известен като стратега на Първата война в Залива през 1991. Тълкувайки Меснер Бойд възприемаме, че „бунтовническата война” е съвременната форма на война. Тя отхвърля традиционните военни норми и шаблони. Участниците в нея не признават класическите, грандиозни, масови сражения. Срещу масовите национални армии те използват **„тактиката на комара”**, а също терора, бандитизма, въстанията, уличните безредици и демонстрациите. Оперативният ход на „бунтовническите” войни преминава през следните фази: деморализация, хаос, терор, постепенно приобщаване към революционната кауза и духовна трансформация на индивида. Крайна цел на стратегията на „бунтовническата” война е разрушаването на държавната структура, защото, както е формулирал Сун Дзъ, *„разрушената държава не може да бъде възстановена, както и мъртвият не може да бъде върнат към живота”*.

В една от последните си статии, озаглавена „Терорът”, Меснер отбелязва: *„Налице са признаци, че в съвсем скоро време агресията на рушителите на Структурата значително ще се усили. Структурата (държавна, обществена, финансова и особено моралната) е обречена да загине, смазана от този натиск, ако не се съпротивлява срещу него (терора-б.а.) и то с военни средства”*. Днес светът се сблъсква тъкмо с такъв тип агресия на международната терористична мрежа като цяло[[45]](#footnote-45). И в тази разгаряща се „бунтовническа” война, партизанските действия, тероризмът и психологическата война (както предвижда и Меснер) играят ключова роля. В статията си „Тероризмът днес. Войната става асиметрична”[[46]](#footnote-46) споменатия германски анализатор Херфрид Мюнклер подчертава, че: *„Терористичната заплаха се характеризира, по правило, с асиметричното разположение на силите. В миналото тероризмът и, разбира се, стратегията на партизанската война, също бяха форми на асиметрична война, но почти винаги тази асиметрия отразяваше слабостта на революционерите или партизаните. С нарастването на силите им, асиметрията постепенно изчезваше. Именно нарастването на силите и постигането на възможност за симетричен удар беше цел на почти всички партизански войни през ХХ век и основа на маоистката партизанска доктрина”[[47]](#footnote-47)*. В най-новите форми на транснационалния тероризъм подобно нещо липсва. Асиметричната конфронтация вече не се разглежда като стъпало към постигането на желаната симетрия, т.е., перспективата за постигане на силов баланс с противника въобще не се разглежда. Възприемането на тази нова стратегия има много сериозни и далеч отиващи последици[[48]](#footnote-48). Тя е доказателство за това, колко реалистично оценяват ситуацията онези, които планират и осъществяват терористичните кампании днес, т.е. най-новите форми на тероризма се базират на това, че не разглеждат асиметрията като временно състояние, а като своеобразен ключ към успеха. Затова те не предвиждат открит военен сблъсък със западните държави дори и в отдалечено бъдеще. Напротив, правят всичко възможно да няма такъв сблъсък. Съвременните терористични организации са зависими в далеч по-голяма степен от слабите места в инфраструктурата на страните, които са избрали като обект на поредната си атака, защото използват елементите на тази инфраструктура като „оръжие за възмездие”. Всичко това позволява на относително слаби „играчи” на международната сцена да се превърнат в смъртоносно предизвикателство за силните във военно отношение държави. Съвременната асиметрична или „бунтовническа война” (която мнозина не без основание определят и като най-голяма заплаха на ХХI век) е доминиращ компонент на постмодерния многополюсен свят, чиято характерна особеност е същественият спад на значението на такъв фактор, като междудържавните въоръжени конфликти и класическите бойни действия. Вместо това, на преден план излизат други приоритети, произтичащи от очерталата се система на глобални и нетрадиционни заплахи, повсеместно изострящи се на различни нива етнически, конфесионални и социално-икономически противоречия, фрагментацията на съюзните (коалиционните) военно-политически взаимоотношения, факторът на многобройните „малки войни” (асиметрични, „бунтовнически войни”, или „конфликти с ниска интензивност”).

Следователно, върху стратегиите за сигурност праз ХХI век, влиянието на средата на асиметричните конфликти и асиметричната война ще се изразява чрез:

*-фактори и тенденции в глобален мащаб*, които оказват въздействие върху воденето на асиме­тричната война на стратегическо, опе­ративно и тактическо ниво. Те включ­ват въздействието на глобализацията, икономическия „стрес”, преобладаващо­то чувство за несигурност, разочаро­ванието сред голяма част от населе­нието от социално-икономическото развитие на отделни и изолирани региони, международния тероризъм, бор­бата между отделните култури и ха­рактера на операционната среда[[49]](#footnote-49).

*-в бъдеще глобализацията ще бъ­де мощна сила,* която съществено ще влияе върху характера на конфликти­те. Новите информационни технологии ще могат да бъдат използвани и от терористите. Това ще им позволи да провеждат децентрализирано планира­не и обучение и да поддържат виртуал­на комуникация между различните еди­ници[[50]](#footnote-50).

*-културата, обществата, социал­ните организации, икономиките и рели­гиите* играят важна роля в асиметрич­ната война. Необходимо е да се позна­ват културата и социалният живот на противника, за да се разбере начинът му на мислене. При асиметричната война социологията, психологията и историята имат съществено влияние върху характера на конфликта, вклю­чително за неговата продължител­ност и интензивност.

-*растящото многообразие на източниците на конфликти и непредсказуемостта на тяхното възникване прави геополитическата обстановка непредсказуема*.

**Използвана литература:**

Попов, И. Война будещего: взгляд из- за океана. М., изд. АСТ „ Астрель, 2004, Глава 4. „Нетрадиционные” войны будущего

Бжежински, З. Изборът. С., изд. Обсидиан, 2004 г.

Семерджиев, Цветан. Стратегическо ръководство и лидерство. Среда.С., 2007.

Цветков, Георги. Концепция на НАТО за асиметрични военни действия. // Военен журнал, 2008, бр. 3

Laffin John.The World in Conflict 1991. Oxford: Brassey’s, 1991

S. Flynn.R. Wedgwood and K. Roth: Combatants or Criminals? How Washington should handle terrorists // Foreign Affairs. 2004. Vol. 83. No 3

I. Arreguin-Toft, How the Weak Wins Wars: A Theory of Asymmetric Conflict //International Security. 2001. Vol. 26. No 1.

Herfried Munkler, "Uber den Krieg. Stationen der Kriegsgeschichte im Spiegel ihrer theoretischen Reflexion". Frankfurt am Main: Velbruck Wissenschaft, 2002

Социология современных войн: Материалы научного семинара / Под ред. П.А. Цыганкова, И.П. Рязанцева. М.: Альфа-М,, 2004; Мюнклер Х. Терроризм сегодня. Война становится асимметричной // International Politik. 2004. № 1

Мейз М. Эпоха стратегической асимметричности: Способность использовать нетрадиционные способы ведения войны определяет победу // Независимое военное обозрение. 2005. № 14; Генис А. Асимметричная война. (<http://www.svoboda.org/programs/OTB/2003/OBT.082303.asp>)

Комлева Н., Борисов А. Асимметричные войны – геополитическая технология современного терроризма // Обозреватель. 2002. № 11-12 (http://rau.su/observer/ N11-12\_02/index.htm).

America the vulnerable // Foreign Affairs. 2002. Vol. 81. No 1.

FIуnn, S., R Wedgwood, К. Roth. Combatants or Criminals? How Washington should handle terrorists. - Foreign Affairs, 2004, Vol. 83, No 3.

Arreguin-Toft. How the Weak Wins Wars: A Theory of Asymmetric Conflict. - International Security, 2001, Vol. 26, No 1.

Кременюк В.А. Современный международный конфликт: проблемы управления // Международные процессы. 2003. № 1.

Хинков, Митко. Новата среда за сигурност и асиметричния характер на съвременните конфликти. // Военен журнал, 2010, № 1-2, 17-30, <http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1>

Професор, доктор по теория на международните отношения и геополитика в Томския държавен университет. <http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1>

Люттвак, Эдвард. Стратегия: Логика войны и мира. Пер. с англ. М., Университет Дмитрий Пожарский”, 2012.

Бъркоуиц, Б. Новото лице на войната. С., ВИ, 2003.

Христов, П. Проблеми на регионалната сигурност в условията на асиметричните опасности и заплахи. С., Научен алманах, ВСУ „Ч. Храбър” и Фондация „Ханс Зайдел”, 2008.

Савов, Александър. Асиметрична война. //Геополитика, 2006, бр. 4. http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1

Хочешь мира, победи мятежевойну. Творческое наследие Е. Э. Месснера, М. Военный университет, Русский путь, 2005.

Стратегия за национална сигурност на Република българия <http://rdsc.md.government.bg/BG/About/Akademi/20110421_nac_otbr_strategia.pdf>

**МОРСКИТЕ ОПЕРАЦИИ НА ЕВРОПЕЙСКАТА АГЕНЦИЯ FRONTEX В ОТГОВОР НА НОВИТЕ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИГУРНОСТТА В РАЙОНА НА ИЗТОЧНОТО СРЕДИЗЕМНОМОРИЕ**

*доктор Калоян Панчелиев*

*Университет по библиотекознание и информационни технологии*

***Резюме:*** *В доклада са представени новите предизвикателства пред сигурността, породени от интензивния трафик на мигранти от Турция към Гърция през 2014 – 2015 г. В центъра на анализа са морските операции на европейската агенция Frontex в района на Източното Средиземноморие, включително и участието на България с гранично-полицейски кораб „Обзор“ (525) през 2016 г. Посочват се възможности за усъвършенстване на съществуващия модел за провеждане на операциите по отношение на неговата организация и управление.*

***Ключови думи:*** *мигранти, морски операции, организация и управление*

В периода 2014 – 2015 г. Европа се изправя пред най-голямата мигрантска криза след Втората световна война (1939 – 1945). Причините за кризата се разглеждат от Европейската комисия (ЕК) в контекста на *„жестоките конфликти в Сирия и Ирак или нестабилността и бедността в някои части от Африка, които принуждават милиони жени, мъже и деца да напуснат своята родина в търсене на защита и по-добър живот“*[[51]](#footnote-51) в други страни, включително и в Европейския съюз (ЕС). Общият брой на мигрантите, които пресичат външните граници на ЕС в периода януари – септември 2015 г. е над 710 000 хил. души според данни на европейската агенция Frontex.[[52]](#footnote-52) Значителен брой (над 300 000 хил. души) пристигат в района на гръцките острови, разположени в източната част на Средиземно море.

През 2015 г. Фредерика Могерини, върховен представител на ЕС по въпросите на външните работи и политиката на сигурност определя мигрантската криза като криза на сигурността.[[53]](#footnote-53) В действителност интензивният трафик на мигранти от Турция към Гърция поставя нови предизвикателства пред сигурността в Източното Средиземноморие. В различни публикации като такива се визират проникването на радикални ислямисти от Сирия и Ирак в Европа, производството и разпространението на наркотици, фалшиви документи и парични знаци, прането на пари[[54]](#footnote-54), контрабандата на хора, оръжия и забранени товари[[55]](#footnote-55), финансирането на терористични дейности от мрежите за контрабанда[[56]](#footnote-56) и др.

В отговор на новите предизвикателства пред сигурността ЕС провежда морски операции с международно участие с цел извършване на координирани оперативни дейности по външните морски граници в региона на Източното Средиземноморие, контролиране на незаконните миграционни потоци към територията на държавите-членки на ЕС и справяне с трансграничната престъпност.

**Обект, предмет и цел на изследване**

Обект на изследване са морските операции на европейската агенция Frontex в района на Източното Средиземноморие. Предмет на изследване са организацията и управлението на морските операции. Целтана изследванетоена базата на анализа и оценката от морските операции, проведени в периода 2014 – 2015 г. да се направят изводи и препоръки за трансформирането на Агенцията в Европейска гранична и брегова охрана (EBCG) и усъвършенстване на нейната организация и управление.

**Структура**

Структурата на доклада включва резюме, ключови думи, увод с посочени обект, предмет и цел на изследването, основни сведения необходими за разбиране на публикацията, изложение, обсъждане на резултатите, изводи и използвана литература.

**Основни сведения за агенцията Frontex**

Европейската агенция за управление на оперативното сътрудничество по външните граници на държавите-членки на Европейския съюз (Frontex) е създадена с Регламент (ЕО) № 2007/2004 на Съвета от 26 октомври 2004 г. В Регламента се посочват следните шест основни задачи на Агенцията:

* координира оперативното сътрудничество между държавите-членки в областта на управлението на външните граници;
* подкрепя държавите-членки за обучението на националните граничари, включително установяване на общи стандарти на обучение;
* извършва анализи на риска;
* следи за напредъка в изследванията, свързани с области, които представляват интерес за контрола и наблюдението на външните граници;
* подкрепя държавите-членки при обстоятелства, които изискват засилена техническа и оперативна помощ по външните граници;
* предоставя необходимата подкрепа на държавите-членки за организирането на съвместни операции по екстрадиция.[[57]](#footnote-57)

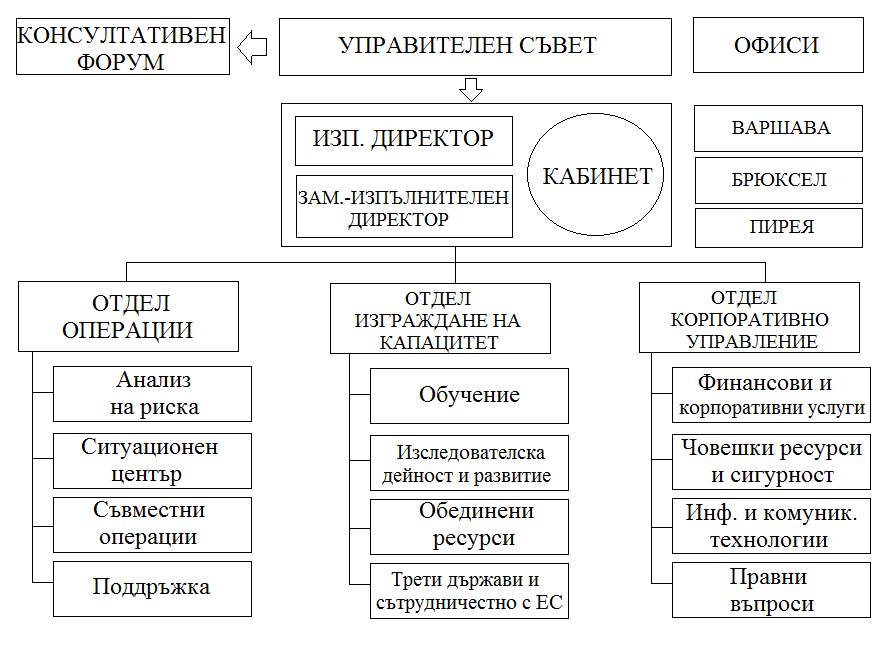
В периода януари – август 2014 г. броят на мигрантите, които пристигат от Турция в Гърция с плавателни съдове в района на Източното Средиземноморие е 22 577 хил. души. За същия период през следващата 2015 г. броят им достига 222 654 хил. души т.е. увеличението е с 886 %.[[58]](#footnote-58) Във връзка с интензивния трафик на мигранти ЕС активизира усилията си за спасяването на човешки животи и предотвратяването на жертви в морето. За целта се провеждат серия от морски операции, координирани от Агенцията, както следва:

* Операция Triton в централната част на Средиземно море;
* Операция Poseidon в района на Източното Средиземноморие.

През 2015 г. бюджетът за провеждане на операция Poseidon е 18 млн. евро, а на операция Triton – 38 млн. евро. През 2016 г. Европейската комисия (ЕК) ще предостави на Агенцията допълнителни средства в размер на 45 млн. евро за двете операции.[[59]](#footnote-59)

**Организационна структура на Агенцията**

В Регламента за създаването на Агенцията се отбелязва, че тя е юридическо лице и орган на Общността, има свой управителен съвет, който назначава изпълнителен директор по предложение на Комисията. Изпълнителният директор се подпомага от заместник-изпълнителен директор. Управителният съвет се състои от по един представител от всяка държава-членка и от двама представители на Комисията. Той излъчва председател и заместник-председател измежду своите членове и създава процедурен правилник и организационна структура на Агенцията. Освен управителен съвет, организационната структура на Frontex включва консултативен форум, кабинет на изпълнителния директор, офиси (във Варшава Брюксел и Пирея), три отдела, съответно „Операции“, „Изграждане на капацитет“ и „Корпоративно управление“ (фиг. 1). В отговорностите на първия отдел (с направления в дейността „Анализ на риска“, „Ситуационен център“, „Съвместни операции“ и „Поддръжка“) попада координирането и провеждането на съвместни операции по суша, въздух и море.



**Фиг. 1. Организационна структура на агенция Frontex[[60]](#footnote-60)**

Агенцията не разполага със собствени кораби, вертолети и самолети, но съгласно Регламента поддържа централизиран регистър на техническите средства за контрол и наблюдение на външните граници, които принадлежат на държавите-членки. Същите са готови да предоставят доброволно технически средства на други държави-членки, които отправят искане за ползването им след анализ на необходимостта и риска, изготвен от Frontex. Една или няколко държави-членки, изправени пред обстоятелства, които изискват по-широка оперативна и техническа помощ за изпълнение на техните задължения в областта на контрола и наблюдението на външните им граници, могат да се обърнат за помощ към Агенцията.

**Механизъм за предоставяне на техническа помощ**

В рамките на 5 дни след получаването на заявление за помощ и изготвянето на анализ на риска, изпълнителният директор на Frontex решава дали да бъде задействан механизма за предоставяне на помощ. Агенцията може да организира съответната оперативна и техническа помощ в интерес на държавата-заявител. При положително решение представителите на Frontex и държавата-заявител разработват план, в който се определят оперативната зона, видът на техническото оборудване и броят на полицейските служители, предназначени за участие в съответната операция. От своя страна Агенцията изпраща до останалите държави-членки заявление за предоставяне на техническа помощ и човешки ресурси. Frontex може да възстанови разходите за гориво и поддръжка на държавата-собственик на техниката след участието й в дадена операция.[[61]](#footnote-61)

**Инициативи в района на Източното Средиземноморие**

През август 2015 г. Агенцията определя основните осем маршрута[[62]](#footnote-62), използвани от нелегалните мигранти за влизане в ЕС, както следва: маршрут 1 (край бреговете на Западна Африка), маршрут 2 (през западната част на Средиземно море), маршрут 3 (през централната част на Средиземно море), маршрут 4 (през Калабрия и Апулия), маршрут 5 (обиколен маршрут от Албания към Гърция), маршрут 6 (през западната част на Балканския полуостров), маршрут 7 (през източната част на Средиземно море), маршрут 8 (през източните граници на ЕС, които преминават през следните държави в посока север – юг: Финландия, Естония, Латвия, Литва, Полша, Словакия, Унгария, Румъния и България).

