

СТРАТЕГИЯТА НА ЕС ЗА СЪЮЗ НА СИГУРНОСТ (2020 – 2025 г.) И НОВИТЕ ПРЕДИЗВИКАТЕЛСТВА

Ирена Цонева Илиева, професор, доктор

*Институт за държавата и правото при Българската академия на науките
ел. поща: irena_ilieva@lawyer.bg*

THE EU SECURITY UNION STRATEGY (2020 – 2025) AND THE NEW CHALLENGES

Irena Tsoneva Ilieva, Professor, PhD

*Institute for the State and the Law by the Bulgarian academy of sciences, email:
irena_ilieva@lawyer.bg*

Abstract: *The EU Security Union Strategy (2020 – 2025) analyses the threats for the security of the European union at the moment of its elaboration and adoption: the problems of the cybersecurity, the hybrid attacks, the terrorism and radicalization, the organized crime and other. The Strategy does not foreseeing a war on the territory of Europe, the followed wave of displaced persons from Ukraine, as well the other resulting of this event threats for the security. The paper is focused on these news threats and challenges.*

Key words: *EU Security Union Strategy, common foreign and security policy, cybersecurity, terrorism, COVID-19 crisis, war in Ukraine, temporary protection.*

Увод

Сега действащата Стратегия ЕС за Съюз на сигурност (2020 - 2025 г.) е само малка част от soft law [1] в уредбата на Общата външна политика и политика на сигурност (ОВППС) на ЕС, силно трансформирана и широко уредена в ДЕС и ДФЕС от Лисабон. Тази политика е сред най-трудно създадените, наситена с най-много национални интереси и специфики, най-късно регламентирана и може би най-сложно еволюираща. Тя се намира в непрекъснато развитие и динамика, която не винаги е лесно предсказуема поради променящата се среда на сигурност.

Настоящият доклад няма за цел да представи еволюцията на правната уредба на ОВППС в първичното право на ЕС, а си поставя ограничената задача да представи правно необвързващия сега действащ компонент, а именно Стратегия ЕС за Съюз на сигурност (2020 - 2025 г.) и необходимостта от нейното преразглеждане в светлината на войната в Украйна и новите заплахи за сигурността на Съюза.

Концепцията за Европейски съюз на сигурност започва да се изгражда през 2015 г. въз основа на Европейския дневен ред за сигурност (European Agenda on Security). Този документ предлага нов подход, основан на споделена отговорност между ЕС и държавите членки. За ръководеното на този процес се създава портфолио на комисар по сигурността през септември 2016 г., подпомагат от работна група (task force), която концентрира експертизата на цялата Комисия.

Концепцията беше въведена през 2016 г. от Европейската комисия с документ, озаглавен „Paving a way towards an effective and genuine Security Union“ [2]. През 2019 г. това портфолио е възложено на еврокомисаря, отговарящ за европейския начин на живот – Маргаритис Схинас.

Европейският съюз за сигурност (European Security Union) има за цел:

- Да осигури, че политиката за сигурност на ЕС отразява промените заплахи на околната среда;
- Изгражда дългосрочна издръжливост;
- Ангажира европейските институции и агенции, правителствата, частния сектор и индивидите в всеобхватен обществен подход;
- Събира много политически области с пряко влияние върху сигурността.

Кратък исторически преглед

Стратегическите документи са важен компонент от системата за национална сигурност, а и от общата външна политика и политика на сигурност на ЕС. Европейският ред на сигурност е широко понятие, което отразява интересите и принципите на ЕС в световен мащаб и колективният смисъл за неговото осъществяване.

Измерението на сигурността се включва постепенно в европейското политическо сътрудничество (създадено в началото на 70-те години на миналия век), преминава през уредбата в ДЕС от Маастрихт, ДЕС от Амстердам, за да придобие съвременната си регламентация в ДЕС и ДФЕС от Лисабон. Сред основополагащите принципи и цели, уредени в чл. 21, ал. 2 ДЕС са посочени следните цели в областта на сигурността:

- а) опазване на своите ценности и основни интереси, на своята сигурност, независимост и цялост;
- в) опазване на мира, предотвратяване на конфликти и укрепване на международната сигурност, съгласно целите и принципите на Устава на Организацията на обединените нации, както и принципите на Заключителния акт от Хелзинки и целите на Парижката харта, включително тези, които се отнасят до външните граници.

Сега действащата уредба в първичното право на ЕС ясно откроява три части от външните действия на ЕС:

- Външна дейност;
- Обща външна политика и политика на сигурност
- Обща политика на сигурност и отбрана.

