ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 30.9.2010
SEC(2010) 1127

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

Придружителен документ към

предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно Европейската агенция за мрежова и информационна сигурност (ENISA)

{COM(2010) 521 окончателен}
{SEC(2010) 1126}

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

1. ОБХВАТ И КОНТЕКСТ

1.1. Обхват

Настоящата оценка на въздействието се фокусира върху това как следва да бъде изградена една модернизирана агенция за мрежова и информационна сигурност (МИС), широко призната като подходящ и необходим политически инструмент за справяне с предизвикателства в сферата на МИС, така че да подкрепи органите на държавите-членки и на Комисията за постигане на целите на политиката в сферата на МИС след изтичането на мандата на Европейската агенция за мрежова и информационна сигурност (ENISA) през март 2012 г.

1.2. Контекст

В съвременния свят обществото и икономиката са силно зависими от правилното функциониране на информационните и комуникационни технологии (ИКТ). Поради това е от първостепенно значение да се гарантира както стабилността на системите, така и доверието на потребителите в тях. Нарастващият брой заплахи, атаки и зловреден софтуер, използвани срещу системите, би могъл да изложи на риск правилното функциониране на основната мрежова и информационна инфраструктура. Предвид транснационалния характер на тези системи и мрежи съществува необходимост от европейски отговор на предизвикателствата в сферата на мрежовата и информационна сигурност (МИС).

За справяне с тези проблеми през 2004 г.[1] беше създадена Европейската агенция за мрежова и информационна сигурност (ENISA) за срок от пет години с цел *„гарантиране на високо и ефективно ниво на мрежова и информационна сигурност в рамките на Общността, (...) и с цел развитие на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и организациите от обществения сектор на Европейския съюз, с което да се допринесе за безпрепятственото функциониране на вътрешния пазар“*.

Впоследствие предизвикателствата в сферата на МИС бележат постоянни промени в съответствие с технологичното и пазарно развитие. Поради това доста преди изтичането на срока на действие на регламента относно ENISA през март 2009 г. Комисията постави началото на процес за определяне, заедно със съответните заинтересовани страни, на предложения за политика, които най-добре биха отговорили на целите на ЕС в сферата на МИС през периода след 2009 г. След направена през 2007 година средносрочна оценка[2] на ENISA и обществено допитване[3], на 24 септември 2008 г. Съветът и Европейският парламент приеха регламент, с който установеният

---

1 Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейска агенция за мрежова и информационна сигурност.

2 Съобщение от Комисията до Европейския парламент и Съвета относно оценката на Европейската агенция за мрежова и информационна сигурност (ENISA), COM(2007)285 окончателен, 1.6.2007 г.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

3 Допитването е проведено от 13 юни до 7 септември 2007 г.

мандат на ENISA се удължава с три години в срок до 13 март 2012 г.[4] В съображенията към този регламент Съветът и Европейският парламент призоваха за ***„по-нататъшно обсъждане на въпросите във връзка с Агенцията [и] общата насока на европейските усилия за все по-голяма мрежова и информационна сигурност***“.

Комисията подпомогна обсъждането, като започна допълнително обществено допитване на ниво ЕС през ноември 2008 г. относно възможните цели на политика за повишаване на МИС и средствата за постигането на тези цели[5]. През декември 2008 г. Комисията също така проведе семинар с експерти в сферата на МИС от компетентните органи на държавите-членки относно инструментите и механизмите за политика на ЕС за повишаване на МИС. В допълнение към това, през март 2009 г. Комисията прие Съобщение относно защитата на критичната информационна инфраструктура (CIIP)[6], в което се определя ключовата роля на ENISA в подкрепа на ЕС за подобряване на сигурността, устойчивостта и подготвеността. Този подход беше одобрен от конференцията на министрите относно CIIP, проведена в Талин на 27 и 28 април 2009 г., едно от заключенията на която беше, че ***„предстоящите нови и трайни предизвикателства изискват цялостно преосмисляне и преформулиране на мандата на Агенцията с цел по-добро фокусиране върху приоритетите и нуждите на ЕС;*** *придобиване на способност за по-гъвкаво реагиране; развиване на европейски умения и компетенции; и за повишаване на оперативната ефективност и цялостното въздействие от страна на Агенцията. По този начин ENISA може да се превърне в постоянен актив на всяка държава-членка и на Европейския съюз като цяло“*.