Във връзка с маршрут № 7 от 2007 г. Агенцията засилва своето присъствие в района на Източното Средиземноморие и по-специално на островите в Егейско море и сухоземната граница между Гърция и Турция чрез различни инициативи, включително пилотни проекти, програми, операции и меморандуми за разбирателство. По-важните инициативи са следните:

* Пилотен проект Attica (2009 г.) в Гърция в рамките, на който Frontex осигурява експерти за установяване на страната на произход на мигрантите (т.нар. процедура „скрийнинг“), обучение за извършване на „скрийнинг“ и откриване на фалшиви документи и улеснява сътрудничеството с посолствата на трети държави;
* Екипи за бърза гранична намеса (RABITs)[[63]](#footnote-63), изпратени от Frontex в района на гр. Орестиада, североизточна Гърция в периода ноември 2010 г. – март 2011 г. Същите включват 175 експерти по граничен контрол от 26 държави-членки, които подпомагат страната в извършването на процедурите „скрийнинг“ и „дебрифинг“ и събират информация за маршрутите, използвани от мигрантите;
* Откриване на оперативен офис на Frontex в пристанище Пирея, Гърция на 1 октомври 2010 г. В организационно отношение той е подчинен на централата на Агенцията във Варшава, през 2012 г. в него работят 7 души, а през 2013 г. – 10 души;
* Меморандум за разбирателство между Frontex и Турция, подписан на 28 май 2012 г. В него са предвидени възможности за обмен на информация, участие в съвместни операции за връщане на незаконни мигранти, обучение в областта на управлението на границите, научно-изследователска и развойна дейност и др.;
* Серия от операции Poseidon (в периода 2007 – 2011 г.) и Poseidon Sea (в периода 2012 – 2015 г.) в района на Източното Средиземноморие (таблица 1);
* Съвместна операция Poseidon Rapid Intervention в района на Източното Средиземноморие, която заменя операция Poseidon Sea, считано от 28 декември 2015 г. и продължава през 2016 г.[[64]](#footnote-64)

|  |  |  |  |
| --- | --- | --- | --- |
| Период | Операция | Страна-домакин | Бюджет, евро |
| 15.05 – 7.10.2007 | Poseidon | България, Гърция,  Италия | 2,250,000.00 |
| 5.05 – 15.12.2008 | Poseidon | България, Гърция | 8,103,542.90 |
| 11.03 – 28.10.2009 | Poseidon | Гърция | 12,886,993.00 |
| 1.04 – 31.12.2010 | Poseidon | Гърция | 12,430,000.00 |
| 1.04.2011 – 31.03.2012 | Poseidon | Гърция | 11,588,926.00 |
| 1.04.2012 – 31.03.2013 | Poseidon Sea | Гърция | 9,166,702.00 |
| 1.04.2013 – 30.04.2014 | Poseidon Sea | Гърция | 8,640,674.00 |
| 1.05.2014 – 31.01.2015 | Poseidon Sea | Гърция | 6,626,661.75 |
| 1.01.2015 – 31.01.2015 | Poseidon Sea 2014 Extension | Гърция | 552,221.81 |
| 1.02.2015 – 27.12.2015 | EPN Poseidon Sea | Гърция | 19,960,291.22 |
| от 28.12.2015 | Poseidon Rapid Intervention | Гърция | NA |

**Таблица 1. Операции на Frontex в Източното Средиземноморие (2007 – 2015 г.)**

**Операции на Frontex в периода 2014 – 2015 г.**

В периода 1 май 2014 – 27 декември 2015 г. се провеждат три операции Poseidon Sea със страна-домакин Гърция и общ бюджет над 27 млн. евро (таблица 1). Целите на операциите са: извършване на координирани оперативни дейности по външните морски граници в региона на Източното Средиземноморие, контролиране на незаконните миграционни потоци към територията на държавите-членки на ЕС и справяне с трансграничната престъпност. В първата операция участват 22 държави: Австрия, Белгия, България, Великобритания, Германия, Дания, Естония, Исландия, Испания, Италия, Латвия, Малта, Нидерландия, Норвегия, Полша, Португалия, Румъния, Словакия, Финландия, Франция, Хърватска и Швеция. Втората операция по същество представлява продължение с един месец на първата и съответно получава наименованието Poseidon Sea 2014 с добавката Extension въпреки, че се провежда през януари 2015 г. В нея участват само държавите Белгия, Нидерландия, Португалия и Финландия, а страна-домакин отново е Гърция.

В периода 1 февруари – 27 декември 2015 г. се провежда съвместната операция EPN Poseidon Sea. В нея участват 22-те страни от първата операция плюс още 6: Албания, Кипър, Литва, Република Чехия, Словения и Украйна.

**Българското участие**

През декември 2015 г. Гърция изпраща до Агенцията искане за съдействие във връзка със засилването на миграционния натиск в района на Източното Средиземноморие. В искането се посочва, че страната се нуждае от техническо оборудване (патрулни кораби и лодки, вертолети, автомобили, камери) и служители от екипите за бърза гранична намеса. В отговор на гръцкото заявление за съдействие Frontex взема решение да изпрати екипи на островите Хиос, Самос, Кос, Лерос и Лесбос в Егейско море, които са най-силно засегнати от нелегалната миграция.[[65]](#footnote-65)

Главна дирекция „Гранична полиция“ към Министерството на вътрешните работи (МВР) на Република България предлага в подкрепа на Гърция в района на Източното Средиземноморие да бъде изпратен гранично-полицейския кораб „Обзор“ (№ 525). В края на декември 2015 г. Агенцията одобрява участието на българския кораб с екипаж от 32 души[[66]](#footnote-66) и през 2016 г. той се включва в операция Poseidon Rapid Intervention. На 18 февруари 2016 г. „Обзор“ извършва три курса от гр. Митилини, разположен на о-в Лесбос до насрещния турски бряг (разстояние от 8 km) и спасява около 900 мигранти. Участието на кораба в спасителната операция се отбелязва в специално изявление на Ева Монкюр, говорител на Frontex.[[67]](#footnote-67)

В допълнение през април 2016 г. петима служители на дирекция „Миграция“ – МВР участват в първата успешна операция по принудително извеждане на чужди граждани от Гърция до Турция. За операцията съобщава пресцентърът на МВР.[[68]](#footnote-68) Българските служители са командировани в периода 3 – 29 април 2016 г. във връзка с искането на Агенцията за съдействие при изпълнението на дейности по реадмисия. На 4 април 2016 г. те участват в първата успешна операция в рамките, на която са върнати принудително 87 чужденци (предимно граждани на Афганистан и Пакистан) с кораб от о-в Хиос, Гърция до гр. Дикили, Турция.

**Резултати**

Броят на нелегалните мигранти, които пристигат на гръцките острови през март 2016 г. намалява значително и възлиза на 26 460 души според данни на Frontex.[[69]](#footnote-69) Експертите от Агенцията определят като възпиращи фактори засиления контрол на границата между Македония и Гърция, влизането в сила от 20 март 2016 г. на споразумението между ЕС и Турция, активацията на операция Poseidon Rapid Intervention и новата операция на НАТО в Егейско море[[70]](#footnote-70).

Тенденцията за намаляването на броя на нелегалните мигранти в Източното Средиземноморие продължава и през първата половина на април 2016 г., когато средният брой на новопристигналите е по-малко от 100 души на ден. Подобряването на граничния контрол и напредъка в управлението на миграционните потоци се отбелязват от Фабрис Легери, изпълнителен директор на Frontex: *„…Благодарение на многобройните инициативи на Европейската комисия, Гърция, Турция и различните агенции на ЕС успяхме да подобрим контрола върху нашите външни граници и започваме да управляваме миграционните потоци по-добре, по един по-рационален и справедлив начин.“*[[71]](#footnote-71)

**Изводи и препоръки за усъвършенстване**

В края на 2015 г. Комисията предлага да бъде създадена Европейска гранична и брегова охрана (European Border and Coast Guard – EBCG) за постигането на по-ефективно управление на миграцията, осигуряването на силно и споделено управление на външните граници, подобряването на вътрешната сигурност на ЕС и съхраняването на принципа на свободно движение на хора. В съобщение на ЕК за медиите от 15 декември 2015 г. се посочва, че *„Европейската гранична и брегова охрана ще обедини Европейска агенция за гранична и брегова охрана, изградена въз основа на агенцията Frontex, и органите на държавите членки, отговарящи за управлението на границите, които ще продължат да извършват ежедневното управление на външните граници.“*[[72]](#footnote-72)Новата агенция ще разполага с резерв от гранични служители и техническо оборудване за бързо развръщане, център за мониторинг и анализ на риска, право на намеса, мандат за работа в трети страни, служба за връщане на нелегални мигранти и други възможности за извършване на своята дейност.

**Насоки за бъдещи изследвания**

Изследването е перспективно, защото може да послужи като отправна точка за бъдещи проучвания, включително сравнителен анализ на операциите с международно участие на агенция Frontex в Средиземно море и съответните национални операции за управление на миграционните потоци, провеждани от Гърция (Aspida и Xenios Zeus) и Италия (Mare Nostrum).

**Използвана литература:**

1. Лечева, М. Организация на оперативното сътрудничество по външните граници на ЕС. // *Научни трудове на Русенския университет*. *Издателски център към Русенски университет „Ангел Кънчев“*, том 52, серия 1.2, 2013, с. 182.
2. Cabot, H. On the Doorstep of Europe: Asylum and Citizenship in Greece. Philadelphia, 2014. 272 p.
3. Cardwell, P. EU External Relations and Systems of Governance. The CFSP, Euro-Mediterranean Partnership and Migration. New York, 2009. 264 p.
4. Ifantis, K. Addressing Irregular Migration in the Mediterranean. Brussels, 2012. 56 p.
5. Papastavridis, E. The Interceptions of Vessels on the High Seas: Contemporary Challenges to the Legal Order of the Oceans. Oxford and Portland, Oregon, 2013. 402 p.
6. Traublinger, J. Boat Refugees in the Mediterranean: Tackle the Root Causes or Build Fortress Europe. Hamburg, 2014. 49 p.
7. Triandafyllidou, A., Maroukis, T. Migrant Smuggling: Irregular Migration from Asia and Africa to Europe. New York, 2012. 238 p.

**Електронна идентификация и сигурност при електронните комуникации**

*доц. д-р Мария Николова*

*Нов български университет*

***Резюме:*** *Поради необходимост от използване на електронни публични услуги нараства нуждата от електронна идентификация за гражданите и бизнеса. Възниква въпрос как ще се постигне сигурност на данните при електронната идентификация. Секторната идентификация позволява по-високо ниво на сигурност. Изборът на идентификационен метод зависи от законодателството, стандартите, контрола и възможностите на дадена страна. Разгледани са системите за електронна идентификация – публична и частна. Проектът за електронна идентификация в България дава решения, които ще служат за бъдещото развитие в посока мобилни решения.*

***Ключови думи:*** *електронна идентификация, сигурност, електронни комуникации*

**Увод**

Според оценките на Gartner една от десетте стратегически технологични тенденции за 2016 година е електронната идентификация на гражданите (e-ID)[[73]](#footnote-73). Терминът “електронна идентификация на гражданите” се отнася към многобройни и интегрирани процеси и технологии, управлявани от администрацията, като целта е да се предостави на гражданите сигурен начин за достъп до публични услуги от всяко устройство или онлайн канал. Необходимо условие за успеха на електронната идентификация е партньорство между администрацията и бизнеса, като фокусът е да се постигне стойност, оперативна съвместимост и положителен ефект за потребителите.

**Електронна идентичност и електронна идентификация**

Съществуват понятията електронна идентичност и електронна идентификация. Електронната идентичност представлява идентификатор на физическото лице, удостоверен от държавен орган и съхраняван върху сигурен носител на електронната идентичност. Електронната идентификация е онлайн процес, чрез който се проверява предоставената електронна идентичност. Данните за идентификация позволяват да се определи самоличността на физическото или юридическото лице. Електронната идентификация позволява идентифициране на самоличността от разстояние. Чрез електронна идентификация е възможно да се осъществи електронно овластяване (делегиране на права) между две физически лица, между физическо лице и стопански субект или между два стопански субекта.

Секторната електронна идентификация е дериват, които се извлича при електронното разделяне на сектори и се извършва от държавата. Наличието на секторна идентификация цели прекратяване пренасянето на ЕГН и обмен на лични данни при идентификация. Данните за лице, притежаващо секторна идентификация, се трансформират по уникален начин и не съдържат лични данни. В секторната идентификация не се съдържа ЕГН, а псевдоним. Невъзможно е да се открие обратната информация - от псевдонима да се извлече ЕГН.

Първоначално за идентификация се използва електронният подпис. В България това е квалифицираният цифров електронен подпис. Поради факта, че в него се съдържат лични данни, които могат да идентифицират физическото лице, квалифицираният електронен подпис продължава да се ползва за идентификация. За уникален електронен идентификатор в България е приет ЕГН. Електронната идентификация е средство, чрез което може да се проведе електронно гласуване[[74]](#footnote-74). В Естония, където се гласува електронно, гражданите притежават електронна лична карта, която съдържа електронна идентификация и електронен подпис.

Правно-нормативната рамка определя доставчика на идентичност в лицето на държавата. Доставчикът в България представлява МВР като държавен орган. Европейският регламент изисква съвместимост между издадените в различните страни електронни идентификатори. Всички останали решения по отношение на правната рамка се вземат от националните законодателства на страните-членки.

Организационно-оперативната рамка на електронната идентификация дефинира дейностите, които се изпълняват от администраторите. Центърът за електронна идентификация изпълнява проверка за валидност на представената идентификация. Идентификационната карта е устройството, необходимо за електронна идентификация и притежава най-високото ниво на сигурност. Субекти в националната схема са: орган за идентификация в лицето на МВР, помощни органи и център за идентификация. Администраторите на е-идентификация, подпомагат дейността на органа по издаване на е-идентичност. Центъра за е-идентификация изпълнява проверката за валидност на представените е-идентичност и идентификация[[75]](#footnote-75).

**Публични и частни средства за електронна идентификация**

Електронната идентификация (eID) е система, която предлага валидиран достъп до електронни услуги. Възможно е да се използват публични или частни средства за идентификация и те може да функционират както в системата за електронна идентификация, така и извън нея.

Правителството в лицето на отговорен министър упражнява контрол върху издаване, прилагане и поддържане на публичните средства за електронна идентификация. Частният сектор контролира издаване, внедряване и поддържане на частните средства за електронна идентификация. Когато частните средства се използват за достъп до обществени услуги, политическа отговорност е същата, както при публичните средства. Но когато частните средства предоставят достъп само до частни услуги, има разлика.

|  |
| --- |
| Онлайн частни услуги  Онлайн публични услуги  Публична система за eID  Частна система за eID  Публичен регистър или PIN |

**Фиг. 1. Средства за електронна идентификация**

При издаване на карта за електронна идентификация чипът върху картата се запълва с информация. Независимо дали ще се използват публични или частни средства за идентификация, в процеса на издаване на картата има намеса частният бизнес. В страни, които използват частни средства за идентификация, администрацията споделя разходите по издаване на картата. Например във Великобритания, Швеция и Дания, които използват частни модели, са създадени собствени структури за финансиране. Великобритания и Дания организират общи търгове, а в Швеция моделът представлява „плащане при използване“. Разходите за карта за електронна идентификация се поемат от гражданите, с изключение на тези от Естония.

Електронната идентификация е технологично неутрална - може да се ползва чрез различни устройства - телефон, четец с лична карта, флашка с по-малка карта.

**Видове електронна идентификация**

Електронната идентификация може да се реализира с разнообразни средства.

* Потребителско име и парола е най-често използваната идентификация. Тя е лесна за прилагане, но е с най-ниско ниво на сигурност.
* Потребителско име и парола с верификация на текст е популярно средство за идентификация и се използва в много търговски сайтове. Счита се за притежаваща по-голяма степен на сигурност.
* Софтуерно базирани сертификати (на основата на инфраструктура на публичните ключове – PKI) представлява идентификация с помощта на електронен подпис. Прилага се в България от 2004 г. Идентификацията е посредством информация, записана върху носител – смарт карта. Смарт картата изисква карточетец или е безконтактна, което позволява четенето да става от разстояние. Сертификатът е записан в чипа върху смарт картата.
* Мобилна електронна идентификация – за идентификация се използва мобилен телефон или комбинация от мобилен телефон и безконтактна смарт карта за по-висока степен на сигурност.

**Електронна идентификация в Европа**

Единният цифров пазар е сред основните приоритети на Европейската комисия. За да бъде той успешен, са от съществено значение електронната идентификация и гарантирането на сигурност на личните данни. Гражданите и бизнесът трябва да са убедени, че техните данни се обработват при спазване на съществуващото законодателство за защита на данните. Сигурността при електронната идентификация е важен фактор, за да се предоставят услуги, да се гарантира защита на данните и да се предотвратяват онлайн измамите.

Чрез електронна идентификация сигурните трансгранични електронни транзакции стават възможни. Необходимо е да се създаде стратегия, чрез която да има възможност националните електронни идентификатори да могат да се използват за електронна самоличност във всяка европейска страна. За момента не съществува оперативна съвместимост и не е създадена обща правна база, чрез която всяка държава-членка може да се задължи да признава и приема електронни идентификации, издадени в други държави-членки. Липсата на трансгранична оперативна съвместимост на националните идентификатори пречи на гражданите и бизнеса да използват без ограничения единния цифров пазар.

**Електронна идентификация в Австрия като пример за успешен модел**

Стартира след въвеждането на успешна стратегия за е-правителство и тя е използвана при внедряването на електронна идентификация. Австрийският модел прилага стратегията за използване на различни среди, като например карти, издадени както от обществения сектор, така и от частния, които да са възможни носители на електронната идентификация. От 2009 г. се прилага мобилна идентификация, която притежава по-голяма ползваемост и удобство. Моделът се контролира от правителството. Решението на австрийското правителство да разработи тази стратегия се базира на решението гражданите да използват средствата, които вече притежават в себе си. Дейността по издаване на идентичност се определя като задача на правителството. Възможно е впоследствие да се появят на пазара за издаване на идентичност и други участници, ако те отговарят на изискванията, поставени от правителството. Поради тази причина австрийският модел се счита за отворен и технологично неутрален.

**Електронна идентификация в България**

В момента се разработва система за управление на електронната идентификация и регистър за електронна идентичност. Дейностите са по проект "Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство", осъществяван от Министерство на транспорта, информационните технологии и съобщенията, с финансовата подкрепа на Оперативна програма "Административен капацитет", съфинансирана от Европейския съюз чрез Европейския социален фонд.

Проектът предвижда в картата за електронна идентификация на българските граждани да се съдържат име на притежателя на картата, защитен код на персоналното ЕГН и парола. Стремежът е картата да не съдържа личи данни. Карта може да притежават български граждани над 14 г. и дългосрочно пребиваващи в страната чужденци. Чрез тази карта гражданите ще имат достъп и удобно ще ползват електронните административни (е-здравеопазване, е-образование, е-правосъдие и др.).

Предложенията за промени в Закона за българските лични документи предвиждат българските лични карти да притежават чип и възможност за електронна идентификация от 2018 г. Не се предлага задължителна смяна на личните карти на българските граждани. Промяната трябва да стане поетапно след изтичане срока на личните карти. Предлага се в чипа върху личната карта да се записват биометрични данни на лицето съгласно препоръките на Международната организация по гражданско въздухоплаване, но само ако притежателят изрично заявяви това. Ползването на новите лични карти като квалифициран електронен подпис също трябва изрично да се заяви. Законопроектът регламентира използването на електронна идентификация в международния паспорт. Законопроектът разширява възможностите за подаване на заявления за издаване на документи по електронен път, като добавя използването на електронната идентификация като алтернатива на квалифицирания електронен подпис[[76]](#footnote-76).