Съгласно чл. 24 ДЕС „Компетентността на Съюза в областта на външната политика и политиката на сигурност обхваща всички области на външната политика, както и всички въпроси на сигурността на Съюза, включително постепенното формиране на обща отбранителна политика, която може да прерасне в обща отбрана“ [3].

За Общата политика за сигурност и отбрана (ОПСО) е създаден специален раздел 2 на Глава 2 ДЕС „Специфични разпоредби относно общата външна политика и политика на сигурност“. Раздел 2 е озаглавен „Разпоредби, свързани с общата политика за сигурност и отбрана“.

В чл. 42 от ДЕС изрично се уточнява, че „Общата политика по сигурност и отбрана е неразделна част от общата външна политика и политика на сигурност“.

Текстът по-нататък доразвива предвидените инструменти: „Тя осигурява на Съюза оперативен капацитет, който почива на граждански и военни средства. Съюзът може да прибегне до тях при изпълнение на мисии извън територията на Съюза, с

цел да осигури поддържането на мира, предотвратяването на конфликти и укрепването на международната сигурност, в съответствие с принципите на УООН. Изпълнението на тези задачи се основава на капацитета, предоставен от държавите-членки”.

През м. юни 2016 г. беше приета Глобалната стратегия на външната политика и политика за сигурност ЕС (съкратено известна като Глобална стратегия на ЕС) [4]. Както сочи в предговора тогавашния Върховен представител по въпросите на общата външна политика и политика на сигурност Федерика Могерини „Стратегията подхранва амбицията за стратегическа автономия на ЕС. Това е необходимо за насърчаване на общите интереси на нашите граждани, както и за нашите принципи и ценности“ [5].

В нея се подчертава, че европейският проект е застрашен, европейският ред на сигурност е нарушен, защото тероризмът и насилието поразяват Северна Африка, Близкия Изток, както и самата Европа [6]. За справяне с тези нови предизвикателства е необходимо съчетаването на вътрешна и външна политики. Глобалната стратегия на ЕС цели да направи Съюза по-ефективен по отношение на енергийната сигурност, миграцията, измененията в климата, насилствен екстремизъм и хибридна война.

През октомври 2016 г. министрите на външните работи решиха кои най-важни стратегически приоритети да се осъществяват (Решения на Съвета от октомври 2016 г.). Те са сигурност и отбрана, изграждане на държавна и социална издръжливост, възприемане на интегриран подход към конфликти и кризи, засилване на регионалния ред за сътрудничество и основано на правила глобално управление. През м. ноември 2016 г. министрите на външните работи и министрите на отбраната решиха на ново амбициозно ниво ключовите стъпки за надграждане на сътрудничеството за осигуряване на сигурността на Съюза в съответствие с Глобалната стратегия. Те бяха основани върху представения от Върховния представител по въпросите на общата външна политика и политика на сигурност Федерика Могерини „План за осъществяване на сигурността и отбраната“. Той предвижда подобряване на защитата на ЕС и неговите граждани, да подпомогне правителствата съвместно да изградят военен капацитет и да се развие по-добър отговор на кризи. Следващите действия са определени в Европейския план за действие по отбрана (European Defense Action Plan), който предлага финансова помощ на държавите членки за по-ефективно съвместно снабдяване и развитие на способности, както и стъпки, съдържащи се в съвместната Декларация ЕС-НАТО.

Настоящата Стратегия ЕС за Съюз на сигурност (2020 - 2025 г.)

Сега действащата Стратегия ЕС за Съюз на сигурност (2020 - 2025 г.) е приета със Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите [7]. Тя замени Европейската стратегия за сигурност от 2003 г. Европейската комисия редовно представя доклади за извършения прогрес по осъществяване на Стратегията. Такива има за 2020 г., два доклада през 2021 г. и два доклада през 2022 г. [8]

Стратегията е един доста наративен документ, претендиращ за всеобхватност, но внимателният анализ показва, че той не е структуриран добре и не приоритизира заплахите за сигурността на ЕС. Той започва с Въведение, което акцентира върху необходимостта от съгласувани усилия между държавите членки и ЕС за гарантиране на сигурността на европейските граждани и разбирането, че от сигурността на една държава членка зависи сигурността на всички [9].