На 18 декември 2009 г. Съветът прие резолюция относно *„относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност“*[7], в която се подчертава, че ***„съгласно един преработен мандат ENISA следва да бъде център на ЕС за експертен опит по въпроси, свързани с мрежовата и информационната сигурност в ЕС“.***

Една от водещите инициативи за осъществяването на стратегията „Европа — 2020“ на Комисията за интелигентен, устойчив и приобщаващ растеж[8] е Програмата в областта на цифровите технологии за Европа, в която МИС играе централна роля. **Целта на тази политическа инициатива за доверие в Програмата в областта на цифровите технологии за Европа е да позволи на ЕС, държавите-членки и заинтересованите страни да развият висока степен на способност и подготвеност за предотвратяване, установяване и по-добро реагиране на проблеми в сферата на МИС.** Това ще допринесе за повишаване на доверието и сигурността в рамките на единния европейски цифров пазар и ще подобри конкурентоспособността на европейските предприятия.

---

4 Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета от 24 септември 2008 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейска агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията, ОВ L 293, 31.10.2008 г.

5 От 7 ноември 2008 г. до 9 януари 2009 г., докладът е публикуван на http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно защитата на критичната информационна инфраструктура, COM (2009)149 окончателен, 30.3.2009 г.

7 Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност (2009/C 321/01).

8 COM(2010)2020.

2. ОПРЕДЕЛЯНЕ НА ПРОБЛЕМА

2.1. В какво се състои проблемът?

Установени са следните фактори за възникване на проблеми, които поставят заинтересованите страни в уязвимо положение откъм заплахи в сферата на МИС и свързани с инциденти в сферата на МИС. Всички те свидетелстват за наличието на нужда от надеждна структура на ниво ЕС за справяне с проблема и за привеждане в съответствие, в рамките на цяла Европа, с постоянно променящите се технологии и пазарни условия в областта на МИС.

- **Разнообразие и фрагментация на националните подходи.** Проблемите в сферата на МИС надхвърлят националните граници и поради това не могат да бъдат разрешавани по ефективен начин единствено на национално ниво. Същевременно държавните органи в отделните държави-членки се справят с проблема по доста различни начини. Многобройните изисквания по отношение на сигурността в отделните държави-членки налагат разходна тежест за предприятията, които осъществяват дейност в рамките на ЕС, което води до фрагментация и липса на конкурентоспособност на европейския вътрешен пазар.

- **Ограничена способност на Европа за ранно предупреждаване и реагиране.** Настоящите национални системи за ранно предупреждаване и действия при инциденти се различават значително в отделните държави-членки, като същевременно не съществува подобна система на ниво ЕС. Налице е необходимост от инструменти на политиката на ЕС за установяване на рискове и уязвими аспекти на МИС, за създаване на подходящи механизми за реагиране и за гарантиране, че заинтересованите страни познават и прилагат тези механизми за реагиране.

- **Липса на надеждни данни и ограничени познания за възникващи проблеми.** Налице е твърде оскъдна надеждна количествена информация за въздействието и дори за възникването на инциденти във връзка с МИС, което затруднява политиците при приемането на подходящи политически мерки, както и предприятията при вземането на решения за инвестиции в сигурността.

- **Липса на осведоменост за рисковете и предизвикателствата в сферата на МИС.** Отговорността за обезпечаване на МИС е на отделните заинтересовани страни; въпреки това техните отговорности невинаги са ясно определени и оповестени. От една страна, потребителите често подценяват рисковете в сферата МИС и пренебрегват своята лична отговорност за сигурността на своите системи за ИКТ. От друга страна, предприятията често се интересуват най-вече от разходите за МИС, а не от произтичащите от нея възможни икономии.