**Сигурност на електронната идентификация**

Сигурността при използване на електронна идентификация на гражданите се определя със следните характеристики:

* Данните в картата дали са защитени от непозволен (неоторизиран) достъп.
* Идентификацията трябва да се осъществява само с притежаване на карта и вярно въведен ПИН код (на принципа „нещо имам – нещо знам“).
* Връзката между компютъра на притежателя на електронна идентификация и услугата трябва да е защитена.
* Само специализирани органи по проверка (валидация) на електронната идентификация да имат права да проверяват и предоставят идентификационните услуги.
* Услугата по идентификация да може да получава само тези данни, които има право да получи (например само дата на раждане).

Данните, които се съдържат в картата за електронна идентификация се наричат „персонален идентификационен запис“ и се състоят от следните елементи: ЕГН/ЛНЧ; криптографски преобразуван електронен идентификатор; трите имена (на кирилица и латиница) на гражданина; рождена дата; ключ за връзка между картата и данните.

Регистрите, които са свързани с електронната идентификация в България, са следните[[77]](#footnote-77).

* Регистър на електронната идентичност – вече е наличен.
* Регистър на услугите, изискващи електронна идентификация – ще се изгражда след въвеждане на нормативната уредба.
* Регистър на овластяванията – ще се изгражда в рамките на портала на електронно управление.

Електронната идентификация, която ще се използва от бизнеса в България, ще използва сегментирането на бизнеса на сектори. Неговата цел е да се преустанови пренасянето на лични данни, като например ЕГН, с цел по-висока сигурност. Пример е електронното гласуване, където ще трябва да се гласува със секторен идентификатор. Всеки сектор ще притежава различен секторен идентификатор. Секторите осигуряват защитата на критична лична информация – например HIV статус, електронно гласуване и др. Няма да е възможно да се получава информация между секторите. Настоящите проблеми са заложени в данните за идентификация на гражданите от разстояние и по-конкретно въвеждането и използването на тяхното ЕГН. Практиката може да бъде променена чрез въвеждането на уникален електронен идентификатор, непроменим във времето - секторен е-идентификатор.

„Нивото на овластяване” е от голямо значение за сигурността в схемата на електронната идентификация, когато дадено лице участва от името на друго лице чрез делегиране на права, което може да замести официално пълномощно.

Практически аспект на сигурността при електронна идентификация е гарантиране на сигурност при електронното гласуване. При него се получава гаранция за сигурността при преброяване на гласовете, защото избирателят получава електронна разписка, че е гласувал, като в нея не е показано как е гласувал[[78]](#footnote-78).

**Бъдещи предизвикателства**

Няколко са предизвикателствата пред въвеждане на електронната идентификация в България.

1. Въвеждане на електронна идентификация в личните документи. Обсъжда се въпросът дали в личните карти да се вгради електронен идентификатор.
2. Дискутира се въпросът как ще бъдат идентифицирани юридическите лица (разчита се движещ механизъм да бъде бизнесът и затова този въпрос е важен). Обмисля се създаването на секторен идентификатор, например финансов, транспортен и др. Ползата от създаването му ще е прекратяване на преноса на лични данни (ЕГН) от доставчик на доставчик. Личните данни (ЕГН) ще бъдат трансформирани до псевдоним, за да бъде защитата успешна.
3. Мобилна електронна идентификация. Тази идентификация ползва мобилния номер (или устройство). Уникалният, заложен в апаратите номер IMEI / International Mobile Station Equipment Identity) , уникалният SIM (Subscriber Identity Module) в комбинация с личен „ключ“, биопараметър (пръстов отпечатък, сканирана ретина, рисунък на вените на ръката или нещо подобно) биха могли да внесат генерална промяна във възможностите на технологиите, използващи и нуждаещи се от електронна идентификация. Вероятно нуждата от няколко банкови карти, с които много граждани разполагат, здравни карти, лична карта, шофьорка книжка постепенно ще бъде наследена и комбинирана в едно „смарт“ устройство.
4. Трансгранична оперативна съвместимост. Развитието на електронната идентификация ще е в посока възможност за ползване на електронни услуги в Европейския съюз.

**Използвана литература:**

1. International Comparison eID Means, Final report, 10 April 2015.
2. Б. Божанов. Електронната идентификация е средство, чрез което изобщо да има електронно гласуване. <http://bnr.bg/post/100672462/b-bojanov-elektronnata-identifikacia-e-sredstvo-chrez-koeto-mojem-izobshto-da-imame-nakakvo-elektronno-glasuvane>, 22.3.2016.
3. Дигиталните иновации – приоритет №1 в ИТ инвестициите на държавната администрация. http://cio.bg/7717\_digitalnite\_inovacii\_\_prioritet\_1\_v\_it\_investiciite\_na\_\_darzhavnata\_administraciya, 26.1.2016.
4. Електронна идентичност, Пилотен проект. http://eid.egov.bg/, Посетен на 20.4.2016.
5. М. Иванова. Личните карти ще са с чип и електронен подпис от 2018 г. <http://www.investor.bg/ikonomika-i-politika/332/a/lichnite-karti-shte-sa-s-chip-i-elektronen-podpis-ot-2018-g-214360/> , 11.4.2016.
6. Пилотен проект за българска електронна идентичност, <http://eid.egov.bg/>
7. С. Хаджистойчев. Национална схема за електронна идентификация, 2016. <http://www.astel-bg.com/Docs/Conf_04_2015/iii-2.pdf>

**Система за управление на сигурността на летище - перспективи на ЕС**

*докторант Албена Попова*

*Нов български университет*

***Резюме:*** *Докладът разглежда необходимостта от въвеждане на ефективно функционираща система за управление на сигурността, която предоставя на летището структуриран подход за управление на авиационната сигурност и инструмент за идентифициране и управление на риска по един непрекъснат и проактивен начин.*

*Доказва се, че системата за управление на сигурността се базира на вече въведени стандарти за сигурност и успешно взаимодейства с други системи за управление.*

***Ключови думи:*** *авиационна сигурност, летище, ефективност, система, управление.*

През последните десетилетия авиацията е атрактивна цел за терористите и заплахата за гражданската авиация е реална и динамична. Струпването на много хора на едно място и експлоатацията на сложно и скъпоструващо оборудване, необходимо за изпълнение на ежедневните авиационни дейности, превръщат гражданската авиация в удобна цел за терористична дейност. Дори една атака да не бъде реализирана в пълния си обем, последствията от нея водят до съществени финансови, материални, морални и политически вреди. Създава се климат на страх сред пътници, персонал и общественост, което оказва негативен ефект върху дейността на авиокомпании, летища и авиационната индустрия като цяло.

Този проблем възниква в края на 60-те години и незабавно поражда необходимост от разработване на законова рамка за противодействие на заплахата. Международната организация за гражданска авиация ICAO (International Civil Aviation Organization) започва да играе водеща роля в разработването на политиките в областта на авиационната сигурност. Повишаването на сигурността на въздухоплаването в глобален аспект става една от стратегическите цели на Организацията.

Събитията от 11 септември 2001 играят решаваща роля в динамиката на процесите по разработване и прилагане на мерки в областта на авиационната сигурност. Анализите след терористичните атаки в Ню Йорк показват, че целта на терористичните организации вече не е само нанасяне на материални щети, но и причиняване на човешки жертви. Тези събития поставят началото на един непрекъснат процес на преразглеждане на мерките за сигурност на международно, европейско и национално ниво в съответствие с нивото на заплаха и оценка на риска. Задачата на разработването и прилагането на хармонизирани мерки, адекватни на степента на заплаха, е да се осигури защитата и безопасността на пътници, екипажи, персонал, общественост, въздухоплавателни средства и оборудване на летищата, обслужващи гражданската авиация от актове на незаконна намеса[[79]](#footnote-79).

Важна стъпка в тази насока е изграждането и поддържането на надеждна система за сигурност, която се състои от превантивни мерки, човешки и материални ресурси[[80]](#footnote-80). Ефективното функциониране на тази система се гарантира от три елемента: (1) установена законодателна рамка, формирана на международно, европейско и национално ниво, (2) прилагане на мерки за сигурност, покриващи изискванията на стандартите за сигурност и отговарящи на степента на заплаха и (3) приети по силата на международни договори правни норми за преследване или екстрадиране на лица, извършили актове на незаконна намеса.

Международната организация за гражданска авиация (ICAO) в своите документи по сигурността, дефинира актовете на незаконна намеса като „действия или опит за действия, целящи да застрашат безопасността на гражданското въздухоплаване и въздушния транспорт”[[81]](#footnote-81). Такива действия са:

* незаконно завземане на въздухоплавателно средство (ВС);
* разрушаване на ВС в експлоатация;
* вземане на заложници на борда на ВС или на летище;
* насилствено качване на борда на ВС, навлизане в летище или в периметъра на аеронавигационно съоръжение;
* внасяне на борда на ВС или на летище на оръжие, опасно устройство или материали, предназначени за криминални цели;
* използване на ВС в експлоатация за причиняване на смърт, нараняване или сериозно увреждане на имущество или околна среда;
* съобщаване на невярна информация, което излага на риск безопасността на ВС в полет или на земята, както и на пътници, екипаж, наземен персонал или общественост на летище или в периметъра на съоръжение на гражданската авиация.

Всяка година Съвета на ICAO представя пред международната авиационна индустрия официален доклад, който съдържа задълбочен преглед на програмите, дейностите и постиженията на Организацията. В този доклад се представя информация за видовете и броя актове на незаконна намеса през годината. Данните се получават от съответните държави, в изпълнение на изискването за докладване, съгласно Стандарт 5.3 от Анекс 17 към Чикагската конвенция.

В таблица 1 са представени данни, обхващащи периода от 2000 г. до 2014 г[[82]](#footnote-82).

**Таблица 1. Актове на незаконна намеса (АНН) в дейността на гражданското въздухоплаване**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Актове на незаконно завземане (отвличане) | | Актове на нападения срещу оборудване | |  | | Ранени и убити по време на АНН | |
| Год. | Общо  АНН | Отвличания | Опит за отвличания | Атаки срещу оборудване | Опит за атаки срещу оборудване | Саботаж | Други1 | Ранени | Убити |
| 2000 | 30 | 12 | 8 | 1 | 0 | 0 | 9 | 50 | 58 |
| 20012 | 24 | 7 | 2 | 7 | 4 | 1 | 3 | 3 217 | 3 525 |
| 2002 | 40 | 2 | 8 | 24 | 2 | 2 | 2 | 14 | 186 |
| 2003 | 35 | 3 | 5 | 10 | 0 | 5 | 12 | 77 | 20 |
| 2004 | 16 | 1 | 4 | 2 | 2 | 4 | 3 | 8 | 91 |
| 2005 | 6 | 2 | 0 | 2 | 0 | 0 | 2 | 60 | 3 |
| 2006 | 17 | 1 | 3 | 4 | 0 | 1 | 83 | 27 | 2 |
| 2007 | 22 | 4 | 2 | 2 | 3 | 0 | 11 | 33 | 18 |
| 2008 | 23 | 1 | 6 | 3 | 0 | 0 | 133 | 31 | 11 |
| 2009 | 23 | 5 | 3 | 1 | 0 | 0 | 143 | 4 | 3 |
| 2010 | 14 | 0 | 1 | 1 | 0 | 1 | 113 | 13 | 6 |
| 2011 | 6 | 0 | 2 | 0 | 0 | 1 | 33 | 152 | 35 |
| 2012 | 10 | 1 | 2 | 2 | 0 | 0 | 53 | 44 | 20 |
|  | | Актове на незаконно завземане (отвличане) | | Актове на нападения срещу оборудване | |  | | Ранени и убити по време на АНН | |
| Год. | Общо  АНН | Отвличания | Опит за отвличания | Атаки срещу оборудване | Опит за атаки срещу оборудване | Саботаж | Други1 | Ранени | Убити |
| 2013 | 8 | 1 | 0 | 3 | 0 | 1 | 23 | 1 | 7 |
| 20144 | 20 | 2 | 2 | 9 | 0 | 1 | 63 | 36 | 44 |

**Легенда:**

1. Включва атаки по време на полет и други АНН
2. Официалните доклади за събитията от 11 септември 2001 в САЩ не включват ранени и загинали на земята. Прогнозният брой е от медийни източници.
3. Включва опити за саботаж.
4. Не включва информацията за полет MH17 на Malaysia Airlines. По това време официалното разследване не е приключило

Видовете заплахи за гражданската авиация и възможността за поява на нови, изискват адекватно противодействие от системата за авиационна сигурност. Това изправя индустрията пред предизвикателството да се търсят нови и по-ефективни начини за постигане на постоянно ниво на съответствие при изпълнение на мерките за сигурност, с цел намаляване на риска от извършване на актове на незаконна намеса.

В последните години усилията на международните организации в областта на гражданската авиация са насочени в посока разработване и внедряване в дейността на авиационната индустрия на интегрирана система за управление на сигурността, съответстваща на нивото на заплаха и оценка на риска. Тази система предоставя на съответната организация структуриран подход за управление на авиационната сигурност и инструмент за идентифициране и управление на риска по един непрекъснат и проактивен начин[[83]](#footnote-83).

За първи път необходимостта от прилагане на интегрирана система за управление на сигурността SeMS (Security Management System) е предмет на дискусия на среща на работната група по сигурността на ICAO през 2006 г[[84]](#footnote-84). От тогава тази концепция става нейна стратегическа задача. От 2007 г. Международната асоциация за въздушен транспорт IATA (International Air Transport Association) въвежда системата за управление на сигурността (SeMS) като задължителна за всички авиокомпании, членки на IATA.

IATA счита, че чрез прилагане на концепцията на системата за управление на сигурността, компаниите получават единна система за управление, която интегрира всички свързани със сигурността дейности на организацията. Чрез системата за управление се осигурява рамка, с помощта на която организациите не само осъзнават, но и адекватно изпълняват своите отговорности[[85]](#footnote-85).

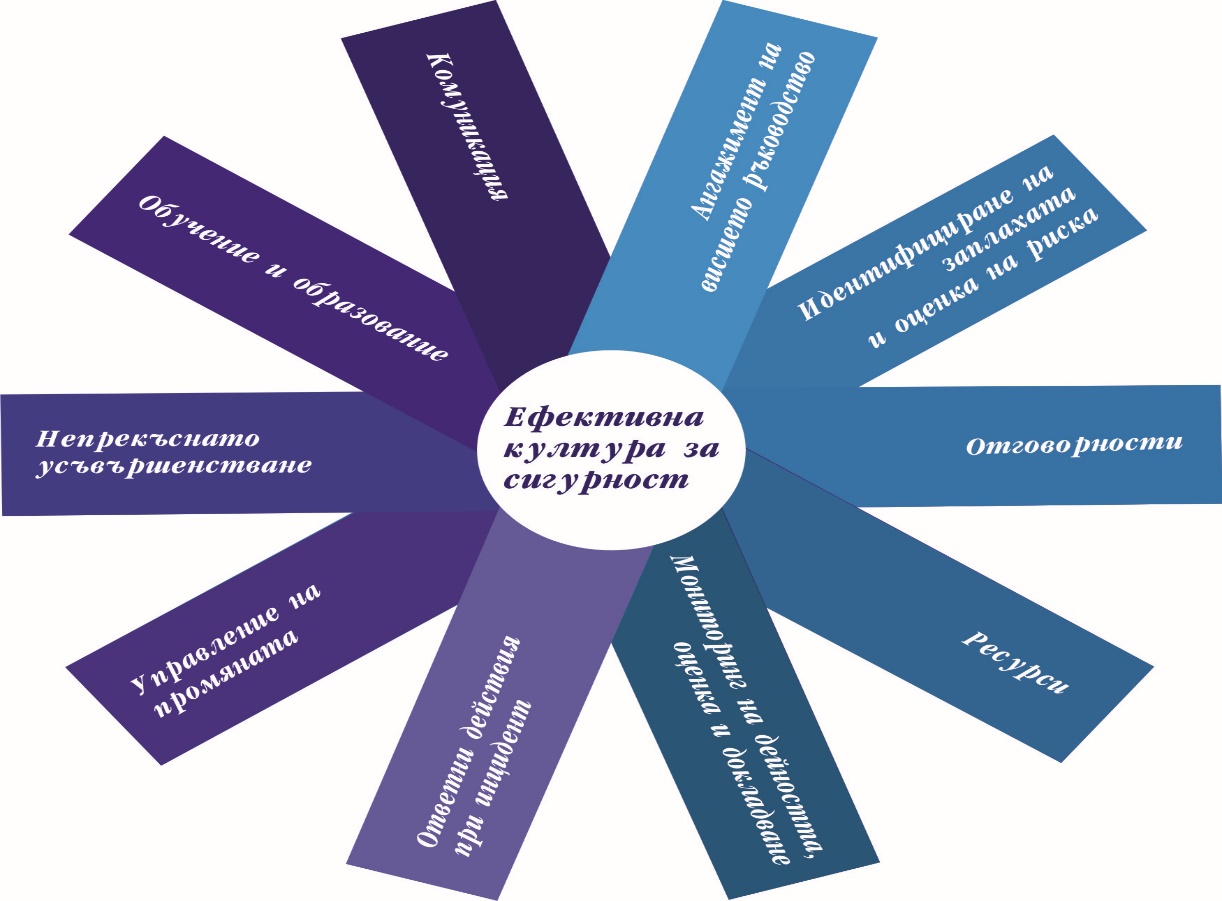
На този етап, въвеждането на „Система за управление на сигурността” (SeMS) за летищата няма задължителен характер. Трябва да се вземе предвид обаче, че основните мерки за авиационна сигурност във всички девет аспекта на обезпечаване на сигурността на полетите се изпълняват на територията на летище. Това поражда необходимостта от създаване и въвеждане на ефективно функционираща система за управление на сигурността, като по този начин се гарантира изпълнение на мерки за сигурност съответстващи на международните и европейски изисквания.

Методологията и техниките на традиционната система за контрол, прилагана на голяма част от летищата в света и Европа към момента, дава информация само за моментното състояние на нивото на съответствие на изпълнение на мерките и процедурите за сигурност. Визия за цялостния процес по обезпечаване на сигурността се получава чрез създаване и въвеждане на един организиран, системен и ефективен подход за управление на сигурността, който определя структурата, отговорностите, политиките и процедурите, необходими за постигане на постоянно ниво на изпълнение на мерките за авиационна сигурност.

Предмет на настоящата разработка е извършване на сравнителен анализ между стандартите за авиационна сигурност в международните, европейските и националните нормативни документи и съответствието им с елементите на системата за управление на сигурността SeMS.

Целта е да се докаже, че SeMS е допълваща, всеобхватна мрежа от елементи и изисквания за вече въведени стандарти за сигурност.

За нуждите на сравнителния анализ са разгледани десетте елемента на SeMS, представени на фигура 1, така както са разработени и изобразени от Департамента по транспорт на Великобритания DfT (Department for Transport)[[86]](#footnote-86)



**Фигура 1. Елементи на система за управление на сигурността (SeMS)**

Елементите са разработени така, че да бъдат приложими към всички типове и размери авиационни субекти[[87]](#footnote-87). По този начин се дава възможност на всеки оператор да прилага системата по начин, по който ще работи най-добре за него, съобразно неговата специфика, като например размер, брой и характер на операциите.