Следва анализ на бързо променящата се европейска картина на заплахите за сигурността. В него на първо място е направен анализ на киберсигурността на тех-

нологиите, на фона на заключението, че те са спомогнали много предприятия да продължат да работят по време на пандемията от КОВИД – 19. Констатира се възхода на „интернета на нещата“ и повишеното използване на изкуствения интелект [10], които благоприятстват вълна от киберпрестъпност. Дават се конкретни примери с фалшифицирани лекарства и експоненциалното нарастване на онлайн материали, съдържащи сексуално насилие над деца, кражби на интелектуална собственост, кибернетични кражби на търговски тайни и др. като по-сложни хибридни атаки.

На следващо място са поставени терористичните нападения в ЕС, заплахите от тероризъм подбуден и организиран от Даеш и Ал-Кайда. Подчертава се и нарастването на насилническия десен екстремизъм, включително антисемитски терористични нападения.

Следват заплахите от организирани престъпни групи: търговия с наркотици; трафика на хора; международна търговия с фалшифицирани фармацевтични продукти и използването на изкуствен интелект.

В този раздел прави впечатление, че никъде не се появява заплахата от въоръжен конфликт и война.

Следващият раздел е посветен на координираната реакция на равнище ЕС за цялото общество. Тя се основава на следните общи цели:

- Изграждане на способности и капацитет за ранно откриване, предотвратяване и бърза реакция при кризи;
- Поставя се акцент върху резултатите, нуждата от надеждно стратегическо разузнаване и подходящо финансиране;
- Приобщаване на всички участници в публичния и частния сектор за полагането на общи усилия.

Раздел 4 съдържа стратегическите приоритети на Съюза на сигурност.

Първият е защитата на критичната инфраструктура. Подчертава се, че Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза [11] и Директива 2008/114/ЕО на Съвета относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита [12] не са в синхрон с променящите се рискове. Държавите членки са упражнили правото си на преценка и са транспонирали това законодателство по различни начини, което увеличава уязвимостта, включително на финансовия сектор, енергийните системи, транспорта, здравеопазването и космическото пространство.

Следващият параграф е посветен на киберсигурността. Увеличеният брой кибератаки засягат основни доставчици на услуги в „облак“, финансовата система, лични данни и др. Освен преразглеждане на Европейската стратегия за киберсигурност, се подчертава необходимостта от разработване на култура на киберсигурност още при проектирането, в която сигурността е вградена в продуктите и услугите от самото начало. Отбелязва се значението на сътрудничеството между Агенцията на ЕС за киберсигурността (ENISA) и органите за защита на данните и Европейския комитет по защита на данните. Предвижда се нова уредба относно сигурността на информацията и киберсигурността за всички институции, органи и агенции на ЕС.

Следващ акцент е защитата на обществените пространства от тероризъм. Както е известно, критична инфраструктура, транспортни центрове, други обществени места, включително за богослужение са „любимо“ място за терористични атаки. Във връзка с това е отделено внимание на пазара на дронове, които имат потенциал да бъдат неправомерно използвани от престъпници и терористи.

В Параграфа, посветен на справянето с променящите за заплахи на първо място е разгледана киберпрестъпността: зловредни атаки, кражби на лични или търговски данни чрез хакерски атаки, прекъсване на цифрови дейности и др. Основният правен инструмент е Директива 2013/40/ЕС относно атаките срещу информационните системи.

Голяма част от този раздел е посветена на съвременното правоприлагане. Правоприлагащите органи и практикуващите юристи трябва да се приспособят към технологичното развитие и да използват нови инструменти: цифрови разследвания, изкуствен интелект, използване на големи информационни масиви, идентифициране на терористично съдържание онлайн; достъп до цифрови доказателства; инфраструктура за мобилни далекосъобщения; работа с криптирана информация.

Особено деликатна и трудна е борбата с незаконното съдържание онлайн. За нея се изисква засилване на доброволното сътрудничество между правоприлагащите органи и частния сектор. Засега са налице актове от типа на soft law, като например Кодекса на поведение във връзка с незаконните изказвания онлайн, пораждащи омраза (2016 г.). Той съдържа доброволен ангажимент от страна на онлайн платформите да премахват съдържание, включващо език на омразата. В този параграф е поставена и борбата срещу сексуалното насилие над деца.