- **Международното измерение на проблемите в сферата на мрежовата и информационна сигурност.** Заплахите за МИС и евентуалните последващи инциденти са международни по своя характер, поради което действията на ЕС могат да не са толкова ефикасни, ако проблемите в сферата на МИС не бъдат разглеждани по подходящ начин на международно ниво. Нуждаем се от разработване на стратегия на ЕС и референтен център за МИС, които да изведат ЕС на по-добри международни позиции.

- **Необходимостта от модели на сътрудничество с цел гарантиране на адекватно изпълнение на политиката.** Адекватното изпълнение на политиките в сферата на МИС изисква модели за сътрудничество на ниво ЕС. Заинтересованите лица се нуждаят от насоки при определяне на заплахите за МИС и от разработване на добри практики за изпълнение на съществуващите политики в сферата на МИС.

- **Необходимостта от по-ефективни действия срещу престъпления в кибернетичното пространство.** Усилията в сферата на МИС са организирани предимно в условията на предишния първи стълб, т.е. въпроси, обсъждани между институциите. С влизането в сила на Лисабонския договор обаче е необходимо да се вземе под внимание един по-широк пакет от задачи на Агенцията за МИС, който да обхваща и области от „втория и третия стълб“, т.е. въпроси, които преди бяха решавани единствено от Съвета.

2.2. Кой е най-засегнат от проблема?

Инцидентите, свързани с МИС, биха могли да окажат огромно въздействие върху различни заинтересовани лица, включително големите и малките предприятия, държавни органи и администрации и отделни граждани. Иначе казано, МИС е грижа и отговорност на всеки.

Налице е малко или почти никаква обективна количествена информация за точния брой на инцидентите в сферата на МИС и/или за съответното им икономическо въздействие. Един от показателите в тази насока се съдържа в пазарно проучване на IDC EMEA[9], според което през последните 12 месеца 28% от домакинствата от ЕС-27 са имали проблеми със спам или вируси. През последната година средно около 7% от предприятията потребители са се сблъскали с инциденти във връзка със сигурността.

3. ОБОСНОВКА НА ДЕЙСТВИЯТА НА ЕС, ДОБАВЕНАТА СТОЙНОСТ НА ЕС И СУБСИДИАРНОСТТА

Взаимозависимостта на мрежовите и информационни системи силно затруднява и дори прави невъзможно за отделните участници да преценяват правилно глобалното икономическо и социално въздействие на техните мерки за защита срещу свързани с МИС инциденти. Различните национални политики и практики водят до нестабилност на вътрешния пазар както поради отрицателните външни последици от свързаните с МИС инциденти (неадекватни политики засягат други държави-членки), така и поради положителните външни последици от добрите практики в сферата на МИС (добрите практики в дадена държава-членка подобряват МИС като цяло, като по този начин носят безспорна социална полза). Поради това политическата намеса на ЕС е оправдана, тъй като би осигурила реална добавена стойност за функционирането на вътрешния пазар. Подобна добавена стойност е призната и в Регламент (ЕО) № 460/2004 относно създаването на ENISA, съгласно който компетенциите на ENISA имат за цел да допринесат за безпрепятственото функциониране на вътрешния пазар.

---

[9] IDC EMEA, Европейски пазар за мрежова и информационна сигурност — сценарий, тенденции и предизвикателства, април 2009 г., с препратки към проучването на Евробарометър за електронните съобщения, април 2007 г.