В таблица 2 са представени елементите на системата за управление на сигурността[[88]](#footnote-88), съдържащи се в Анекс 17, европейските и националните документи по авиационна сигурност.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Таблица 2. Елементи на системата за управление на сигурността, съдържащи се в Анекс 17, европейските и националните документи по авиационна сигурност** | | | | | | |
| **№** | **Елементи на SeMS** | **Съставни елементи** | **Анекс 17**  **(SARPs)1** | **Рег. 300/2008** | **Национални**  **документи** | **Липсващи съставни елементи** | |
| 1 | Ангажимент на висшето ръководство | Политика за сигурност  Ангажимент към сигурността.  Предоставяне на ресурси.  Процедури за докладване.  Указва поведение, което е неприемливо.  Довежда се до знанието на цялата организация.  Преразглежда се периодично.  Подписва се от отговорния ръководител. | - | - | **-** | **Разработена и внедрена политика за сигурност, подписана от Отговорния ръководител.**  **Декларация за поемане на ангажименти.** | |
| 2 | Отговорности | Отговорен ръководител  Ръководител по сигурността | 3.2.2 | Чл. 12, ал. 1  Рег. 2015/1998 | ЗГВ2, чл. 16м  НПСГВ3 Гл. 01 |  | |
| 3 | Идентифициране на заплахата и оценка на риска | Оценка на заплахата | 3.1.3 | Ал. (9) | НПСГВ  Глава 01 |  | |
| Оценка на риска | 3.1.3 | Чл. 6, ал. 1 |
| 4 | Ресурси: персонал и оборудване | Програма за обучение  Подбор и оценка на персонала  Обучение на персонала  Сертифициране на персонала  Информираност по сигурност | 3.1.6  3.4.1  3.4.2  3.4.3  3.1.10 | Приложение  т. 11.1 | НПСГВ  Глава 11  НПОССГВ4 |  | |
| Оборудване, съгласно изискванията | 2.5.3 | Приложение  т. 12 | НПСГВ |
| 5 | Мониторинг на дейността, оценка и докладване | Мониторинг за съответствие | 3.4.4  3.4.5 | Чл. 12, ал. 2  Чл. 15  Рег. 18/2010 | ЗГВ, чл. 16г  НПКК5 |  | |
| Одити, инспекции, обследване, разследване. | 3.4.6 | Рег. 18/2010 | НПКК |  | |
| Мониторинг в съответствие с КПЕ. | - | - | - | **Разработване на ключови показатели за ефективност (КПЕ)** | |
| Предприемане на коригиращи действия. | 3.4.6 | Рег. 18/2010  НПКК | Рег. 18/2010  НПКК |  | |
| Мониторинг на доставчиците на услуги. | 3.4.9 | Рег. 18/2010  НПКК | Рег. 18/2010  НПКК |  | |
| **№** | **Елементи на SeMS** | **Съставни елементи** | **Анекс 17**  **(SARPs)** | **Рег. 300/2008** | **Национални**  **документи** | **Липсващи съставни елементи** | |
| 6 | Ответни действия при извънредни ситуации и инцидент | План за действия при извънредни ситуации  Готовност и ответни действия  Ръководство на ответни действия | 5.1.4  5.2.1  5.3.2 | - | ЗГВ, чл. 16г  Национален план6 |  | |
| 7 | Управление на промяната | Процес за идентифициране на външна и вътрешна промяна, която може да рефлектира върху нивото на риск за сигурността.  Материална база; персонал; процедури; оборудване; технологии; информационни системи | 4.9  критични  инф. системи | - | НПСГВ  критични  инф. системи | **Управление-процес-структуриран подход.**  **Управление на риска във връзка с промяната.** | |
| 8 | Непрекъснато усъвършенстване | Проактивна и реактивна оценка на ефективността и ефикасността на дейността по сигурността. | 3.4.8 | Рег. 18/2010 | НПКК | **Разработване на ключови показатели за ефективност (КПЕ)** | |
| 9 | Обучение и образование | Програма за обучение на целия персонал, вкл. всички нива на ръководството | 3.1.10 | Приложение  т. 11.2 | НПСГВ  т. 11.2.6 | Информиране за **отговорности** и нива на **отчетност** в организацията  **Политика за сигурност** | |
| 10 | Комуникация | Целите и процедурите на SeMS се довеждат до знанието на всички ангажирани лица и организации |  |  |  |  | |
| Съобщава се критична за сигурността информация.  Обясняват се определени действия, които се предприемат.  Излагат се причините за нововъведени или променени процедури. | 3.1.4  3.1.5  3.2.3  5.3 | Чл. 6, ал. 2  Чл. 8  Чл. 18 | ЗГВ  НПСГВ |  | |

1 Стандарти и препоръчителни практики (Standards and Recommended Practices SARPs)

2 ЗГВ - Закон за гражданското въздухоплаване

3 НПСГВ - Национална програма за сигурност в гражданското въздухоплаване

4 НПОССГВ - Национална програма за обучение и сертифициране по сигурност в гражданското въздухоплаване

5 НПКК - Национална програма за контрол на качеството по сигурността в гражданското въздухоплаване

6 Национален план за действия при актове на незаконна намеса в дейността на гражданското въздухоплаване

От сравнителния анализ в таблица 2, може да се направи извод, че повечето от компонентите на SeMS вече съществуват. Разгледани поотделно, те са насочени към изпълнение само на една задача. Смисълът на прилагането на такава система за управление е, че тя има потенциала да координира всички тези задачи „под един покрив”[[89]](#footnote-89). Насоченото им действие и функционирането им като единна система изграждат в организацията култура за сигурност. Развиването и насърчаването на позитивна култура за сигурност е от съществено значение за поддържане на сигурна среда, в която всички оперативни дейности на летището се изпълняват ефективно и без прекъсване.

През 2011 г. Европейският съюз публикува доклад “Flightpath 2050”, разработен от работна група под ръководството на Европейската комисия. Документът представя европейската визия за развитие на въздушния транспорт до 2050 г. Една от поставените цели е през 2050 г. системата за авиационна сигурност на летището да функционира по такъв начин, че прецизната оценка на заплахата и риска да гарантират един непрекъснат, безпроблемен и ефикасен въздушен транспорт[[90]](#footnote-90).

Това може да бъде постигнато чрез ефективно функционираща система за управление на сигурността, която предоставя на летището структуриран подход за управление на авиационната сигурност и инструмент за идентифициране и управление на риска по един проактивен начин.

Анализ на дейността на летищата, обслужващи гражданската авиация в България, показва, че системата за сигурност все още не функционира чрез прилагане на принципите на SeMS в пълен обем. Няма установена концепция за прилагане на проактивен подход за управление на риска. За създаването на ефективна система за управление на сигурността е необходимо да се проведат научни изследвания със задълбочен анализ на моментното състояние и моделиране на система чрез използване на математически методи.

**Използвана литература:**

1. European Commission, Researh and Innovation, Europe's Vision for Aviation Flightpath 2050, Published on: 31/03/2011, стр. 17. [online] <http://ec.europa.eu/research/transport/publications>
2. ICAO, Security Manual (Doc 8973) 7th edition, Volume I, стр. I-6. [online]. <https://www.scribd.com/doc/109423612/VOL-I-National-Organization-and-Administration>
3. ICAO, Annex 17 9th edition, 2011, стр. 1-1. [online]. <https://www.bazl.admin.ch>
4. ICAO, Annual Report 2014, Appendix 1, Table 11 [online]. <http://www.icao.int/annual-report-2014>
5. ICAO, Results of the meeting on Aviation Security Management System (SeMS), AVSEC/FAL/RG/5- WP/08, 28/05/15. [online]. [www.icao.int](http://www.icao.int)
6. ICAO, Laying the Foundations for a more risk-based ICAO Annex 17-Security: Security Management System (Presented by IATA), DGCA-MID/1-IP/9, March 2011. [online]. www.icao.int
7. IATA, Security Management System (SEMS) for Air Transport Operators, 2011. [online]. [www.iata.org](http://www.iata.org)
8. Department for Transport, Framework for an Aviation Security Management System (SEMS), 2014. [online]. [www.gov.uk](http://www.gov.uk)

**Съвременният тероризъм - негативен фактор в европейската среда за сигурност**

*доц. д-р Йордан Бакалов*

*Нов български университет*

***Резюме:*** *Събитията в последните години показаха, че една от най-големите заплахи и предизвикателство за човечеството е тероризма, а войната срещу тероризма е нов вид война. Война, която се води от нов вид участници с различни методи и средства за воюване. Война, в която е въвлечено и реално участва цивилното население. Насилието, заплахата от насилие и способността за извършване на насилие е равно на тероризъм.*

***Ключови думи:*** *среда на сигурност, национална сигурност, насилие, тероризъм.*

Средата на сигурност във второто десетилетие на ХХІ век е значително променена в сравнение с предходните десетилетия. Това се отнася както за средата на сигурност на света и на региона така и за средата на вътрешна сигурност на Република България.

Специфичен момент, който е в пряка връзка със сигурността на страната ни е, че нейното относително тегло в международните отношения е сравнително малко, но веднага следва да се отбележи, че процесите и тенденциите в съвременния свят ни засягат не по-малко от другите участници в него, а в някои отношения нашите проблеми са дори по-сложни за разрешаване от тези в други страни. Например след атаките в Париж и Брюксел Европейският съюз е изправен пред сложни и трудно преодолими препятствия за създаване на единна мрежова сигурност. Когато става въпрос за борба с международната престъпност и тероризма, отделните страни-членки на организацията имат различни приоритети, ресурси и нива на компетентност. Големите държави като Франция, Обединеното кралство и Германия имат значителен опит в борбата с тероризма и достатъчно човешки и материални ресурси, за да поддържат добре работещи разузнавателни и антитерористични агенции. Това не е вярно за по-малките страни, с по-малко опит и по-малки бюджети, и още по-малко по време на икономически кризи, когато правителствата на малките държави трябва да балансират между необходимостта за финансиране на системите си за сигурност с постоянните дефицити.

Позитивните фактори на средата за сигурност имат важна роля в нашата политика за сигурност. Тяхното отчитане е задължително при изготвянето на политиката. Сред позитивните фактори са стабилността на европейския регион, принадлежността на страната ни към семейството на демократичните държави, наличието на световни мрежи в икономиката, в информацията и разбира се в различни сфери на сигурността, необратимостта на демократичните процеси у нас.

Средата на сигурност обаче е особено важна за политиката за сигурност със своите вредни въздействия. Те са тези, които следва да се отчитат, да се анализират, те са тези, на които следва да се подготвят адекватни отговори и в крайна сметка да се контролират. Трудно е тези въздействия да се подреждат по степен на значимост, поради което в статията се следва честотата на тяхното споменаване в публичното пространство, което не означава непременно степен на интензивност.

Негативен фактор в световната среда за сигурност е съвременният тероризъм. Събитията в последните години показаха, че една от най-големите заплахи и предизвикателство за човечеството е тероризма, а войната срещу тероризма е нов вид война. Война, която се води от нов вид участници с различни методи и средства за воюване. Война, в която е въвлечено и реално участва цивилното население.

Според много анализатори, особено след терористичните актове в Европа, тероризмът и ислямския фундаментализъм заемат едно от първите места на заплахите за всяка държава,както и на глобалната сигурност. Прояви на терор се наблюдават от много години, на нашето съществуване. Разглеждането на цивилното население като военна мишена, за да се тероризират цели нации,е един от най-старите методи за водене и печелене на воини.

,,Върхът,, на действията на терористичните групи се постига през седемдесетте години на миналия век, както в Палестина - многообразие от терористични организации, Германия - ,,Баадер-Майнхоф“, Италия – най-действената ,,Червените бригади,, и т.н.

В края на двадесети век и началото на двадесет и първи век, благодарение на глобализацията на световната информационна мрежа и напредъка на нашата цивилизация, като че ли точно от глобализацията и развитието на обществото, най-много се възползват терористичните мрежи, защото извършването на терористичния акт, може да от текне във всяка точка на Земята и да постигне своя психологически ефект. Изпитвайки страх,голяма част от хората не взимат адекватни решения,допускат грешки и се ръководят от грешни принципи.

За това е необходимо обществото да подобри ,своите способности да се съпротивлява на тероризма.Разбираемо е противодействието на м.н.тероризъм да не е лесно,така както не е лесно противодействието на криминалната престъпност.

Религиозния тероризъм,може да се окаже по-труден за противодействие,защото се ползва със симпатиите на по - широки слоеве от младото население. Ислямът е много по авторитарна и йерархична религия в сравнение с другите религии,защото се противопоставя на прокарването на демократични идеи за правата на отделната личност.

Според професор Карш от Кралския колеж в Лондон: ,,Участието в усилията за изкореняване на другите религии,може да се смята за интегрална част от опитите на мюсюлманите за постигане на личностна себе изява. В ислямските общества не съществува стремеж към демокрация, присъщ на западните народи, така че всеки опит за налагане на подобна система рискува да се сблъска с недоволството на масите и да се разглежда от местното население като вид неоимпериализъм или налагане на съвременните модни течения“.

Разликите между християнските и мюсюлманските религии се свежда до това,че обществата които ги изповядват са на различен етап от своето развитие. За голямо съжаление управляващите на мюсюлманските държави в повечето случаи водят изолационистична политика,което води до трудното възприемане на ,,цивилизационните закони,, от техните общества.

Влиянието на екстремистите организации и терористични групи за съществуването на т.н. ,,терористи самоубийци,, е водещо. Особено въздействащо е това влияние сред хора, които имат ограничени, фанатични и непълни представи за съществуващите религии и крайни философски концепции,които имат ярко изразено негативно отношение към политическите модели,към отделни държави или групи страни.

Идеологията на екстремистките организации е една сложна смесица от обещания за по-хармонично съществуване, чрез премахване на посочения враг и спасение на душата след смъртта. Такава идеология много лесно намира почва сред хора,които се намират в състояние на криза,лесно се поддават на ексремиски внушения и по този начин се стремят да преодолеят душевната си болка. Обикновено такива хора възприемат ″другарите″ си, като по-добрата част на заобикалящото ги общество, имат обща идея,обща цел и могат да използват всякакви средства за постигането и. Участниците в терористични групи могат да се доверят единствено един на друг, тяхната обвързаност ги откъсва от обществото, те си взаимодействат в затворена общност. Изолацията и възприятието на враждебно обкръжение засилват споделените убеждения и правят вярата в каузата безапелационна. Особеното на тези групи са фиксацията към лидера, който за тях е духовен и религиозен авторитет. Примерът на подражание на духовния водач в исляма оказва значителен ефект върху психиката на последователите,както и на тези които са в началото на развитие на възгледите си относно исляма и терористичната дейност.

Неправилно е да се смята, че всички ислямски екстремисти си приличат по мотивите на поведение. Важно е да се разбере, че в началния етап на оформяне на личността и емоционалното състояние, в съчетание с насилието сами по себе си не са достатъчни за формиране на екстремистка личност до степен да извърши самоубийствен терористичен акт без мотивационния компонент. Интересното което може да се отбележи е, че лидерите на терористичните движения до Ал-Кайда набираха съмишленици от собствените си държави, а сега се набират единомишленици от цял свят.

Насилието, заплахата от насилие и способността за извършване на насилие е равно на тероризъм. Не е необходимо насилието да бъде извършено напълно т.е не означава, че имаме тероризъм само тогава, когато актът е извършен, за насилие говорим и когато е налице готовност за извършване на насилствен акт. Когато хората очакват в страх атентатът да бъде извършен. Типичен пример са атентатите които се извършиха на 13 ноември в Париж.

Извода който можем да направим от това е, че влиянието на терористичните актове не се свежда единствено до броя на жертвите а и до всяване на страх сред населението.

Всеобща констатация е, че съвременният свят е изправен пред заплахата от международен тероризъм. Той е дело преди всичко на екстремистки групи, които много често застават зад идеите на фундаменталисткия ислям. Основна причина за активизирането на фундаментализма се дължи на наличието на преобладаващо население в младежка възраст, в чието поведение са характерни активност, бунтарство и дори агресивност. Полученото образование е далеч под нивото на усилията, които се полагат за неговото масовизиране. Ключът за разпространението на тероризма е въздействащата идеология, подкрепата на местното население, слабите афганистанска, иракска и сирийска армии,силата на терора и подходящо финансиране и въоръжение са в основата на успеха на ислямска държава. Чрез обявяването на халифат, принуждават всички от ислямския свят,да ги подкрепят,в противен случай са заплашени да бъдат посочени като вероотстьпници. Халифата е ,,пирамидално,, изградена полицейска държава, подчинена на насилието и страха.Употребата на термина за радикализацията на мюсюлманското население е сравнително нова ,започна да се употребява масово след 11септември. Радикализацията дава възможност да погледнем на терористите като отделни индивиди които са недоволни от собствената си реализация,липсващата им интеграция в обществото или стремежа им,към лична значимост,като за всичко това са готови да предприемат насилствени действия. Някои от основните мотиви за радикализацията са:

1.Обработване чрез радикална идеология и трансцедентални ползи. Водещ мотив за радикализацията са ползите които ще се получат в отвъдния живот, заради богоугодните действия в този живот. Ако тези ползи като катализатор за радикализацията могат да бъдат оспорени,то влиянието на ислямиската идеология е несъмнено. Извършителите на терористични атаки,са били под влияние на радикални имами или са посещавали джамии,в които са се разпространявали радикални идеи.

2. Несправедливо отношение към мюсюлманската религия. Един от водещите мотиви е, ,,убеждението,,че мюсюлманската религия е несправедливо репресирана от демократичния свят.Това е свързано с разликите в поколенията емигранти и много по голямата радикализация на младото поколение,което е родено там.

3. Отдаденост на героизъм ,романтика и политическа кауза. Сред младото поколение мигранти се открива желание за постигане на обществен идеал ,героизъм и жажда за романтика.Част от привлекателността на И.Д. се дължи на,представянето на обществения идеал за изграждането на един нов свят.

4. Враждата към шиитите. Според изявления на лидери на И.Д.,най-големия враг са шиитите.Враждата между сунити и шиити доведе до жертви от едната и другата общност.

5. Икономика и благосъстояние. Неплащането на данъци и обещание за благосъстояние

6. Желание за реализация, психични проблеми. Във всеки военен конфликт има хора които търсят военна реализация.

Радикалния ислям играе роля на колективен отдушник и ясна алтернатива на индивидуалния избор. Мюсюлманинът приема подчинението спрямо управника като свое задължение. В противен случай той ще допусне грях, равен на престъпление. На практика ислямският фундаментализъм се оказа част от невидимия фронт, чиято демаркационна линия не съществува.

Провежданата от Европейския съюз политика за мултикултурализъм доведе до увеличаване на мюсюлманското население, което се оказа податливо на манипулацията провеждана от ислямистите. Терористите имат подкрепа от местните и това е разкрито в хода на следствените дейности в Сен Дени след терористичните нападения в Париж през ноември м.г. По принцип, всекидневният живот в Сен Дени и в други предградия е свързан с известен риск, което позволява на потенциалните терористи да се слеят с тълпата, да се укрият в среда, където царят мълчание, взаимна отговорност и всесилна религия.

Тези групи действат в мрежи и често са готови да извършват самоубийствени терористични актове, както и атентати с използване на химически, бактериологични и радиологични оръжия. Съществува заплаха от терористични атаки срещу важни елементи на националната критична инфраструктура, както и заплаха от електронни атаки. Улесняващо обстоятелство за съвременните терористи е високо развитата комуникационна среда в съвременния свят, която позволява достъп до нужната им информация и координиране на действията им по начин, непознат в миналото.