Следващата проблематика е свързана с хибридните атаки. Всъщност Стратегията съдържа доста широко определение за хибридни атаки като обхващащи комбинацията от насилнически и подривни дейности, конвенционални и неконвенционални методи (т.е. дипломатически, военни, икономически, технологични), които се използват по координиран начин от държавни или недържавни субекти с цел постигане на конкретни цели (в отсъствие на официално обявена война). Тук се подчертава, че отговорността за борбата с хибридните атаки се носи основно от държавите членки, но някои уязвими точки са общи като трансгранични мрежи или инфраструктура. Борбата с тях е комплексна и изисква използване на резултатите от концептуализацията на хибридните заплахи, основаване на взетите решения върху изчерпателни разузнавателни данни и засилване на сътрудничеството в областта на разузнаването.

Следващият параграф е посветен на защитата на европейските граждани от тероризъм и организирана престъпност. Сочи се, че борбата с тероризма започва със справяне с причините, ред които и радикализацията. Тук е подчертана ролята на т. нар. „меки политики“ в областта на образованието, културата, младежта и спорта, които биха могли да предотвратят радикализацията.

Друга опасност е придобиването и използването от терористи на химически, биологични, радиологични и ядрени оръжия, както и необходимите знания и капацитет да ги използват. Подчертава се необходимостта от укрепване на капацитета на механизма на ЕС за гражданска защита (rescEU).

Заплахата от взривни устройства, изработени в домашни условия е висока и те се използват а множество атаки в рамките на Съюза, въпреки налично законодателство (Регламент (ЕС) 2019/1148 за предлагането на пазара и употребата на прекурсори на взривни вещества).

Голяма част от този раздел е посветена на борбата с чуждестранните бойци терористи [13]. В действителност международноправната уредба на тази борба е създадена под егидата на Съвета на Европа, докато ЕС акцентира върху базите данни за обмен на информация относно заподозрени лица и сигурността на външните граници. Като добра практика е посочен Съвместния план за действие в областта на борбата с тероризма за Западните Балкани. Подчертава се необходимостта от сътрудничество с водещи международни организации като ООН, НАТО, Съвета на Европа, ОССЕ, Интерпол.

В раздела за борбата с организираната престъпност логично поради актуалността си на първо място е отделено внимание на кражбите и грабежите на здравни и санитарни продукти, свързани с пандемията от КОВИД-19. След това е поставено борбата с трафика на наркотици, търговията с незаконни огнестрелни оръжия, незаконната миграция, трафика на хора, престъпленията против околната среда [14], трафика на културни ценности, икономически и финансови престъпления, изпирането на пари. Направена е връзка между организираната престъпност и корупцията.

В параграф 4, озаглавен „Силна европейска екосистема за сигурността“ се прави важна връзка между сигурността и борбата с домашното насилие. Тази изключително наболяла проблематика в нашата страна и в дискусиите по законодателните промени подминаха темата за сигурността.

Особено важно е сътрудничеството и обмена на информация. То включва много аспекти. Сред тях на първо място Стратегията е поставила оперативното сътрудничество между държавите членки в областта на правоприлагането. Един от основните инструменти е Шенгенската информационна система (ШИС) за обмен на данни относно издирвани и изчезнали лица и вещи в реално време. Оперативното сътрудничество в областта на правоприлагането е създадено преди повече от 30 години и представлява сложна мрежа от двустранни споразумения между държавите членки, които или са остарели, или не се прилагат. Отбелязва се, че оперативното сътрудничество чрез използване на нови технологии не се обхваща от действащото право на ЕС. Основна роля в него играе Европол, но той е изправен пред редица ограничения, най-вече във връзка с прекия обмен на лични данни с частноправни субекти. Посочена е ролята на Евроюст и на ЕМРАСТ (Европейска мултидисциплинарна платформа за борба с криминални заплахи).

Отбелязва се, че информацията за пътниците е спомогнала за подобряване на граничния контрол, намаляването на незаконната миграция и идентифицирането на лица, представляващи риск за сигурността. Все пак, трябва да отбележим времето, в което е приета Стратегията, а именно периода на затваряне на границите и изолацията по време на пандемията от КОВИД-19. Отчитането на такива „успехи“ се дължи най-вече на обективни обстоятелства и борбата с пандемията, а не толкова на ефикасността на правната уредба. Към онзи момент се отчита положителен ефект от действието на Директива (ЕС) 2016/681 относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления (т. нар. PNR данни). Към момента на приемането на Стратегията се подчертава необходимостта от осигуряване на средства за работата на Европейската прокуратура и Евроюст, както и от създаване на нова цифрова система за обмен, чрез която да се предават европейски заповеди за разследване, искания за правно помощ и свързани съобщения между държавите членки.