Освен това намесата на ЕС в политиката в сферата на МИС е оправдана от *принципа за субсидиарност*. Както е посочено в Съобщението за CIIP, една стратегия на ЕС за пълна ненамеса в националните политики в сферата на МИС би била почти равностойна на изискването всяка държава-членка да се грижи единствено за себе си, независимо от взаимозависимостта на информационните системи. Поради това подходяща степен на координация между държавите-членки с цел да осигуряване на добро управление на трансграничните последствия от рискове във връзка с МИС е в съответствие с принципа за субсидиарност. Освен това действията на ЕС биха подобрили ефективността на всички съществуващи национални политики.

Гражданите на ЕС все повече поверяват своите данни на сложни информационни системи (например „изчислителен облак“). Поради това съгласуваните и съвместни политически действия в сферата на МИС могат да окажат силно благоприятно влияние върху ефективната *защита на основни права*, и по-специално правото *на защита на личните данни и неприкосновеността на личния живот*. Поради същата причина допълнителните политически действия от страна на ЕС изглеждат напълно оправдани.

4. ЦЕЛИ НА ПОЛИТИКАТА

В настоящата оценка на въздействието се изследва степента, до която една модернизирана агенция за МИС, широко призната като най-подходящата организационна структура, може да бъде структурирана по най-добър начин, за да допринесе, заедно с други инструменти на ЕС, за постигането на целите на политиката.

Общата цел е да се даде възможност на ЕС, на държавите-членки и заинтересованите страни да развият висока степен на способност и подготвеност за предотвратяване, установяване и по-добро реагиране на проблеми в сферата на МИС. Това ще допринесе за повишаване на доверието в европейския единен цифров пазар и ще подобри конкурентоспособността на европейските предприятия.

Тази цел е разделена на седем **специфични цели**:

(1) **съгласуваност на регулаторните подходи** — предоставяне на насоки и консултации за Комисията и на държавите-членки относно актуализирането и разработването на цялостна нормативна рамка в сферата на МИС;

(2) **предотвратяване, установяване и реагиране** — подобряване на подготвеността чрез подпомагане на европейската способност за ранно предупреждаване и реагиране на инциденти, както и на паневропейски планове и учения за действие при извънредни ситуации;

(3) **подкрепа за разработване на политики** — предоставяне на помощ и консултации за Комисията и държавите-членки;

(4) **упълномощаване на заинтересованите страни** — създаване на култура на управление на сигурността и риска чрез насърчаване на споделянето на информация и широко сътрудничество между участниците от публичния и частния сектор, също и в пряка полза на гражданите и малките и средни предприятия, както и чрез изграждане на култура на осведоменост във връзка с МИС;

(5) **превръщане на Европа в реален фактор в международен контекст** — постигане на високо ниво на сътрудничество с трети държави и международни

организации за насърчаване на общ глобален подход към въпросите на МИС и придаване на тежест на международни инициативи на високо ниво в Европа;

(6) **съвместно изпълнение** — улесняване на сътрудничеството при изпълнението на политиките относно МИС;

(7) **борба срещу престъпленията в кибернетичното пространство** — развиване на способност за ефективно реагиране на свързаните с МИС аспекти на престъпленията в кибернетичното пространство чрез сътрудничество с органи от (предишния) втори и трети стълб, например с Европол.

5. ВЪЗМОЖНИ ОРГАНИЗАЦИОННИ ФОРМАТИ И ВАРИАНТИ НА ПОЛИТИКА

В оценката на въздействието (глава 4 и приложение 4) са изследвани няколко възможни организационни формати за изпълнение на горепосочените варианти на политика, включително i) агенция, ii) до една или друга степен формализирано публично-частно партньорство (ПЧП), iii) неформална мрежа за контакти, iv) постоянна мрежа от компетентни органи и v) пряко включване в дадена служба на Комисията.

При сравняване на тези различни организационни формати този на агенция изглежда най-подходящ избор за инструмент за политика поради неговите предимства по отношение на: 1) правната сигурност на организационната структура, както и по същество, 2) неговата пригодност за специфичните проблеми на един толкова чувствителен сектор като МИС (орган за външни експертни становища, координиране на отношенията със заинтересованите страни, включване/ангажираност на държавите-членки) и 3) приемането и репутацията на ENISA в общността на МИС.