Трите основни елемента на терористичната дейност са политическа мотивация, насилие и организация на действията.Политическата мотивация е тази, която отличава тероризма от криминалната и организираната престъпност. Целите на тероризма винаги са политически, а на организираната престъпност са винаги икономически. Пресечната точка между тероризма и организираната престъпност може да бъдат финансовите средства, придобити по престъпен начин. Характерно за тероризма е и това, че те действат нелегално под добре организирано прикритие. Тероризма служи за политическа изява на терористите, независимо от мотивациите им; (идеологически, религиозни, етнически). Много често самите терористи създават собствените си каузи.Тероризма винаги си поставя като основна стратегическа цел именно властта ,да господства и подчинява,да сплашва и да контролира и като краен ефект да предизвиква политически промени.Затова насилието е условие без което терористите не могат да изградят нито стратегията си,нито тактиката си.

Когато говорим за съвременните форми на тероризма, не можем да не забележим, че терористичните атаки в Брюксел, са извършени по начин, подобен на терористичните атаки в Париж: нечовешки в своята форма, и чудовищни в своето съдържание. Те показват, че терористите на ислямска държава притежават не само собствен почерк, но и силата и желанието да проведат верига от подобни експлозии в Европа. Основните характеристики на съвременните терористични атаки се различат от по-рано извършените. Актове на тероризъм са извършени от млади хора основно араби, някои от тях родени в Европа, но с арабски корени, а не на атентатори самоубийци. Актовете на тероризъм са извършени срещу цивилното население на страните, които участват в борбата срещу ислямска държава.

Атаките не са отделни единични акции. Те са поредица от атаки и са извършени с основна цел сплашване на населението и създаване на обща атмосфера на очаквани нови експлозии. В Париж на 13 ноември 2015 година, това са серия от почти едновременни терористични атаки: експлозия в близост до стадион "Стад дьо Франс", показен разстрел на гостите в няколко ресторанта и вземане на заложници в концертна зала "Батаклан". Резултатът е очакван и е интерес на терористите, властите въведоха извънредно положение в страната, а хората в Париж чака в страх нови терористични атаки. Денят на атаките (петък) не е избран случайно, това е времето на максимално струпване на хора. Терористите са разделени в три групи, всяка от които има своя собствена цел. В резултат на терористични атаки загинаха 130 души, ранени са повече от 350 души. В Брюксел почеркът на терористите е сходен: терористичните актове са извършени на няколко места в столицата на Белгия - два на международно летище Завентем, едно в станцията на метрото Малбек. Една (четвърта) експлозия е обезвредена. Според първите оценки в резултат на атаките загиват 31 души, 250 са ранени. В новият почерк на терористите се откроява желанието им да се създаде и разпространява обща паника, да се създаде в хората усещане на очакване за нови бъдещи атаки. Ефектът е постигнат. Белгийският кризисен център препоръчва след бомбените атентати гражданите да не излизат от домовете си, персоналът на някои институции е посъветван да не напускат офиса е др.

Последните две години агентурата мрежа на Ислямска държава работи много по-професионално. Макар, че продължават да се използват терористи самоубийци, организаторите участващи в атаката съхраняват своя живот с цел организиране на нови атаки.

Страната ни се намира в зона на доскорошни кървави конфликти, поради което в региона продължават да съществуват потенциални огнища на напрежение на националистическа, етническа и религиозна основа, които при определени критични обстоятелства могат да генерират терористични атаки.

Въпреки това Република България не е пряка цел на международния тероризъм. Но страната ни има своята активна позиция в международните усилия в борбата с тероризма, поради което не може да се смята за застрахована от неговите жестоки прояви. Без да има стратегически характер терористичната заплаха е сред най-сериозните заплахи, пред които сме изправени.

Като заключение от представянето на средата на сигурност може да се каже, че промените в нея, нейната динамика имат взаимосвързан и взаимозависим характер. Но тези връзки са изключително сложни и многостранни, при това се намират в непрекъснато движение. Политиката за сигурност на Република България зависи преди всичко от развиването на способност за следене на промените в средата на сигурност в реално време, в нужната дълбочина и взаимна свързаност. Комплексното въздействие върху нашата сигурност изисква комплексен отговор и силен капацитет за операционен анализ и вземане на ефективни решения.

Политиката за сигурност следва да дава адекватни отговори на основните предизвикателства пред сигурността. Нейното предназначение е да осигури възможности за съгласувана реакция на непрекъснатите промени в средата на сигурност, както и ефективно, изпреварващо управление на промяна в системата за сигурност. Доброто управление в системата за сигурност е основно изискване за защита на интересите на гражданите, обществото и държавата.

Основни елементи на политиката за сигурност са втората основна част на политиката за сигурност. Те съставляват отговора на предизвикателствата, заплахите и рисковете произтичащи от средата на сигурност в нейните две измерения – външно и вътрешно.

Основният, интегриращ елемент на политиката за национална сигурност на Република България следва да бъде изграждането и поддържането на оптимално функционираща система за национална сигурност, която да работи в тясно сътрудничество с НАТО, ЕС, ООН, ОССЕ и с другите международни институции.

Такава система за национална сигурност следва да бъде основана на партньорството на държавата, местната власт, организациите и гражданите, да се ръководи оперативно на базата на единна комуникационно-информационна среда, почиваща върху интегрирана информационна система с нужната периферия от индикатори, пораждаща способности за предлагане на обработена информация и управленски решения. Системата за национална сигурност трябва да следи в реален мащаб на времето състоянието на средата на сигурност, както и своето собствено състояние, като реагира адекватно и своевременно на промените в тях.

Този основен интегриращ елемент е редно да не бъде интерпретиран в аспекта на идейните различия на основните партии в Република България, поради очевидно необходимия национален характер на подобна система. Освен това система от този тип, с непрекъснато действие в променяща се среда, се нуждае от висока степен на приемственост, когато се сменя една или друга власт в страната, което е още един аргумент в полза на нейния по възможност надпартиен характер.

Системата за национална сигурност е инструментът на политиката за сигурност, който следва да дава адекватния отговор на въздействията на средата на сигурност.

Политиката за сигурност се реализира в системата за национална сигурност, но в себе си политиката съдържа цял ред обособени елементи, чрез които тя отговаря на въздействията на средата.

Антитерористичният елемент на политиката за сигурност е един от основните. Вярно е, че в структурите за сигурност Република България създаде и развива сили за борба с тероризма. Широко е разгърната изследователската и практическо-приложната работа по изучаването, анализа и разработването на противодействието на съвременния тероризъм. От началото на века българската научна мисъл в сферата на сигурността е силно ангажирана с този тип изследвания. Изучаването на тероризма, на неговите прояви и противодействието му е съществена част от тематиката в редица висши учебни заведения, където се обучават както български, така и чуждестранни студенти.

Също така в страната се развиват способности за антитерористична защита на българските военнослужещи, полицаи и граждански лица участващи в мисии по установяване и поддържане на мира в конфликтни точки по целия свят. В тези мисии българските представители са подложени на относително по-висок риск от терористични атаки, в сравнение с гражданите на територията на Република България.

По тези въпроси нашата страна е в тясна връзка и в сътрудничество с други страни, които са наши съюзници и партньори за подпомагане на антитерористични акции в чужбина. Република България е член на коалицията на желаещите и в това си качество взе и продължава да взема участие в установяването на демократични условия в Ирак. Страната ни участва в подкрепа на законното правителство на Афганистан и допринася за намаляване и преустановяване на дейността на терористичните мрежи в тази държава.

Намирайки се относително настрани от преките терористични заплахи Република България следва да бъде ориентирана към няколко основни насоки.

Първата от тях е да се поддържа непрестанна активност на анализаторите, на разузнавателните и на полицейските служби, за да има страната висока способност за откриване и неутрализиране на терористични акции на територията на Република България. Следващата насока е да се поддържат и развиват държавните граници, като важен орган на националната сигурност и бариера срещу проникването на терористични мрежи и групи на територията на страната, а по този начин и на територията на Европейския съюз. Прилагане на високотехнологични средства за контрол на границата, както и развитие и усъвършенстване на национална идентификационна система.

Друга насока е подготовката на страната и на населението за подобряване на способността ни да се справяме с последиците от терористично нападение, като успоредно с тази подготовка да се обърне вниманието на държавата и на нейните партньори в лицето на частния сектор, отделните граждани и местната власт към подобряване на защитата на уязвима обществена инфраструктура и интензивно посещавани обществени обекти и места, като се подобри тяхното планиране, изграждане, пряка защита и контрол, както и снабдяването им с необходимите критични запаси в случай на криза и в частност на терористична атака. В дейностите по защитата от терористичен акт следва да се ангажират всички институции, власти и групи хора, да се включи населението на страната, представителите на практикуваните религиозни култове у нас, медиите. За целта е необходимо да се създадат правни условия за широко участие и за съвместни действия в интерес на борбата срещу терористичната заплаха.

В тази връзка е и следващата насока, а именно да се развива правната уредба отнасяща се до борбата с тероризма, така че да се постига нужната оперативна свобода на антитерористичните действия, но без да се стига до превишаване на правомощия, които да не допуснат нормалния живот на обществото.

Накрая, естествено е да се осигури нужното финансиране на тези дейности, да се поддържат тесни съюзнически отношения, както в зоните на нашето участие в регулиране на конфликти, така и съюзния формат на нашите отношения и разбира се да продължава изучаването на тероризма и набелязване на мерки за противодействието му, като акцентът да се поставя все повече върху превенцията, свързана с разкриване на антихуманния заряд на екстремистките идеи, както и върху усилията, които Република България реално полага за подпомагане на нормалния живот в зоните на конфликт, поразени от екстремистките действия.

**Използвана литература:**

1. Common Foreign and Security Policy - CFSP

European Security and Defense Policy - ESDP

Тагарев, Т., Отбранителна политика, обхват, основни компоненти и зависимости /Международни отношения, 36,2007, №1-2, с. 143.

1. Танев, Т., Истинската независимост се гарантира от доброто управление/Гласове, № 38,2008 г., с. 8.

Smith S. The Self-Image of a Discipline: A Genealogy of International Relations Theory // Theory of International Relations Today. Ed. by Steve Smith and Ken Booth. Cambridge, 1995., p. 19.

Waltz, K.N., Theory of international Politics, ed. Addisn-Wesley, Reading,1979.

Бахчеванов, Г.Малката държава в началото на ХХІ в., Военен журнал, 2005, № 2, с. 62-76.

Георгиев Хр. Принципи на изграждане и функциониране на специалните служби.Особености на гражданския контрол. Научен доклад на международна конференция, организирана от Балканския форум по сигурността. С., 2004, Публикувана в: “Разширяването на НАТО – повишаване на сигурността и защита на личността”

Бахчеванов, Г. Необходим ли е на Европа „нов“ съюз за сигурност в борбата срещу тероризма. Пловдив, ВУСИ, 2016.

Гилен Шеврие. Животът във френските „Моленбеци”. 2016. <http://www.memoriabg.com/2016/04/06/v-francia-sa-poseti-semenata-na-grajdanskata-voina/>.

[Efraim Karsh](https://www.google.bg/search?hl=bg&tbo=p&tbm=bks&q=inauthor:%22Efraim+Karsh%22). Islamic Imperialism: A History (Yale University Press, 2006). <https://books.google.bg/books?id=8Rw0NokDdzkC&redir_esc=y>

**Environmental Security: A Case Study of Climate Change Impacts in South – East Europe**

*Цветан Спасов, д.н.*

*Нов български университет*

***Abstract:***

***Keywords:***

**За необходимостта от прилагането на по-ефективни методи и средства в борбата с тероризма**

*проф. д-р Георги БОТЕВ*

*Академия на МВР*

***Резюме:*** *В доклада са представени данни за увеличаващата се честота и загуби от терористични атаки в света. Специално внимание е отделено на атаки срещу обекти от сектор „Транспорт”. Предложени са конкретни мерки за повишаване качеството на управление на риска от терористични атаки.*

***Ключови думи:*** *тероризъм, терористични атаки, борба с тероризма*

През последните години терористичните атаки в света се увеличиха значително. Както се вижда от данните на Департамента за вътрешна сигурност на САЩ, посочени в табл.1 и на фиг.1, през 1998 г. техния брой е бил 929, докато 2014 г. са извършени 16818 акта, т.е.18 пъти повече. Особено интензивно е нарастването на терористичните атаки в периода след 2010 г. Значително се е увеличил и броя на загиналите в резултат на същите. През 2000 г. в резултат на терористични атаки в света са загинали 3329 души, докато през 2014 г. този брой е32658, т.е. увеличението е близо 10 пъти.

**Таблица 1**. **Брой терористични актове в света в периода 1994 – 2014 г.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Година** | **Брой терористични**  **актове в света** | **Година** | **Брой терористични**  **актове в света** | **Година** | **Брой терористични**  **актове в света** |
| 1994 | 3455 | 2001 | 1882 | 2008 | 4779 |
| 1995 | 3079 | 2002 | 1297 | 2009 | 4713 |
| 1996 | 3023 | 2003 | 1253 | 2010 | 4782 |
| 1997 | 3201 | 2004 | 1156 | 2011 | 5007 |
| 1998 | 929 | 2005 | 2012 | 2012 | 8491 |
| 1999 | 1383 | 2006 | 2729 | 2013 | 11999 |
| 2000 | 1778 | 2007 | 3236 | 2014 | 16818 |

**Фиг. 1. Брой терористични актове в света в периода 1994 – 2014 г.**

Икономическите загуби от терористичните атаки в света достигат десетки, а в отделни години и стотици милиарди USD. За периода 2000 – 2014 г. преките икономически загуби от тези събития в света са представени в табл.№2 и на фиг.2. За 2014 г. по данни на лондонския Институт за икономика и мир от доклад "Световен рейтинг на тероризма"[1] само преките икономически загуби от същите се оценяват на 52.9 млрд. USD. Икономическите загуби (преките и само част от косвените) от терористичната атака срещу Световния търговски център в Ню Йорк и сградата на Пентагона във Вашингтон - САЩ на 11.09.2001 г. възлизат на над 100 млрд. USD[2].

**Таблица 2. Преки икономически загуби от извършените в света терористични атаки в периода 2000 – 2014 г.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Година** | **Преки икномически загуби, млрд. USD** | **Година** | **Преки икномически загуби, млрд. USD** | **Година** | **Преки икномически загуби, млрд. USD** |
| 2000 | 4,93 | 2005 | 11,07 | 2010 | 12,00 |
| 2001 | 51,51 | 2006 | 15,78 | 2011 | 12,31 |
| 2002 | 7,65 | 2007 | 20., 4 | 2012 | 16,96 |
| 2003 | 5,42 | 2008 | 13,40 | 2013 | 32,92 |
| 2004 | 10,99 | 2009 | 14,74 | 2014 | 52,90 |

**Фиг.2. Преки икономически загуби от извършените в света**

**терористични атаки в периода 2000 – 2014 г.**

Посочените по-горе данни показват, че днес тероризмът се превръща във все по-голямо предизвикателство пред човечеството. За отделните страни то е различно и променливо във времето. За нивото на същото до голяма степен дава представа глобалния индекс на тероризма (индексът измерва нивото на терористична дейност в отделните държави за предходния 10 годишен период по четири показателя: брой на терористичните актове, брой на жертвите, брой на ранените и равнище на преките материални загуби), който варира от 0 до 10. По данни на лондонския Институт за икономика и мир за глобалния индекс на тероризма за страните в света[1] към 2015 г. водещи в негативната класация са Ирак (индекс 10), Афганистан (индекс 9.233), Нигерия (индекс 9.213), Пакистан (9.065) и др. България с индекс 2.421 е на 70 - то място в класацията, а Белгия на с индекс 1.977 е на 82 - ро.

Няма държава в света, която да е защитена от терористични атаки. Наскоро извършените големи координирани такива в Париж и Брюксел отново потвърждават тази теза. Това налага необходимостта от усъвършенстване управлението на този риск, борбата с който налага обединяване на световната общност.

По данни на Департамента за вътрешна сигурност на САЩ за извършените терористични нападения, в периода 1970 – 2014 г. в света са регистрирани 141966 терористични акта (приетите критерии за класифициране на нападението като терористичен акт са: акта (атаката) цели постигането на политически, икономически, религиозни или социална цел; акта цели създаване на психоза сред населението за непосредствена заплаха от предизвикване на жертви сред същото; акта е в разрез с нормите на международното хуманитарно право (при военен конфликт е насочен срещу цивилното население).

Разпределението на извършените в света в периода 1970 – 2014 г. 141966 терористични акта по региони е посочено в табл. 3.

**Таблица 3. Разпределение на извършените в света периода 1970 – 2014 г. терористични атаки по региони**

|  |  |  |
| --- | --- | --- |
| **№ по ред** | **Регион** | **Брой терористични атаки 1970 – 2014 г.** |
| 1 | Австралия и Океания | 239 |
| 2 | Централна Америка и Карибите | 10338 |
| 3 | Централна Азия | 529 |
| 4 | Източна Азия | 758 |
| 5 | Източна Европа | 4204 |
| 6 | Средна източна и Северна Африка | 34462 |
| 7 | Северна Америка | 3195 |
| 8 | Южна Америка | 18453 |
| 9 | Южна Азия | 33273 |
| 10 | Югоизточна Азия | 9313 |
| 11 | Африка под Сахара | 11493 |
| 12 | Западна Европа | 15709 |

Както се вижда от данните, посочени в табл. 3, най-голям брой терористични атаки са извършени в Средна Източна и Северна Африка (24.3% от случаите), следвана от Южна Азия (23.4% от случаите), Южна Америка (13% от случаите), Западна Европа (11% от случаите), Централна Америка и Карибите (7.3%% от случаите) и др. В Източна Европа за този период са извършени 3% от терористичните атаки. През последните три години от анализирания период (т.е. за периода 2012 – 2014 г.) най-голям брой терористични атаки са извършени в региона на Средна източна и Северна Африка – 13750, следван от Южна Азия – 13388 и Африка под Сахара – 4446. През този период в Източна Европа са извършени 1024 терористични атаки, в Западна Европа техния брой е бил 779, а в Северна Америка – 318.

Разпределението на извършените терористични актове по използвани способи за терористична атака е представено в табл. 4.

**Таблица 4. Разпределение на извършените терористични атаки в периода 1970 – 2014 г. по използвани средства за атаката**

|  |  |  |
| --- | --- | --- |
| **№ по ред** | **Използвани средства** | **Брой терористични актове 1970 – 2014 г.** |
| 1 | Биологически опасни агенти | 36 |
| 2 | Химически опасни вещества | 264 |
| 3 | Експлозиви, взривни устройства | 73494 |
| 4 | Радиологически опасни вещества | 13 |
| 5 | Съботажна екипировка | 185 |
| 6 | С фалшиви средства | 53 |
| 7 | Огнестрелни оръжия | 51904 |
| 8 | Запалителни средства | 10907 |
| 9 | Ръкопашен бой | 3784 |
| 10 | Други | 178 |
| 11 | Превозно транспортно средство | 115 |
| 12 | Неизвестни | 15809 |

**Забележка:** При част от терористичните актове е използвано повече от едно средство.

Видно от данните, посочени в табл. 4, най-често използваните средства за терористична атака са експлозивите и взривните устройства ( в 51.7 % от случаите), следвани от огнестрелни оръжия (36.5% от случаите) и др. Зачестяват атаките със самоубийствени бомби. В периода 2000 - 2014 г. повече от 3600 терористични нападения в света са извършени с такива бомби, което представлява 5,1% от всички терористични атаки[3].