Пандемията постави на дневен ред и въпроса да се проучат възможностите за създаване на механизъм на равнище ЕС за координация на полицейските сили в случай на форсмажорни обстоятелства като пандемии.

Въпросът за сигурността на външните граници е също част от този раздел. Тук влизат дейността на Европейската агенция за гранична и брегова охрана (FRONTEX) [15], митническите дейности за откриване на рискове за безопасността и сигурността на всички стоки, преди да достигнат в ЕС, системата за влизане и излизане (СВИ), системата за информация за пътуванията и разрешаването им (ETIAS) и др.

Системата за влизане/излизане (СВИ) се създава като част от Стратегията на Съюза за интегрирано управление на границите. Тя трябва да регистрира по елек-

тронен път времето и мястото на влизане и излизане на гражданите на трети страни, допуснати за краткосрочен престой на територията на държавите членки, и да изчислява продължителността на техния разрешен престой. Тя следва да замени задължението за подпечатване на паспортите на граждани на трети страни, което се прилага за всички държави членки. Тя също ще се прилага за гражданите на трети страни, на които е отказано влизане за краткосрочен престой.

Въвеждането в действие на СВИ беше доста забавено. Въвеждането в действие първоначално беше предвидено за 2022 г., след това за м. май 2023 г. и отново отложено до края на 2023 г. Очаква се да започне да функционира през 2024 г., най-вероятно след провеждане на Олимпийските игри в Париж. Забавянето засегна и функционирането на друга важна система – European Travel Information and Authorisation System (ETIAS) [16].

Особено внимание в Стратегията е отделено на засилването на научните изследвания и иновациите в областта на сигурността. Борбата с киберпрестъпленията, организираната престъпност, тероризма в голяма степен зависи от научните изследвания и използването на новите технологии. Иновациите се разглеждат в документа като стратегически инструмент за противодействие на тези заплахи и предвиждане на бъдещи рискове. Освен това, научните изследвания, иновациите и технологичното развитие в ЕС дават възможност аспектът „сигурност“ да се вземе предвид още при тяхното разработване. Документът дава пример с Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежата от национални координационни центрове, които да обединят капацитета и резултатите от научните изследвания в областта на киберсигурността. В Стратегията се обмисля и възможността да се създаде Европейски център за иновации в областта на вътрешната сигурност.

Последната част от Стратегията е посветена на повишаване на уменията и осведомеността за справяне със заплахите за сигурността. Това са инициативи за цифрово образование, допълнителни действия по програмата „Цифрова Европа“, необходимата помощ и достъп на жертвите до техните права, повишаване на уменията на правоприлагащите органи. Ключова роля тук има CEPOL – Агенцията на ЕС за обучение в областта на правоприлагането

Какво липсва в Стратегията ?

Липсва най-старата, традиционна и съпътствала човечеството през цялата му история заплаха: войната.

Следователно липсва и анализ на последиците от война в Европа: вълна от разселени лица, увеличена заплаха от трафик на хора; тежката проблематика на непридружени непълнолетни, икономическите последици за системите на снабдяване с храни и други ресурси; заплахата за националните системи за сигурност, социални, здравни, образователни и други услуги.

Липсва анализ на връзката между драстичните нарушения на международното хуманитарно право и националната и сигурността на ЕС.

Липсва връзката със закрилата на основните права на човека.

Липсва анализ на прилагането на Директивата за временна закрила във връзка със заплахата за националната сигурност. От нея са изключени изрично заподозрени за извършване на:

- Престъпления против мира,
- Военни престъпления,

- Престъпления против човечеството,
- Тежки не-политически престъпления;
- Действия против целите и принципите на Обединените нации
- Заплаха за сигурността на приемащата държава членка [17].

Заклучение

Познаването на Стратегия ЕС за Съюз на сигурност (2020 - 2025 г.) е важно от гледна точка на преразглеждането на актуализираната Стратегия за национална сигурност на Република България (приета с решение на НС от 14.03.2018 г.) [18]. Тя е за периода до 2025 г., но също има необходимост от преразглеждане във връзка с новата геополитическа реалност и най-вече агресията на Руската федерация и войната в Украйна.

За съжаление анализът на Стратегията на ЕС за сигурност не ни дава надежден модел за предефиниране на нашата Стратегия за национална сигурност. Тя, по мое мнение, не може да ни послужи нито като медал за структуриране, нито като добра практика за изпълнение.