Поради това бяха разработени и подробно оценени следните варианти на политика за организационния формат на агенция.

Вариант на политика 1: Липса на политика

При варианта „Липса на политика“ се предполага, че ENISA ще преустанови съществуването си след март 2012 г. и че никоя друга институция на ЕС няма да поеме изцяло или отчасти текущите дейности на ENISA.

Закриването на ENISA би означавало всички осъществени досега инвестиции, например за изграждане на организация, способна да привлича висококвалифицирани специалисти, за натрупване на експертен опит и за създаване на мрежи със и между заинтересовани лица и с международни институции, да бъдат оттеглени в момент, когато съществуващата агенция е набрала пълна скорост.

Комплексният характер на проблема във връзка с МИС в цяла Европа изисква модернизирана и стабилна агенция, а не закриването на сегашната. Това се потвърждава от ясно определената роля, предоставена на ENISA, например в реформираната регулаторна рамка за електронните съобщения[10], и изразената от заинтересованите страни обща подкрепа за придаване на по-голямо значение на ролята на една европейска агенция за МИС.

[10] Вж. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML

Вариант на политика 2: Продължаване без изменения

Вариант 2 представлява сценарий за „обичайната работа“, т.е. продължаване на същия инструмент на политика в същата форма и със същите ресурси. Сред заинтересованите страни съществува общ консенсус, че ENISA се е утвърдила като референтен център по въпросите на МИС и се е превърнала в център за високи постижения в своята област.

Предвид настоящите ограничения по отношение на персонала и бюджета Агенцията ще оказва влияние само върху силно ограничен кръг от проблеми, свързани с МИС. Това обаче е в противоречие с цялостните очаквания на заинтересованите страни. Лишаването на Агенцията от възможността да се развива допълнително и да оправдае тези все по-високи очаквания в крайна сметка може да доведе до криза на доверие.

Вариант на политика 3: Разширяване на понастоящем определените функции на ENISA и добавяне на агенциите за правоприлагане и защита на неприкосновеността на личния живот като пълноправни заинтересовани страни

Съгласно този вариант ролята на една агенция за МИС ще се разшири, като се фокусира върху:

- изграждане и поддържане на мрежа за връзка между заинтересованите страни и мрежа за познания;
- превръщане на Агенцията в център за подпомагане на МИС чрез разработване и прилагане на политики (по-специално по отношение на правото на неприкосновеност на личния живот и електронните съобщения, електронния подпис, електронната идентификация и стандартите за обществени поръчки във връзка с МИС);
- подкрепа на политиката на ЕС по отношение на CIIP и политиката за устойчивост (например учения, EP3R[11], Европейска система за информационен обмен и предупреждаване и др.);
- създаване на рамка на ЕС за събирането на данни във връзка с МИС, включително разработване на методи и практики за изисквани от закона задължения за докладване и споделяне на данни;
- изследвания и изготвяне на доклади относно икономиката на МИС;
- стимулиране на сътрудничеството с трети държави и международни организации с цел насърчаване на общ глобален подход към въпросите на МИС и придаване на тежест на международни инициативи на високо ниво в Европа);
- осъществяване на задачи с неоперативен характер, свързани с аспекти на МИС, в областта на правоприлагането и съдебното сътрудничество.

Агенцията ще разполага с всички необходими ресурси за изпълнение на своите дейности по задоволителен и задълбочен начин, т.е. за оказване на реално влияние. При наличие на повече ресурси ENISA би могла да играе много по-активна роля и да предприема повече инициативи за стимулиране на активното участие на заинтересованите страни. Освен това тази нова ситуация би позволила по-голяма гъвкавост за бързо реагиране на промените в постоянно развиваща се среда на МИС.

[11] Европейско публично-частно партньорство за устойчивост, вж. COM(2009)149.