През последните години се увеличава значително честотата на терористичните атаки срещу обекти на сектор „Транспорт”, в т.ч. летища и авиопревозвачи. За периода 1970 – 2014 г. са извършени 7524 нападения срещу мишени от този сектор, представляващи 5.3% от всички терористични атаки, докато извършените през периода 2012 – 2014 г. 738 акта срещу такива обекти представляват 19% от всички терористични атаки[3]. Данни за част от същите са представени в табл. 5.

**Таблица 5. Данни за извършени терористични атаки срещу обекти от сектор „Транспорт” в периода 1970 – 2014 г.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Дата и обект (мишена) на терористичната атака** | **Средство, начин на извършване** | **Заги-нали, бр.** | **Постра-дали, бр.** |
| **1** | **2** | **3** | **4** | **5** |
| 1 | 01.08.1980 г., жп гара в Болоня, Италия | Взривно устройство | 85 | 200 |
| 2 | 30.08.1984 г., жп гара Пловдив (в чакалнята) | Взривно устройство | 1 | 40 |
| 3 | 09.03.1985 г., пътнически влак на гара Буново (вагон за майки с деца) | Взривно устройство | 7 | 9 |
| 4 | 22.07.1985 г., самолет “Боинг 747” на индийска авиокомпания над Ирландско море | Взривно устройство | 329 | - |
| 5 | 21.12.1988 г., самолет Боинг 767 на компания “PanAm” над град Локърби, Шотландия | Взривно устройство | 259 | - |
| 6 | 21.12.1994 г., метрото в Ню-Йорк | Взривно устройство |  | 50 |
| 7 | 20.03.1995 г., метрото в Токио | Обгазяване със зарин | 12 | 5000 |
| 8 | 25.12.1995 г., метрото в Париж | Взривно устройство | 7 | 60 |
| 9 | 17.10.1995 г. , метрото в Париж | Взривно устройство | - | 30 |
| 10 | 03.12.1996 г., метрото в Париж | Взривно устройство | 3 | 92 |
| 11 | 08.08.2000 г., метрото в Москва | Взривно устройство | 13 | 130 |
| 12 | 10.08.2001 г., пътнически влак в Ангола | Взривно устройство | 152 | 150 |
| 13 | 11.09.2001 г., два самолета Боинг-767 на авиокомпания “American Airlines” се врязват в северната и южната кули на Световния търговски център в Ню Йорк | Сблъсък на самолет в сграда | 2843 | - |
| 14 | 11.09.2001 г., самолет Боинг-767 на авиокомпания “American Airlines” се врязва в сградата на Пентагона | Сблъсък на самолет в сграда | 189 | - |
| 15 | 18.02.2002 г., метрото в гр. Тегу, Южна Корея | Взривно устройство (заложено от душевно болен) | 198 | 150 |
| 16 | 06.02.2004 г., метрото в Москва | Взривно устройство  Самоубийствена бомба (СБ) | 42 | 250 |
| 17 | 25.08.2004 г., самолет Ту-154 на авиокомпания “Сибир” над гр. Ростов на Дон, Русия | Взривно устройство  Жена СБ | 46 | - |
| 18 | 25.08.2004 г., самолет Ту-134 на авиокомпания “Волга-Авия” над гр.Тула, Русия | Взривно устройство  Жена СБ | 34 | - |
| 19 | 05.03.2004 г., четири пътнически влакови композиции в Мадрид, Испания | Десет взривни устройства | 192 | 1500 |
| 20 | 07.07.2005 г., метрото в Лондон и автобус | Четири взривни устройства  Четири СБ | 52 | 1000 |
| 21 | 11.07.2006 г., в ж.п.гари и влакови композиции в гр.Мумбай, Индия | Седем взривни устройства | 182 | 900 |
| 22 | 29.03.2010 г. Московско метро, станции Лубянка и Парк на културата | Две взривни устройства  Две жени СБ | 37 | 102 |
| 23 | 24.01.2011 г. Летище Демодедово, Москва | Взривно устройство  СБ | 35 | 110 |
| 24 | 21.10.2013 г. Волгоград, автобус | Взривно устройство  Жена СБ | 6 | 32 |
| 25 | 29.12.2013 г. Волгоград, жп гара | Взривно устройство  Жена СБ | 15 | 35 |
| 26. | 18.07.2012 г. автобус на летище Бургас | Взривно устройство  СБ | 7 | - |
| 27 | 22.03.2016 г. Брюксел летище „Завентем” | Взривно устройство  СБ | 14 | 100 |
| 28 | 22.03.2016 г. Брюксел метростанция „Малбек | Взривно устройство  СБ | 20 | 106 |

Средната смъртност при една терористична атака за периода 1970 – 2014 г. е 2.3 души, докато срещу обект от сектора „Транспорт” тя е 2.8 души[3]. Една от причините за това е по-голямата концентрация на хора в обекти на транспорта, видно и от последиците от извършени атаки, представени в табл.5 .

Процентното разпределение на терористичните атаки срещу конкретни групи обекти (мишени) от сектор „Транспорт” за периода 1970 – 2014 г. е представено на фиг.3 [3].



**Фиг. 3. Процентно разпределение на терористичните атаки срещу конкретни групи обекти (мишени) от сектор „Транспорт” за периода 1970 – 2014 г.**

Както се вижда от фиг. 3 най-често мишена на терористична атака са автобуси, следвани от влакове, съставляващи общо 61.6% от всички атаки срещу обекти от сектор „Транспорт”. Макар и значително по-малко обаче, атаките срещу автогари, летища, въздухоплавателни средства по време на полет и обекти на метрото поради голямата концентрация на хора не са по-малко щетоносни.

Защитата на обекти от сектор „Транспорт” от терористични атаки е сложна за изпълнение задача. Макар, че по същата се работи от дълги години, дори в страни с най-добри практики, като Израел, САЩ и др., все още сигурността на такива обекти не може да бъде гарантирана. Зачестяващите терористични атаки срещу автобуси, влакове, автогари, летища, метро и други обекти налагат нови методи и средства за тяхната защита. При това следва да се намери баланса, при който ефективността на функционирането на тези средства, обекти и системи, в т.ч. и икономическата, няма да бъда значително намалена.

Много са мерките, които следва да се приложат за гарантиране по-висока степен на сигурност на обектите от сектор ”Транспорт”. Част от тях са мерки за повишаване ефективността на системата за защита от терористични атаки като цяло. Като важни такива се предлага да се обърне внимание на следните:

1. Необходимо е да се усъвършенства съществуващата система за антитерористична защита. Съществува потребност от законодателно уреждане на правата и задълженията на всички органи за управление, сили за реагиране и населението при терористични атаки, координацията при управлението на дейностите по защитата от такива, в т.ч. по командването и контрола, конкретните ограничения на правата на гражданите, които могат да се наложат при такива ситуации и др.
2. Следва да се разработи и нормативно регламентира ефикасна методология за оценка на риска от терористични атаки срещу определени критични активи с конкретни критерии и показатели за нива на риска.
3. Необходимо е да се привлекат гражданите да оказват активна помощ на държавата в тази дейност. Добрата практика (например тази в САЩ) показва, че около 40% от терористичните атаки в страната се предотвратяват благодарение на подаването на сигнал до федералните власти от бдителни граждани за лица или други обекти или действия, предполагащи подготовката или извършването на такива. В тази насока у нас много малко се работи. Ето защо, повишаването подготовката на гражданите за идентифициране на лица и други обекти и сигнализиране при евентуална подготовка на терористични атаки, както и за действие и оказване на помощ при извършени такива, следва да бъде една от основните задачи на държавните органи, общинските управи и юридическите лица, стопанисващи обекти предполагаеми мишени (например собственици/оператори на критична инфраструктура и др.). Същата следва да обхване всички възрастови групи от населението. Активно участие при нейното изпълнение следва да имат медиите и НПО.
4. Следва да се изгради на териториално и обектово ниво система от технически и организационни мерки за контрол и защита от терористични атаки.

4.1. В технически план е необходимо да се обърне внимание на следните мерки:

4.1.1. Широко приложение на детектори за дистанционно откриване на експлозиви. Детекторите за дистанционно откриването на експлозиви (от 20м и повече) могат да помогнат за своевременно откриване на взривни устройства и боеприпаси и предотвратяване внасянето на такива в обекти, в т.ч. на обществения транспорт, контролирането на същите при транспортирането им по пътищата и други приложения. Независимо, че вече на пазара се предлагат такива детектори (например „Снифекс”), ограничените им възможности и специфичен начин за работа налагат разработването на нови такива с по-големи възможности и за по-широко приложение.

4.1.2. Ограничаване достъпа на автомобили (освен на обществения транспорт) в близост до аерогари, жп и автогари и до други обекти, в които се събират големи групи от хора. При подходящо планиране тази мярка би ограничила въздействието на коли-бомби при терористични нападения.

4.1.3. Изграждане на защитни бариери за пренасочване на ударна вълна от експлозия на коли-бомби, бариери за спиране нападението срещу обекти с автомобили и др.

4.1.4. По-широко приложение на системи за видеонаблюдение на обектово и териториално ниво с възможности за разпознаване на образи на лица, в т.ч. издирвани или свързани с терористични организации.

4.1.5. Проектиране на обекти от критичната инфраструктура с необходимата степен на защита от терористични атаки.

4.2. В организационен план е необходимо да се обърне внимание на следните мерки:

4.2.1. Следва да се изгради система за ефективен контрол на производството, търговията и употребата на вещества, които могат да бъдат използвани за самоделни взривни устройства.

4.2.2. Има необходимост от подобряване на плановете и процедурите за координиране на дейностите и реагиране при терористични атаки на всички нива – обектово, общинско, областно, ведомствено и национално.

5. Европейският съюз следва да изгради Механизъм на съюза за защита от терористични атаки. Основни елементи в него следва да бъдат: Оперативен център за координация; Обща система за комуникация и информация; екипи от подготвени експерти и капацитет от специализирани сили за реагиране, участващи под формата на доброволно обединяване на заявени от държави-членки ресурси; точки за контакт в държавите членки. Механизмът следва да бъде финансово осигурен с европейски средства и да подпомага държавите членки в осъществяването на управлението на риска от терористични атаки във всички етапи на цикъла, през които същото протича – от анализа и оценката на риска от такива атаки до анализа на операциите по противодействието на същите и набелязване на мерки за усъвършенстване управлението на този риск.

С посоченото по-горе не се изчерпват всички мерки, които следва да се приложат за повишаване качеството на управление на риска от терористични атаки. Нарастващата терористична заплаха, резултат на средата, в която живеем днес, реализираните терористични атаки и последиците от същите показват, че ние сме много уязвими и недостатъчно защитени от такива събития. Сложността на решаването на този световен проблем налага консулидирането в борбата с тероризма на цялото прогресивно човечество, прилагането на адекватни политики, стратегии и методологии за управление на този риск, както и разходването на по-големи ресурси за сигурност.

В национален план е необходимо да се изгради ефективна система за управление на националната сигурност, в която основно място да бъде отделено на дейностите касаещи управлението на риска от терористични атаки. Приетият наскоро Закон зауправление и функциониране на системата за защита на националната сигурност за съжаление не е добра основа за това.

**Използвана литература:**

1. Global Terrorism Index 2015.Institute for Economics and Peace. November 2015 London.
2. How much did the September 11 terrorist attack cost America? Institute for the Analysis of Global Security. <http://www.iags.org/costof911.html>.
3. Terrorism in Belgium and Western Europe; Attacks against Transportation Targets; Coordinated Terrorist Attacks. National Consortium for the Study of Terrorism and Responses to Terrorism.Report, March 2016.

**Стратегически аспект на киберсигурността на национално и регионално равнище**

*проф. д-р Венелин ГЕОРГИЕВ*

*Нов български университет*

***Резюме****: Успешното решаване на проблемите пред сигурността на различни равнища на сигурност зависи от редица фактори, сред които намира място синхронът и приемствеността в политиките и стратегии за справяне с тези проблеми. Това твърдение е в сила и по отношение на проблемите пред киберсигурността. От друга страна характерът на стратегията за киберсигурност изразява намеренията на нейните автори за начинът, по който се очаква да бъдат използвани ресурсите за постигане на целите в областта на сигурността на киберпространството. В доклада се представят резултатите от проведено изследване на стратегиите за киберсигурност на България и на ЕС, в основата на което се поставя тезата, че успехът на стратегическите документи в областта на киберсигурността на различни равнища на сигурност в значителна степен зависи от степента на тяхната приемственост и съгласуваност по отношение на принципите, мерките и действията.*

***Ключови думи***: *киберсигурност, стратегия, устойчивост, киберпространство, киберпрестъпление*

**Въведение**

Съвременните анализи на заплахите за сигурността извеждат на преден план тези, свързани с използване на информационните и комуникационните технологии, системи и мрежи в бизнеса и бита, познати като заплахи за киберсигурността или още заплахи в киберпространството. Сред основните аргументи за тази констатация намират място нарастващият дял на on-line услугите, увеличаването на броя на хората, разполагащи с достъп до интернет, нарастващият брой на престъпленията, експлоатиращи първите два фактора и т.н. Значимостта на заплахите за киберсигурността изискват фокусиране на вниманието върху съществуващите уязвимости и върху способностите за справяне с тях, което в комплексния си вид изисква провеждане на адекватни изследвания в областта.

В доклада се представят резултатите от направено изследване, в което като цел се поставя определяне на характера на предлаганата за обсъждане национална стратегия за киберсигурност „Кибер устойчива България 2020“ и степента на приемственост и съгласуваност на тази стратегия с аналогичната на нея, отнасяща се до регионално ниво на сигурност „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace“. Тезата, доказването на която се преследва в рамките на изследването се състои в това, че успехът на стратегическите документи в областта на киберсигурността на различни равнища на сигурност в значителна степен зависи от степента на тяхната приемственост и съгласуваност по отношение на принципите, мерките и действията. Изследователската методика включва основно използване на сравнителния анализ, с помощта на който на първо място е определен характерът на националната стратегия, а в последствие е определена степента на сходство с аналогичната стратегия на ЕС.

**Определяне на характера на националната стратегия за киберсигурност**

Един от възможните подходи за разработване на стратегия, в частност на стратегия за киберсигурност, е чрез използване на резултатите от предварително извършен анализ на силните и слабите страни, на възможностите и заплахите пред изследвания обект, т.е. с помощта на SWOT-анализ. Съчетаването на резултатите в тези четири области в съдържанието на разработваната стратегия дава възможност за създаване на четири типа стратегии[[91]](#footnote-91):

- настъпателна стратегия (SO), съчетаваща в себе си предимствата на разкритите силни страни при реализиране на възможностите, разкриващи се пред изследвания обект;

- отбранителна стратегия (ST), в съдържанието на която разкритите силни страни се използват за справяне с идентифицираните заплахи;

- стратегия за развитие (WO), характеризираща се със съчетаване на възможностите и слабите страни с идея за тяхното преодоляване;

- сдържаща стратегия (WT), при която усилията са насочени към отстраняване на идентифицираните слаби страни и снижаване на съществуващите заплахи.

За нуждите на изследването, от текста на националната стратегия за киберсигурност за извадени десет произволно избрани зависимости (логически връзки), за които е определено коя от изброените по-горе зависимости е в сила. Като източник на информация за силните и слабите страни, възможностите и заплахите за киберсигурността са използвани резултатите от SWOT-анализа, публикувани в края на документа. Резултатите от проведеното изследване са представени в таблица 1.

*Таблица 1. Характер на логическите връзки в националната стратегия за киберсигурност*

|  |  |  |  |
| --- | --- | --- | --- |
| Развитие на стратегии, политики и мерки | **W** | **O** | Постигане на високо равнище на мрежова и информационна сигурност |
| Изграждане на собствен организа - ционен и технически капацитет на бизнеса | **W** | **O** | Запазване на устойчивостта на киберпространството |
| Използване на партньорството с операторите на критична инфраструктура | **S** | **W** | Създаване на общи и специфични стандарти за киберсигурност |
| Хармонизиране на националното законодателство | **W** | **O** | Извеждане на тенденциите в заплахите за киберсигурността |
| Разкриване и разследване на киберпрестъпленията | **S** | **W** | Създаване на мерки за ранно идентифициране, откриване и превенция |
| Повишаване на информираността на потребителите | **W** | **O** | Избягване на престъпните деяния в киберпространството |
| Използване на форми за публично-частно партньорство | **S** | **O** | Повишаване на сигурността на връзките и инфраструктурата |
| Развитие на политиките и доктрините на въоръжените сили | **O** | **W** | Развитие на способностите за киберсигурност |
| Създаване на експертен капацитет за киберотбрана | **S** | **O** | Провеждане на периодични обучение и тренировки |
| Специализация на България в областта на киберотбраната | **W** | **O** | Създаване на адекватни организационни структури и използване на възможностите на програми за изграждане на центрове и лаборатории |

От анализа на резултатите, представени в таблица 1, става ясно, че при избраните логически връзки от текста на националната стратегия за киберсигурност преобладават тези от типа слаби страни – възможности WO (60%), което дава основание да се направи извода, че стратегията се отнася до групата на т.нар. стратегии за развитие.

**Изследване на степента на приемственост и съгласуваност между националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС**

Различните равнища на сигурност се характеризират с различен обхват и степен на детайлност на заплахите, уязвимостите, влияещите фактори и мерките за справяне с несигурността. В същото време между различните равнища на сигурност следва да съществува достатъчна степен на приемственост и съгласуваност в изброените направления, с което да се осигури увереност за постигане на желаните резултатите. Тези твърдения са в сила и по отношение на равнищата за киберсигурност, което предизвиква интереса към изследване на степента на съгласуваност между националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС. Изследването е направено с помощта на сравнителен анализ. Критериите, по които е извършено сравнението, са определени по метода на художествена абстракция, при която авторът сам избира кои са съществените критерии, които най-добри биха изразили степента на сходство или различие между изследваните обекти.

Сравнителният анализ на националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС е извършено с помощта на следните критерии:

- съвременна среда за киберсигурност;

- принципи, върху които се изгражда и поддържа киберсигурността;

- приоритети, мерки и дейности в областта на киберсигурността.

*Съвременна среда за киберсигурност*

В стратегията за киберсигурност на Европейския съюз се прави оценка, че през последните две десетилетия Интернет като цяло и в по-широк аспект киберпространството оказват изключително влияние върху обществата и тяхното развитие в различни области: ежедневен живот, социално взаимодействие, фундаментални права, икономика, сигурност и т.н. Благодарение на своите особености, киберпространството премахва бариерите на физическите и географските граници между отделните страни и техните граждани, като в същото време създава условия за споделяне на данни и информация в глобален мащаб. Информационните и комуникационните технологии се превръщат в гръбнака на икономическото развитие и в същото време представляват критически важен ресурс за икономическия сектор. Успоредно с нарастването на свободата на потребителите в киберпространството, нараства и потребността от защита на техните права и като цяло защита на принципите на демократичното общество и валидността на закона. В документа се прави констатацията, че свободата на on-line услугите и комуникациите се нуждае без съмнение от защитеност и сигурност. Водещата роля в това направление се делегира на отделните държави. От друга страна, частният бизнес се определя като един от големите собственици и потребители в киберпространството, което определя значимостта на неговото място и неговата роля и отговорности за създаване на сигурно киберпространство.