В настоящата Стратегия липсва заплаха от конвенционална война и анализ на последиците от нея. Войната в Украйна предизвиква редица реални нови проблеми основният сред тях е решаването на проблема с разселените лица, които са основно жени и деца и прилагането на Директивата за временна закрила. Агенцията за основните права в ЕС изследва широкомащабно и въз основа на достоверни данни този проблем [19].

Остава трайна тенденцията за нарастване на кибератаките, увеличи се риска от трафик на хора, особено тежко е положението на украинските деца [19]. Реални и непосредствени са заплахата от химически и ядрени инциденти; заплахата от екологични инциденти (такъв вече се случи с взривяването на стената на язовир Каховка); незаконния трафик на оръжия; саботажа на газопровода Северен поток; заплахи за дигиталната инфраструктура, транспорта, космическото пространство, морската критична инфраструктура.

Всички посочени в изложението предизвикателства и липси в настоящата Стратегия на ЕС за Съюз на сигурност налагат спешното ѝ преразглеждане, както и актуализирането на Стратегията за национална сигурност на Република България.

Литература:

1. Илиева, Ирена, Soft law на международните организации. Soft law и съвременното право, Сиби, 2017.
2. Communication from the Commission to the European Parliament, the European Council and the Council delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM(2016) 230 final, Brussels, 20.04.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0230>, последно посетен на 13.09.2023 г.
3. Договори за ЕС. Съдебна практика, Сиби, С., 2009.
4. Достъпна на eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf, последно посетен на 25.08.2023 г.
5. Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign and Security Policy.
6. Пак там, с. 1

7. COM (2020) 605 final, Брюксел, 24.07.2020 г. достъпна на <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX%3A52020DC0605>, последно посетен на 25.08.2023 г.
8. Всички са достъпни на https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en, последно посетен на 25.08.2023 г.
9. COM (2020) 605 final, Брюксел, 24.07.2020 г., с. 1.
10. Относно понятието за изкуствен интелект и проекта на регламент за неговото регулиране вж. по-подр. Илиева, Ирена. Върховенството на правото и изкуственият интелект, сп. „Известия“, Икономически университет Варна, том 64, № 3/2020, с. 210 – 226 и Защитата от дискриминация и изкуственият интелект, в Сборник с доклади от Международна научна конференция „Изкуственият интелект в сферата на сигурността – предимства и заплахи“, 30 септември 2022 г., Висше училище по сигурност и икономика Пловдив, Пловдив, 2022, с. 8 - 16.
11. Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, ОВ L 194, 19.07.2016 г.
12. Директива 2008/114/ЕО на Съвета относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита, ОВ L 345, 23.12.2008 г.
13. Относно определението за „чуждестранни бойци терористи“ вж. по-подр. Илиева, Ирена. Допълнителният протокол към Конвенцията на Съвета на Европа за предотвратяване на тероризма и борбата срещу чуждестранните бойци терористи, в Сборник в чест на 70-годишнината на проф. д-р Емил Константинов, БАН-ИДП, С., 2018, с. 60 – 77.
14. Такива са например незаконен лов и търговия с екземпляри от дивата флора и фауна, незаконна минна дейност, дърводобив, незаконно депониране и превози на отпадъци, престъпно използване на схемите за търговия с емисии, злоупотреба с финансиране, предназначено за екологична устойчивост и др.
15. Относно създаването на агенцията вж. по. подр. Илиева, Ирена. Международно-правна уредба, регламентация в правото на ЕС и в националното законодателство, в Глава шеста от книга: Владимирова, К. и кол. (2019). Миграция и национална идентичност. В: ИИНЧ-БАН. Мерки за преодоляване на демографската криза в Република България, т. 3, С., Издателство на БАН „Проф. М. Дринов“, с. 414 – 415.
16. <https://www.schengenvisainfo.com/news/eu-confirms-it-doesnt-have-a-date-for-implementation-of-entry-exit-system-yet/>, последно посетен на 29.07.2023 г.
17. Council directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0055>, последно посетен на 21.11.2022
18. Достъпна на: <https://www.me.government.bg/files/useruploads/files/akt.strategiq.2020.pdf>, последно посетен на 14.09.2023 г.
19. Fundamental Rights Report 2023 <https://fra.europa.eu/en/publication/2023/fundamental-rights-report-2023>, последно посетен на 16.11.2023 г.
20. The Russian aggression against Ukraine - Displaced children finding protection in the EU - Bulletin 3, <https://fra.europa.eu/en/publication/2023/ukraine-bulletin-3-2023>, последно посетен на 16.11.2023 г.