Вариант на политика 4: Добавяне на оперативни функции при борбата срещу атаки в кибернетичното пространство и реагирането на инциденти в кибернетичното пространство

В допълнение към посочените във вариант 3 дейности Агенцията ще поеме оперативни функции, като играе по-активна роля във връзка с CIIP на ЕС, например при предотвратяване и реагиране на инциденти, по-специално функционирайки като екип на ЕС за действие при инциденти в информационната сигурност (CERT) във връзка с МИС и чрез координиране на националните екипи за действие при инциденти в информационната сигурност като кризисен център на ЕС по отношение на МИС, като успоредно ще се извършват както ежедневни управленски дейности, така и спешни услуги.

Този вариант би изисквал съществено увеличение на бюджета и човешките ресурси на Агенцията, което буди притеснения относно капацитета ѝ за усвояване и ефективно използване на бюджета по отношение на очакваните ползи.

Вариант на политика 5: Добавяне на оперативни функции в подкрепа на правоприлагащите и съдебните органи при борбата срещу престъпленията в кибернетичното пространство

В допълнение към изброените във вариант 4 дейности този вариант би включвал функции на агенцията, свързани с:

- предоставяне на подкрепа във връзка с процесуалното право (вж. Конвенцията за престъпленията в кибернетичното пространство): например събиране на данни за трафика, прехващане на данни за съдържание, мониторинг на потоците в случай на атаки от типа „отказ на услуги“;
- превръщането ѝ в център за експертен опит по отношение на разследване на престъпления, които включват аспекти на МИС.

Подобно на вариант 4, това би изисквало съществено увеличаване на ресурсите на Агенцията и е свързано с аналогични притеснения относно капацитета за усвояване и ефективното използване на бюджета.

6. СРАВНИТЕЛЕН АНАЛИЗ НА ВАРИАНТИТЕ НА ПОЛИТИКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЯТА

Анализът на възможните икономически, социални и екологични въздействия показва, че ***вариант 1*** би имал отрицателен ефект във всички аспекти и ситуацията би се влошила.

Вариант 2 се оказва недостатъчно оптимален, тъй като Агенцията не би разполагала с необходимите ресурси за успешно справяне с предизвикателствата на постоянно променящия се контекст на МИС, което би могло да изложи репутацията ѝ на риск и в крайна сметка да доведе до криза на доверие.

Съгласно ***вариант 3*** една модернизирана агенция за МИС би допринесла за:

Намаляване на фрагментацията на националните подходи (фактор за възникване на проблеми № 1), активизиране на политиката, базирана на данни и познания/ информация, и на вземането на решения (фактор за възникване на проблеми № 3) и

повишаване на цялостната осведоменост за и справяне с рискове и предизвикателства в сферата на МИС (фактор за възникване на проблеми № 4), чрез допринасяне за:

- по-ефективно събиране на съответната информация относно рискове, заплахи и уязвими аспекти от всяка отделна държава-членка;

- увеличаване на наличната информация относно текущите и бъдещи предизвикателства и рискове в сферата на МИС;

- осигуряване на по-високо качество на политиката в сферата на МИС в държавите-членки.

Подобряване на европейска способност за ранно предупреждаване и реагиране (фактор за възникване на проблеми № 2) чрез:

- подпомагане на Комисията и държавите-членки за организиране на паневропейски учения, като по този начин се постигат икономии от мащаба при реагиране на инциденти, засягащи целия ЕС;

- улесняване на функционирането на EP3R, което в крайна сметка би могло да доведе до нарастване на инвестициите в резултат на общи политически цели и стандарти за сигурност и устойчивост, приложими в целия ЕС.

Насърчаване на общия глобален подход към МИС (фактор за възникване на проблеми № 5) чрез:

- увеличаване на обмена на информация и познания с държави извън ЕС.