Особено внимание в съдържанието на стратегията на ЕС за киберсигурност следва да се обърне на оценката за това, че случващото се през последните години от една страна доказва предимствата и възможностите, които киберпространството предлага, но от друга страна категорично подчертава уязвимостите пред сигурността на това пространство. Броят на инцидентите с киберсигурността, които в огромната си част са с международен характер, нараства с алармиращи темпове и води до създаване на различен тип кризи в различни области на социално-икономическия живот: кризи със сигурността на веригите за доставка на стоки и услуги; кризи с управлението и функционирането на обекти от критичната инфраструктура и т.н. Оценката на заплахите за киберсигурността по отношение на техния източник е категорична и включва организираната престъпност, международния тероризъм, политически мотиви, държавно спонсорирани атаки, природни бедствия, неумишлени и умишлени човешки действия и др. Характерна особеност е стремежът на киберпрестъпниците да развиват и използват все по-нови, усъвършенствани и иновативни методи и инструменти за добиване на нерегламентиран достъп до компютърни системи и мрежи, кражба на чувствителна информация, извършване на икономически шпионаж и т.н. В страните извън ЕС съществуват държави, чиито правителства използват киберпространството за наблюдение и контролиране на дейността и живота на гражданите.

В проекта на национална стратегия за киберсигурност се посочва тенденцията за целенасочено използване на възможностите на киберпространството за развитие на различни сфери на обществения живот: икономика, социални отношения, култура, наука, образование, политически живот и т.н. Изразена в цифри тази тенденция показва, че близо 60% от домакинствата и над 90% от фирмите разполагат и използват достъп до Интернет. Освен това 50% от фирмите използват автоматизиран обмен на данни с външни за тях информационни и комуникационни системи. Оценката е, че почти цялата комуникация между бизнеса и публичната администрация е по електронен път, а броят на услугите за гражданите, предоставяни с помощта на Интернет, нараства. Заслужава да се отбележат оценките за това, че на национално ниво страната се нарежда сред първите двадесет страни по осигуряване на скоростен Интернет, което представлява сериозна предпоставка за развитие на предлаганите услуги[[92]](#footnote-92).

Успоредно с ползите от развитието на киберпространството, в проекта за национална стратегия за киберсигурност се изтъква появата на нови свързани заплахи и рискове, източниците на които се търсят в дейността на държавни, военни и терористични организации, индустриален шпионаж, киберпрестъпници, умишлени или неумишлени действия на крайни потребители. Обхватът на мотивите за извършване на киберпрестъпления се оценява като широк и включващ от извличане на икономически ползи до проява на любопитство и демонстриране на надмощие. Заслужава да бъде обърнато внимание на оценката за това, че кибератаките са „асиметрични“, т.е. такива, които с помощта на малки усилия и неголеми инвестиции могат да нанесат огромни поражения, които при това не винаги са предсказуеми.

Обобщаването на резултатите от сравнителния анализ по отношение на съвременната среда за киберсигурност дава възможност да се направи извода, че в съдържанието на проекта за национална стратегия за киберсигурност и стратегията за киберсигурност на ЕС съществува необходимото ниво на синхрон и приемственост, което създава обща или сходна основа за по-нататъшното изследване на проблемите, свързани с киберсигурността.

*Принципи, върху които се изгражда и поддържа киберсигурността*

В стратегията на ЕС са посочени основните принципи, които служат като основа или като фундамент при създаване на политики, разработване и прилагане на мерки за постигане на приемливо ниво на киберсигурност на регионално равнище. Тези принципи се отнасят до следното[[93]](#footnote-93):

- прилагане на политики, процедури и мерки за киберсигурност, които отговарят и защитават ключовите ценности на Европейския съюз;

- защита на фундаменталните права на всички актьори в киберпространството, защита на свободата на словото, личното пространство, личните данни и идентичността на гражданите;

- осигуряване на достъп на всеки потребител до Интернет, предлаганите услуги и публичните потоци от информация;

- изграждане и прилагане на ефективни модели за управление в киберпространството, зачитащи демократичните ценности при участие на всички заинтересовани страни;

- споделена отговорност на всички участници в киберпространството по отношение на гарантиране на сигурността.

В проекта за национална стратегия за киберсигурност са изброени принципите, върху които трябва да стъпи изграждането на среда за киберсигурност и на способности за противодействие срещу киберпрестъпността. Централно място в списъка на принципите заема осигуряване на защитата на основните ценности на ЕС и запазване на силата на закона. Като допълващи или подпомагащи принципи са изведени следните[[94]](#footnote-94):

- неделимост на киберсигурността от националната сигурност;

- защита на правата на гражданите, свободата на словото, личните данни и личния живот на хората;

- пропорционалност на разходите и обхвата на мерките за осигуряване на киберсигурност и значимостта на съответните заплахи и рискове;

- споделена отговорност, намираща израз в прилагане на интегриран подход при разпределение на ролите и отговорностите, свързани с киберсигурността на всички нива на управление и в областите на държавните институции, частния бизнес и гражданите;

- периодична оценка на състоянието на заплахите и рисковете за киберсигурността, както и на способностите за противодействие срещу киберпрестъпността при използване на адекватни методи и интегриране на резултатите в осъвременените варианти на стратегии и пакети от мерки;

- прозрачност при формиране и изпълнение на политиките за киберсигурност и кибер устойчивост;

- ангажираност на всички заинтересовани страни и развиване на адекватни механизми за публично-частно партньорство, мрежово управление и мета-управление;

- съгласуваност с международните ангажименти и принципи на сътрудничество, активно участие в процеса по създаване на общи способности за защита на киберпространството;

- обвързване на целите, приоритетите и мерките от стратегията с конкретен план за действие, отговорности, ресурси и показатели за ефективност.

Сравнителният анализ показва съответствие между принципите, на базата на които се предвижда създаването на мерки за киберсигурност и които са формулирани в проекта за национална стратегия за киберсигурност и стратегията за киберсигурност на ЕС.

*Приоритети, мерки и дейности в областта на киберсигурността*

Във фокуса на дейностите и мерките за постигане на киберсигурност на регионално равнище са поставени няколко основни зависимости. На първо място в стратегията на ЕС за киберсигурност се посочва стремежа към балансиране на достъпността до киберпространството и сигурността на същото това пространство. Очевидна е обратно пропорционалната зависимост, която свързва тези два параметъра: при увеличаване на достъпността ще намалее сигурността на услугите в киберпространството и обратно – засилването на мерките за сигурност като следствие ще снижат достъпността до предлаганите услуги. Търсенето на баланс между достъпност и сигурност се затруднява от една страна предвид динамичния характер на промените в киберпространството и от друга страна за сметка на необходимостта от постигане на баланс на различни нива и между апетитите на риска на различни актьори в киберпространството. Друга зависимост определя отделните държави като носители на основната отговорност за справяне с предизвикателствата пред киберсигурността. В своята цялост, дейностите и мерките, които ЕС определя в стратегията за киберсигурност, могат да бъдат определени като краткосрочни и дългосрочни, включващи изискванията на разнообразни политически документи, изпълнявани от различен тип актьори, опериращи в киберпространството. Всички предвидени мерки и дейности на регионално равнище обслужват зададените в стратегията приоритети, които могат да бъдат определени по следния начин[[95]](#footnote-95):

- постигане на киберсигурност, която в последствие да прерасне в кибер устойчивост: ключов момент при изграждане на среда за киберсигурност на регионално ниво и възможности за противодействие срещу киберпрестъпността е създаване на общи способности и процедури за ефективно взаимодействие. Съществен компонент на процеса по изграждане на пакет от способности за киберсигурност е обучението на всички участници в киберпространството за разпознаване и противодействие срещу инциденти от различен тип;

- нарастване на степента на готовност за отговор на инциденти с киберсигурността: в основата на този приоритет стои разбирането за това, че киберсигурността представлява обща и споделена отговорност на страните от ЕС, на държавните институции, частния бизнес, академичната общност и отделните потребители. Нещо повече, в стратегията за киберсигурност на ЕС се прави оценката, че крайните потребители на услугите в киберпространството играят ключова роля при осигуряване на сигурността на компютърните системи и мрежи;

- снижаване на размерите на киберпрестъпността в нейните различни нюанси (области): в анализираната стратегия се подчертава факта, че киберпрестъпността към момента е най-бързо развиващата се престъпност на регионално равнище (като пример: за един ден броят на жертвите на киберпрестъпления в световен мащаб се оценява на един милион души). Мерките за повишаване на ефективността на противодействието срещу киберпрестъпността следва да отчитат особеностите на киберпрестъпленията, каквито са: използването на нови технологии; сравнително нисък риск за престъпниците; наличие на висока мотивация, идваща от възможностите за извличане на значителни ползи, в това число и финансови и т.н.

- изграждане на оперативни способности за противодействие срещу киберпрестъпленията: в този аспект в стратегията за киберсигурност на ЕС се прави оценка, че правоприлагащите органи не са в състояние да противодействат по един достатъчно ефективен начин на киберпрестъпленията с помощта на традиционните методи и средства или поне не без комбиниране на традиционните методи и средства със специфични инструменти, отговарящи на особеностите на този вид престъпност. В стратегията се препоръчва на страните да обърнат внимание върху изграждането на специализирани структури и способности за противодействие срещу киберпрестъпността, които освен всичко друго да предполагат достатъчно ефективно международно сътрудничество;

- подобряване на координацията на ниво ЕС при изграждане на среда за киберсигурност и противодействие срещу киберпрестъпленията.

В проекта за национална стратегия за киберсигурност са определени неотложните действия (приоритетите) в областта на киберсигурността. Сред тези приоритети попадат:

- създаване на обща визия, национална стратегия и политика за киберсигурност и кибер устойчивост

- обединяване на капацитета и способностите на всички заинтересовани страни, в това число държава, бизнес, академични, научни и неправителствени организации;

- осигуряване на необходимите човешки, финансови, организационни и технически ресурси за изграждане и поддържане на среда за киберсигурност;

- периодичен преглед и оценка на рисковете за киберсигурността и координиране на стратегиите за противодействие срещу кибер заплахите;

- усъвършенстване на правната рамка и регулаторните механизми в областта на киберсигурността;

- балансиране на мерките по отношение на запазване на правата и свободите на гражданите и изграждане и поддържане на желано ниво на сигурност;

- особено внимание и ангажимент към проблемите на киберсигурността на обектите от критичната инфраструктура;

- компенсиране на сравнителното изоставане от партньорите от НАТО и ЕС в мерките и дейностите във връзка с киберсигурността.

Така изброените приоритети очертават полето от дейности, които са намерили място в проекта за национална стратегия за киберсигурност. В документа тези дейности са групирани в няколко направления, всяко от които е подробно описано. На първо място като област на действие е посочено установяването и развитието на национална система за киберсигурност и кибер устойчивост, която се характеризира с достатъчно високи нива на ефективност и ефикасност. Тази система се разглежда като неделима част на системата за управление и защита на националната сигурност и включва органи и институции с определени роли и задължения на национално и секторно ниво. Съвкупността от мерки, целящи изграждане и поддържане на национална система за киберсигурност включва:

- разработване и внедряване на стратегически документи под формата на политики, стратегии и планове за изграждане на желано ниво на киберсигурност. В организационен аспект стратегията предвижда създаване на Съвет за кибер устойчивост към Министерски съвет с направляващи и стратегически функции. Ролята на секретар на съвета по кибер устойчивост се изпълнява от Националния координатор по киберсигурност;

- постигане на оперативна координираност между всички участници в киберпространството с акцент върху проблемите на сигурността. Стратегията предвижда на оперативно ниво да се създаде организационна мрежа със съответната техническа платформа, а именно Национална координационно-организационна мрежа за киберсигурност, както и Национален кибер ситуационен център, който да бъде в рамките на Националния ситуационен център;

- изграждане на Национална система за управление при кибер кризи, която да бъде интегрирана част на Националната система за управление при кризи. Управленските процедури при възникване на кибер криза е предвидено да следват насоките от Европейските стандартни оперативни процедури за взаимодействие и модела за взаимодействие и управление при кризи на НАТО.

Втората област от дейности в проекта на стратегия за киберсигурност на България се отнася до мрежовата и информационната сигурност, които се представят като фундамент на кибер устойчивостта. Тези дейности са насочени към:

- постигане на високо общо ниво на мрежова и информационна сигурност във всички сегменти на киберпространството;

- постигане на сигурност и устойчивост на комуникационните и информационните системи на държавните институции, администрацията и електронното управление;

- ангажиране на частния сектор в подобряване на мрежовата и информационната сигурност;

- развитие от киберсигурност към кибер устойчивост.

Следващата група дейности в проекта за национална стратегия за киберсигурност касае защитата и устойчивостта на дигитално зависимата критична инфраструктура и целят гарантиране на надеждно и безпроблемно изпълнение на основните функции на тази чувствителна от гледна точка на сигурността система. Като основни направления за развитие на дейностите в това направление се разглеждат:

- подобряването на взаимодействието между държавата и операторите на критични инфраструктури. Като възможни инструменти се посочват разпределението на ангажиментите и засилване на сътрудничеството между държавата и операторите на критична инфраструктура, изработване и внедряване на общи и специфични стандарти за киберсигурност, прилагане на процес за оценяване и управление на рисковете за киберсигурността, въвеждане на оперативни процедури за комуникация и координация в условия на кибер криза и др.

- развитие и модернизация на системата за управление и защита на критична инфраструктура;

- своевременна защита на новите области на киберпространството, появяващи се за сметка на разширяване на оценката за критичност на информационните и комуникационни системи.

Като обособена група от дейности, към които са насочени мерките в проекта за национална стратегия за киберсигурност са определени тези, свързани с подобряване на взаимодействието и споделяне на информация между държава, бизнес и общество. Тези мерки са разделени в следните групи:

- установяване на ефективни механизми за споделяне на информация и ангажираност на всички заинтересовани лица, което включва идентифициране на тези лица; определяне на техните роли, интереси и адекватни форми за участие в националната система за киберсигурност; създаване на условия за споделяне на информация чрез изграждане на колективни платформи; изграждане на доверие за обмен на информация чрез използване на адекватни протоколи и правила; установяване на ефективно публично-частно партньорство за киберсигурност

- развитие на индустриален технологичен капацитет и споделени способности, което да бъде постигнато за сметка на технологично развитие на индустрията, модернизация и интелигентна специализация; изграждане на технологични паркове, центрове за върхови постижения и центрове за компетентност; създаване на достатъчно ефективни механизми за споделяне на ресурси, капацитет и способности за киберсигурност; стимулиране на националните и мултинационалните компании в областта на информационните и комуникационни системи;

- фокус върху малкия и среден бизнес, към който ще бъдат отправени предложения под формата на проекти и програми за развитие на конкурентоспособността чрез изграждане на адекватна кибер култура; включване в мрежите за превенция и споделяне на информация; организиране на специфични секторни и между-секторни упражнения, симулации и учения;

- установяване на обща комуникационна стратегия за информираност относно кибер въздействия и противодействия;

- изграждане на сигурна, свободна и достъпна интернет среда посредством адаптиране и прилагане на препоръките на международните интернет институции и организации.

Анализът на съдържанието на двете стратегии в частта им, описваща приоритетите, мерките и дейностите в областта на киберсигурността, показва наличие на сходство и приемственост.

**Заключение**

Резултатите от проведеното изследване, които са представени в доклада, дават възможност да бъдат направени два основни извода. На първо място може да се каже, че определеният характер на националната стратегия за киберсигурност като „стратегия за развитие“ отговаря на намеренията на страната да изгражда способности за киберсигурност, да си партнира със страните от НАТО и ЕС в тази област и дори в определени сегменти да се пребори за заемане на водеща роля. На второ място резултатите от изследването доказват наличието на видима степен на съгласуваност и приемственост между двата аналогични документа, отнасящи се до национално и регионално равнище на сигурност. Този факт засилва положителните очаквания за приноса, който стратегиите за киберсигурност ще осигурят по пътя към изграждане на сигурно киберпространство и преход към кибер устойчивост. Като цяло може да се каже също така, че резултатите от изследването потвърждават формулираната теза, доказват постигането на целта и като следствие определят приноса на самото изследване към решаване на проблемите по справяне със заплахите за киберсигурността.

**Използвана литература**

1. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013

2. Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016

3. Георгиев В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015

**България в ЕС – перспективи и проблеми**

1. *Afghanistan Opium Survey 2014 - Cultivation and Production - http://www.unodc.org/documents/crop-monitoring/Afghanistan/Afghan-opium-survey-2014.pdf* [↑](#footnote-ref-1)
2. *Съгласно измененията от 18.03.2015, №1176; № 1177* [↑](#footnote-ref-2)
3. *Например Испания е въвела наказателна отговорност за ЮЛ при престъпления свързан с трафик на хора.*  [↑](#footnote-ref-3)
4. *Например в чл. 13 Законът против наркотиците на Иран (приет през 1997 г., посл. изм 2013 г.) предвижда отнемане на лицензиите за дейност на търговски предприятия, които съхраняват, произвеждат или разпространяват наркотици.* [↑](#footnote-ref-4)
5. *Законодателството на Таджикистан в тази сфера обаче демонстрира друг дефицит. Чл. 262 изглежда има по-тясно приложно поле ratione materiae от минималните стандарти на конвенциите на ООН (напр. чл. 6 Конвенцията от Палермо).* [↑](#footnote-ref-5)
6. *Иранската законодателна рамка показва и друг значителен дефицит – все още е предстояща изричното включване на финансирането на тероризма като предикатно престъпление.*  [↑](#footnote-ref-6)
7. *Обосноваването на глоба като възможно единствено наказание с цел да се постигне възстановяване на вредите, не може да бъде подкрепено поради резултата от систематичното тълкуване на чл. 262 и чл. 57 от Наказателни кодекс на Таджикистан. Чл. 57 предвижда конфискация на облагите от престъплението пране на пари.*  [↑](#footnote-ref-7)
8. *Минската конвенция има по-широка, а Кишиневската по-тясна приложимост в бившите съветски републики.*  [↑](#footnote-ref-8)
9. *Аналогично Texaco v Libya 53 ILR 389, 461 (1977) реферирайки към този принцип.*  [↑](#footnote-ref-9)
10. *Към лятото на 2015 г. Иран има двустранни договори по въпросите на международната правна помощ с Ирак (2012), Тайланд (2011), Афганистан, Турция, ОАЕ (2010), Инди я (2009), Армения, Беларус (2008), Република Южна Африка, Киргизстан, Туркменистан (2007), Казахстан, Украйна (2006), Кувейт (2005), Алжир (2004), Сирия (2002) и Азербайджан (1999).* [↑](#footnote-ref-10)
11. *Виж Khodzhayev v. Russia (no. 52466/08), Khaydarov v. Russia (no. 21055/09), Iskandarov v. Russia (17185/05), Gaforov v. Russia (no. 25404/09) и Dzhurayev v. Russia (no. 71386/10).* [↑](#footnote-ref-11)
12. *Освен това Законът за прилагане на финансовите присъди (2014 г.) и Законът за прилагане на гражданските съдебни решение (1977 г.) също предвиждат форми на конфискация извън наказателния процес.* [↑](#footnote-ref-12)
13. *Ще има ли Европа собствени въоръжени сили?* ***a-specto. 31.08.2015 г.*** [*http://a-specto.bg/eu-army/*](http://a-specto.bg/eu-army/) [↑](#footnote-ref-13)
14. *Договорът от Лисабон – отражение върху политиката за сигурност и отбрана на Европейския съюз, изводи и перспективи за България. МО на Република България. Дирекция „Политика за сигурност и отбрана”. София 2009* [↑](#footnote-ref-14)
15. *Ще има ли Европа армия?* [*http://glasove.com/categories/komentari/news/shte-ima-li-evropa-armiya*](http://glasove.com/categories/komentari/news/shte-ima-li-evropa-armiya) [↑](#footnote-ref-15)
16. ***Христо А. Христов. Аспекти на общата политика за сигурност и отбрана на Европейския съюз*** [↑](#footnote-ref-16)
17. ## *Jérôme Legrand. Обща политика за сигурност и отбрана. Европейски парламент. 11.2015.* [*http://www.europarl.europa.eu/atyourservice/bg/displayFtu.html?ftuId=FTU\_6.1.2.html#\_ftn1*](http://www.europarl.europa.eu/atyourservice/bg/displayFtu.html?ftuId=FTU_6.1.2.html#_ftn1)