По-ефективна и ефикасна борба с престъпленията в кибернетичното пространство (фактор за възникване на проблеми № 7) чрез:

- ангажиране със задачи с неоперативен характер, свързани с аспекти на МИС, по отношение на правоприлагането и съдебното сътрудничество, като например двустранен обмен на информация и обучения (например в сътрудничество с Европейския полицейски колеж — CEPOL).

Вариант 4 би оказал по-голямо въздействие на оперативно ниво, в допълнение към въздействията, които да бъдат постигнати съгласно вариант 3. Функционирайки като екип на ЕС за действие при инциденти в информационната сигурност (CERT) във връзка с МИС и чрез координиране на националните екипи за действие при инциденти в информационната сигурност, Агенцията би допринесла например за по-големи икономии от мащаба при реагиране на инциденти, засягащи целия ЕС, както и за по-ниски оперативни рискове за предприятията поради по-високи нива на сигурност и устойчивост.

Вариант 5 би постигнал по-голяма ефективност в борбата с атаки в кибернетичното пространство в сравнение с варианти 3 и 4 благодарение на добавянето на оперативни функции при подпомагане на правоприлагащите и съдебните органи.

При все това, въпреки че както вариант 4, така и вариант 5 би оказал по-голямо положително въздействие в сравнение с вариант 3, и двата варианта биха били политически чувствителни за държавите-членки във връзка с техните отговорности по

отношение на CIIP (т.е. някои държави-членки не биха подкрепили централизирани оперативни функции). Освен това разгледаното във варианти 4 и 5 удължаване на мандата може да придаде двусмислие на позицията на Агенцията. Нещо повече, добавянето на тези нови и коренно различни задачи с оперативен характер към мандата на Агенцията може да се окаже сериозно предизвикателство в краткосрочен план и съществува значителен риск Агенцията да не се справи успешно с подобна задача в разумен срок. Не на последно място, разходите за изпълнение на варианти 4 и 5 са прекомерно високи — изискваният бюджет би надвишил четирикратно или петкратно настоящия бюджет на ENISA.

Сравнителният анализ на въздействията на петте варианта на политика за организационния формат на една модернизирана агенция за МИС показва, че варианти 1 и 2 трябва да отпаднат, тъй като нито един от тях не би позволил адекватно справяне със сложния проблем с МИС на ниво ЕС. От друга страна, варианти 3, 4 и 5 биха позволили на ЕС успешно да разглежда бъдещи варианти на политика за МИС. За момента варианти 4 и 5 изглеждат прекалено амбициозни както по отношение на политическата чувствителност на по-голяма част от държавите-членки, така и на отражението върху бюджета. Следователно ***вариант 3 изглежда най-добрият вариант за справяне по-най-ефективен начин с установените седем проблема в сферата на МИС.***

7. МОНИТОРИНГ И ОЦЕНКА: КАК МОГАТ ДА БЪДАТ ИЗМЕРЕНИ ДЕЙСТВИТЕЛНИТЕ РАЗХОДИ И ПОЛЗИ И ПОСТИГАНЕТО НА ЖЕЛАНИТЕ ЕФЕКТИ?

Настоящата политическа инициатива би осигурила периодични оценки, които да бъдат препращани от Комисията до Европейския парламент и Съвета и да бъдат публикувани. В тези оценки ще бъдат взети под внимание мненията на всички съответни заинтересовани страни на основата на условия, договорени с управителния съвет на Агенцията, и ще бъде оценена ефективността на Агенцията при постигането на целите ѝ, както и дали тя все още представлява ефективен инструмент и дали следва да бъдат направени някакви промени в нейния мандат и/или други аспекти на регламента за нейното създаване. След извършване на оценка управителният съвет на Агенцията ще издаде препоръки до Комисията относно подходящи промени, които да бъдат направени в регламента. Управителният съвет и изпълнителният директор на Агенцията следва да вземат под внимание резултатите от оценката в многогодишното планиране на Агенцията.

Действията на Агенцията подлежат на надзор от страна на омбудсмана в съответствие с член 228 от Договора.