    [↑](#footnote-ref-17)
18. *Данните са за 2010 г., публикувани от Евростат.*  [↑](#footnote-ref-18)
19. *European Aeronautic Defence and Space Company (EADS).* [*http://www.britannica.com/topic/European-Aeronautic-Defence-and-Space-Company*](http://www.britannica.com/topic/European-Aeronautic-Defence-and-Space-Company)*.*  [↑](#footnote-ref-19)
20. *Член 6. За целите на член 5 за въоръжено нападение срещу една или повече от страните по Договора ще се смята въоръжено нападение: срещу територията на някоя от страните по Договора в Европа или Северна Америка, срещу Алжирските департаменти на Франция, срещу територията на Турция или срещу островите в Северноатлантическата зона на север от Тропика на рака, намиращи се под юрисдикцията на някоя от страните по Договора; срещу въоръжените сили, кораби или самолети на някоя от страните по Договора, когато те се намират върху или над тези територии или друг район на Европа, в който от датата на влизането на Договора в сила са били разположени окупационни сили на някоя от страните по Договора, в Средиземно море или в Северноатлантическата зона на север от Тропика на рака.* [↑](#footnote-ref-20)
21. *Secret Plot Exposed: EU in stealth plan to set up army by merging German and Dutch forces. An EU armed forces is being set up "by stealth" with the merger of the German and Dutch armies and navies, it has emerged. By David*  [↑](#footnote-ref-21)
22. *Стратегия за национална сигурност на Република българия* [*http://rdsc.md.government.bg/BG/About/Akademi/20110421\_nac\_otbr\_strategia.pdf*](http://rdsc.md.government.bg/BG/About/Akademi/20110421_nac_otbr_strategia.pdf) *(достъпен на 20.04.2016)* [↑](#footnote-ref-22)
23. *Вж. по-подробно: Laffin John.The World in Conflict 1991. Oxford: Brassey’s, 1991* [↑](#footnote-ref-23)
24. *Попов, И. Война будещего: взгляд из- за океана. М., изд. АСТ „ Астрель, 2004, Глава 4. „Нетрадиционные” войны будущего* [↑](#footnote-ref-24)
25. *Бжежински, З. Изборът. С., изд. Обсидиан, 2004 г., с. 25-26.* [↑](#footnote-ref-25)
26. *Пак там, с. 30* [↑](#footnote-ref-26)
27. *Вж. по-подробно:Семерджиев, Цветан. Стратегическо ръководство и лидерство. Среда.С., 2007, с.236-246.* [↑](#footnote-ref-27)
28. *Цветков, Георги. Концепция на НАТО за асиметрични военни действия. // Военен журнал, 2008, бр. 3, с. 6.* [↑](#footnote-ref-28)
29. *В англоезичната литература се използват термините: аsymmetric warfare, threats, tactics, conflicts. Виж например: S. Flynn.R. Wedgwood and K. Roth: Combatants or Criminals? How Washington should handle terrorists // Foreign Affairs. 2004. Vol. 83. No 3; I. Arreguin-Toft, How the Weak Wins Wars: A Theory of Asymmetric Conflict //International Security. 2001. Vol. 26. No 1. Виж също: Социология современных войн: Материалы научного семинара / Под ред. П.А. Цыганкова, И.П. Рязанцева. М.: Альфа-М, 2004; Мюнклер Х. Терроризм сегодня. Война становится асимметричной // International Politik. 2004. № 1; Мейз М. Эпоха стратегической асимметричности: Способность использовать нетрадиционные способы ведения войны определяет победу // Независимое военное обозрение. 2005. № 14; Генис А. Асимметричная война.*

    *(*[*http://www.svoboda.org/programs/OTB/2003/OBT.082303.asp*](http://www.svoboda.org/programs/OTB/2003/OBT.082303.asp)*); Комлева Н., Борисов А. Асимметричные войны – геополитическая технология современного терроризма // Обозреватель. 2002. № 11-12 (http://rau.su/observer/ N11-12\_02/index.htm). America the vulnerable // Foreign Affairs. 2002. Vol. 81. No 1* [↑](#footnote-ref-29)
30. *FIуnn, S., R Wedgwood, К. Roth. Combatants or Criminals? How Washington should handle terrorists. - Foreign Affairs, 2004, Vol. 83, No 3; Arreguin-Toft. How the Weak Wins Wars: A Theory of Asymmetric Conflict. - International Security, 2001, Vol. 26, No 1. Кременюк В.А. Современный международный конфликт: проблемы управления // Международные процессы. 2003. № 1. Вж. по-подробно: Хинков, Митко. Новата среда за сигурност и асиметричния характер на съвременните конфликти. // Военен журнал, 2010, № 1-2, 17-30,* [*http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1*](http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1) *(достъпни на 20.04.2016)* [↑](#footnote-ref-30)
31. *Вж. по-подробно: Хинков, Митко. Новата среда за сигурност и асиметричния характер на съвременните конфликти. // Военен журнал, 2010, № 1-2, 17-30* [↑](#footnote-ref-31)
32. *Професор, доктор по теория на международните отношения и геополитика в Томския държавен университет.* [*http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1*](http://geopolitica.eu/drugi-statii/839-asimetrichniyat-harakter-na-savremennite-konflikti?showall=1) *(достъпен на 20.04.2016)* [↑](#footnote-ref-32)
33. *Люттвак, Эдвард. Стратегия: Логика войны и мира. Пер. с англ. М., Университет Дмитрий Пожарский”, 2012.С. 283.* [↑](#footnote-ref-33)
34. *Хинков, Митко. Новата среда за сигурност и асиметричния характер...,с.18.* [↑](#footnote-ref-34)
35. *Вж. по-подробно: Цветков, Георги. Концепция на НАТО за асиметрични военни действия. // Военен журнал, 2008, бр. 3, с. 8-9.* [↑](#footnote-ref-35)
36. *Хинков, Митко. Новата среда за сигурност и асиметричния характер, с. 19-20.* [↑](#footnote-ref-36)
37. *Пак там, с. 20-22.* [↑](#footnote-ref-37)
38. *Пак там, с. 22.* [↑](#footnote-ref-38)
39. *Бъркоуиц, Б. Новото лице на войната. С., ВИ, 2003, с. 88.* [↑](#footnote-ref-39)
40. *Христов, П. Проблеми на регионалната сигурност в условията на асиметричните опасности и заплахи. С., Научен алманах, ВСУ „Ч. Храбър” и Фондация „Ханс Зайдел”, 2008 г., с. 10.* [↑](#footnote-ref-40)
41. *Вж. по-подробно: Савов, Александър. Асиметрична война. // Геополитика, 2006, бр. 4.* [*http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1*](http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1) *(достъпен на 16.04.2016)* [↑](#footnote-ref-41)
42. *Хочешь мира, победи мятежевойну. Творческое наследие Е. Э. Месснера, М. Военный университет, Русский путь, 2005. С. 132–159.* [↑](#footnote-ref-42)
43. *Савов, Александър. Асиметрична война.//Геополитика, 2006, бр. 4.* [*http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1*](http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1) *(достъпен на 16.04.2016)* [↑](#footnote-ref-43)
44. *Хочешь мира, победи мятежевойну. Творческое наследие Е. Э. Месснера, М. Военный университет, Русский путь, 2005. с. 132–159.* [↑](#footnote-ref-44)
45. *Савов, Александър. Асиметрична война.//Геополитика, 2006, бр. 4.* [*http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1*](http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1) *(достъпен на 16.04.2016)* [↑](#footnote-ref-45)
46. *Herfried Munkler, "Uber den Krieg. Stationen der Kriegsgeschichte im Spiegel ihrer theoretischen Reflexion". Frankfurt am Main: Velbruck Wissenschaft, 2002* [↑](#footnote-ref-46)
47. *Пак там.* [↑](#footnote-ref-47)
48. *Савов, Александър. Асиметрична война.//Геополитика, 2006, бр. 4.* [*http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1*](http://geopolitica.eu/2006/broi42006/547-asimetrichnata-voyna-?showall=1) *(достъпен на 16.04.2016)* [↑](#footnote-ref-48)
49. *Вж. по-подробно: Цветков, Георги. Концепция на НАТО за асиметрични военни действия. // Военен журнал, 2008, бр. 3, с. 5.* [↑](#footnote-ref-49)
50. *Пак там, с. 6.* [↑](#footnote-ref-50)
51. *Brussels, 9.9.2015 JOIN (2015) 40 final. European Commission. High Representative of the Union for Foreign Affairs and Security Policy. Addressing the Refugee Crisis in Europe: The Role of EU External Action. 2015. <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/communication\_on\_addressing\_the\_external\_dimension\_of\_the\_refugee\_crisis\_en.pdf> 9.05.2016* [↑](#footnote-ref-51)
52. *710 000 Migrants Entered EU in the First Nine Months of 2015. 2015. <http://frontex.europa.eu/news/710-000-migrants-entered-eu-in-first-nine-months-of-2015-NUiBkk> 9.05.2016* [↑](#footnote-ref-52)
53. *“Migrant crisis is a security crisis”, says EU foreign policy chief. 2015. <http://www.telegraph.co.uk/news/worldnews/europe/eu/11597651/Migrant-crisis-is-a-security-crisis-says-EU-foreign-policy-chief.html> 9.05.2016* [↑](#footnote-ref-53)
54. *Стефанов, Н. Миграционната вълна и заплахите за националната сигурност. // Сборник с доклади на Институт за стратегии и анализи от национална конференция „Бежанската вълна и предизвикателствата пред националната сигурност“, 2015, с. 38.* [↑](#footnote-ref-54)
55. *Migration crisis and terror threat fueled by un-policed seas on Europe’s Doorstep. 2016. <http://www.express.co.uk/news/uk/641543/Migrant-crisis-terrorists-people-smugglers-exploiting-Mediterranean-sea> 9.05.2016* [↑](#footnote-ref-55)
56. *“Migrant crisis is a security crisis”, says EU foreign policy chief. 2015. <http://www.telegraph.co.uk/news/worldnews/europe/eu/11597651/Migrant-crisis-is-a-security-crisis-says-EU-foreign-policy-chief.html> 9.05.2016* [↑](#footnote-ref-56)
57. *Официален вестник на Европейския съюз. Регламент (ЕО) № 2007/2004 на Съвета от 26 октомври 2004 година за създаване на Европейска агенция за управление на оперативното сътрудничество по външните граници на държавите-членки на Европейския съюз. 2004. <http://eur-lex.europa.eu/eli/reg/2004/2007/oj> 9.05.2016* [↑](#footnote-ref-57)
58. *Frontex Press Pack on the General Migratory Situation at the External Borders of the EU. 2015. <https://fullfact.org/wp-content/uploads/2015/09/general-press-pack-september-2015.pdf> 9.05.2016* [↑](#footnote-ref-58)
59. *Среща на върха по въпросите на миграцията, Ла Валета, 2015 г. – обща информация относно действията на ЕС. 2015. < http://www.consilium.europa.eu/bg/meetings/international-summit/2015/11/11-valletta-summit-press-pack/> 9.05.2016* [↑](#footnote-ref-59)
60. *За съставянето на фиг. 1 е използвана информация от Регламент (ЕО) № 2007/2004 на Съвета от 26 октомври 2004 година за създаване на Европейска агенция за управление на оперативното сътрудничество по външните граници на държавите-членки на Европейския съюз, както и от Frontex Structure. 2016. <http://frontex.europa.eu/about-frontex/organisation/structure/> 9.05.2016* [↑](#footnote-ref-60)
61. *Frontex Press Pack on the General Migratory Situation at the External Borders of the EU. 2015. <https://fullfact.org/wp-content/uploads/2015/09/general-press-pack-september-2015.pdf> 9.05.2016* [↑](#footnote-ref-61)
62. *Townsend, R. The European Migrant Crisis. Lulu Press, 2015. p.2.* [↑](#footnote-ref-62)
63. *Съкращението RABIT произлиза от първите букви на всяка от думите в разгърнатото наименование на екипите на английски език, съответно* ***RA****pid* ***B****order* ***I****ntervention* ***T****eam.* [↑](#footnote-ref-63)
64. *За съставянето на списъка с инициативи е използвана информация от Frontex Between Greece and Turkey: At the Border of Denial. 2014. <http://www.migreurop.org/IMG/pdf/rapport\_en\_web-3.pdf> 9.05.2016* [↑](#footnote-ref-64)
65. *Съвместна операция на полицейски кораб и агенция Фронтекс. Корабът „Обзор“ ще бъде изпратен в подкрепа на Гърция. 2016. <http://eurocom.bg/news/article/suvmestna-operaciia-na-policeiski-korab-i-agenciia-fronteks> 9.05.2016* [↑](#footnote-ref-65)
66. *Bulgarian Ship Participating in Frontex Mission Rescues 900 Migrants Near Lesbos. 2016. <http://www.novinite.com/articles/173179/Bulgarian+Ship+Participating+in+Frontex+Mission+Rescues+900+Migrants+Near+Lesbos> 9.05.2016* [↑](#footnote-ref-66)
67. *Български кораб спаси 900 мигранти край Лесбос. 2016. <http://dnes.dir.bg/news/obzor-bezhanskiat-natisk-frontex-lesbos-21757582> 9.05.2016* [↑](#footnote-ref-67)
68. *Български полицаи участваха в принудителното връщане на мигранти в Турция. 2016. <http://fakti.bg/world/180900-balgarski-policai-uchastvaha-v-prinuditelnoto-vrashtane-na-migranti-v-turcia> 9.05.2016* [↑](#footnote-ref-68)
69. *Number of Migrants Arriving in Greece Dropped in March. 2016. <http://frontex.europa.eu/news/number-of-migrants-arriving-in-greece-dropped-in-march-aInDt3> 9.05.2016* [↑](#footnote-ref-69)
70. *С решение на министрите на отбраната на НАТО от 11.02.2016 г. Втора постоянна морска група на Алианса (SNMG2) извършва разузнаване, мониторинг и наблюдение на маршрутите на нелегалните мигранти в Егейско море в подкрепа на гръцките и турските власти, както и на Frontex. В състава на групата под командването на контраадмирал Йорг Клайн влизат фрегатите Fredericton (Канада), Salamis (Гърция), Van Amstel (Нидерландия), Gokova (Турция), патрулен кораб Commandant Bouan (Франция), танкер Bonn (Германия) и спомагателен десантен кораб-док Mounts Bay (Великобритания).* [↑](#footnote-ref-70)
71. *Number of Migrants Arriving in Greece Dropped in March. 2016. <http://frontex.europa.eu/news/number-of-migrants-arriving-in-greece-dropped-in-march-aInDt3> 9.05.2016* [↑](#footnote-ref-71)
72. *Европейска комисия – Съобщение за медиите. Европейска гранична и брегова охрана за защита на външните граници на Европа. 2015. <http://europa.eu/rapid/press-release\_IP-15-6327\_bg.htm> 9.05.2016* [↑](#footnote-ref-72)
73. *Дигиталните иновации – приоритет №1 в ИТ инвестициите на държавната администрация, 26.1.2016.* [↑](#footnote-ref-73)
74. *Б. Божанов, Електронната идентификация е средство, чрез което изобщо да има електронно гласуване, 22.3.2016.* [↑](#footnote-ref-74)
75. [*http://eid.egov.bg/*](http://eid.egov.bg/)*, Електронна идентичност, Пилотен проект* [↑](#footnote-ref-75)
76. *М. Иванова. Личните карти ще са с чип и електронен подпис от 2018 г., 11.4.2016.* [↑](#footnote-ref-76)
77. *С. Хаджистойчев, Национална схема за електронна идентификация.* [↑](#footnote-ref-77)
78. *Б. Божанов: Електронната идентификация е средство, чрез което изобщо да има електронно гласуване* [↑](#footnote-ref-78)
79. *ICAO, Security Manual (Doc 8973) 7th edition, Volume I, стр. I-6. [online].*

    *https://www.scribd.com/doc/109423612/VOL-I-National-Organization-and-Administration* [↑](#footnote-ref-79)
80. *Пак там, стр. I-6* [↑](#footnote-ref-80)
81. *ICAO, Annex 17 9th edition, 2011, стр. 1-1. [online]. https://www.bazl.admin.ch* [↑](#footnote-ref-81)
82. *ICAO, Annual Report 2014, Appendix 1, Table 11 [online]. http://www.icao.int/annual-report- 2014*  [↑](#footnote-ref-82)
83. *ICAO, Results of the meeting on Aviation Security Management System (SeMS), AVSEC/FAL/RG/5- WP/08, 28/05/15. [online]. www.icao.int* [↑](#footnote-ref-83)
84. *ICAO,**Laying the Foundations for a more risk-based ICAO Annex 17-Security: Security Management System (Presented by IATA), DGCA-MID/1-IP/9, March 2011. [online]. www.icao.int* [↑](#footnote-ref-84)
85. *IATA, Security Management System (SEMS) for Air Transport Operators, 2011. [online]. www.iata.org* [↑](#footnote-ref-85)
86. *Department for Transport****,*** *Framework**for an Aviation Security Management System (SEMS), 2014. [online].* [*www.gov.uk*](http://www.gov.uk) [↑](#footnote-ref-86)
87. *Пак там, стр. 5* [↑](#footnote-ref-87)
88. *Пак там, стр. 6-26* [↑](#footnote-ref-88)
89. *ICAO,**Laying the Foundations for a more risk-based ICAO Annex 17-Security: Security Management System (Presented by IATA), DGCA-MID/1-IP/9, March 2011. [online]. www.icao.int* [↑](#footnote-ref-89)
90. *European Commission, Researh and Innovation, Europe's Vision for Aviation Flightpath 2050, Published on: 31/03/2011, стр. 17. [online]* [*http://ec.europa.eu/research/transport/publications*](http://ec.europa.eu/research/transport/publications) [↑](#footnote-ref-90)
91. *Георгиев В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015*  [↑](#footnote-ref-91)
92. *Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016* [↑](#footnote-ref-92)
93. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013* [↑](#footnote-ref-93)
94. *Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016* [↑](#footnote-ref-94)
95. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013* [↑](#footnote-ref-95)