

BG

BG

BG



КОМИСИЯ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ

Брюксел, 27.10.2008
SEC(2008) 2702

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

придружителен документ към

Предложение за

РЕШЕНИЕ НА СЪВЕТА

**относно Предупредителна информационна мрежа за критичната инфраструктура
(CIWIN)**

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

{COM(2008) 676 final}
{SEC(2008) 2701}

На 6 юни 2008 г. Комитетът за оценка на въздействието на Европейската комисия представи становище по предварителния вариант на доклада за оценка на въздействието. Накратко в становището се твърди, че докладът се изготвя на ясен език, разбираем и за неспециалисти, и предоставя подробен анализ на евентуалния проект на системата. Що се отнася до основните препоръки, в него се твърди, че текстът трябва да се усъвършенства, така че да описва по-добре съществуващите системи за обявяване на тревога в държавите-членки и следва по-ясно да представя ползите от CIWIN.

Освен това Комитетът заяви, че:

- Основният сценарий трябва да се разработи, като се подчертае добавената стойност на инициативата CIWIN.
- Документът следва да анализира доколко държавите-членки прилагат инициативата.

1. Инициативата CIWIN

Инициативата Предупредителна информационна мрежа за критичната инфраструктура (CIWIN) е част от Европейската програма за защита на критичната инфраструктура (EPCIP) и се занимава конкретно с процеса за обмен на информация между държавите-членки и с ИТ системата, която поддържа този процес. Въпросът за създаването на CIWIN бе повдигнат в Съобщението за EPCIP (COM (2006) 786 окончателен), което очерта хоризонталната рамка за защита на критичната инфраструктура в ЕС, и което включва мерки за улесняване на прилагането на EPCIP, включително на CIWIN.

Създаването на CIWIN вече е одобрено в заключенията на Съвета относно „Предотвратяване, готовност и реакция при терористични атаки“ и в „Програма за солидарност на ЕС относно последствията от терористични заплахи и атаки“, приети през декември 2004 г.¹

Основните проблеми към настоящия момент са:

- нуждата от по-подробна оценка как точно да се защити критичната инфраструктура на ЕС;
- нуждата от задълбочено сътрудничество и обмен на информация за критичните инфраструктури между държавите-членки на ЕС;
- дублиране на дейности;
- недостатъчно доверие и слабо желание от страна на участниците да обменят чувствителна информация.

2. Цели

Конкретният проблем, който налага действие на равнище ЕС, е да се улесни обменът на информация между органите на държавите-членки (например относно най-добри

¹ 14894/04

практики) и да им се предостави възможност да използват системата за бърза тревога за защита на критичната инфраструктура (ЗКИ).

Целта на CIWIN е да се подобри защитата на критичната инфраструктура в ЕС и да се улесни координацията и сътрудничеството по информация за ЗКИ на равнище ЕС.

Оперативните цели на CIWIN са:

- да осигури ИТ инструмент, който ще помогне на тези държави-членки, които желаят да си сътрудничат, да го сторят;
- да предложи ефикасна и бърза алтернатива на изискващите време методи за търсене на информация, т.е. да създаде един вид „система на едно гише“ за всякаква значима информация относно критичните структури в рамките на ЕС;
- да гарантира сигурност на споделяната информация;
- да предостави възможност на държавите-членки непосредствено да общуват и да качват в системата информацията, която смятат за важна.

Тъй като някои държави-членки биха предпочели да използват само някои от функциите, предлагани от CIWIN, една от основните оперативни цели е да се намери решение, което да предостави на държавите-членки възможност да участват или не в някои аспекти на системата.

3. ВАРИАНТИ НА ПОЛИТИКАТА

В оценката на въздействието се предлагат пет основни варианта на политиката.

Запазване на статуквото

Съгласно този вариант не се предприема никакво хоризонтално действие на европейско равнище, като всяка държава-членка се оставя сама да се справя с този въпрос.

CIWIN като усъвършенствана версия на съществуващите системи за бърза тревога (RAS)

Съгласно този вариант CIWIN ще представлява усъвършенствана система, която интегрира съществуващите RAS в една междусекторна RAS за критичната инфраструктура, до която имат достъп по-широк спектър от участници, а не само службите за извънредни ситуации. При все това този вариант няма да позволи обмена на обща информация и най-добри практики.

CIWIN като открита платформа за (незащитен) обмен на информация, свързана със ЗКИ

Съгласно този вариант се създава ИТ инструмент, отворен за широката общественост. Това несъмнено ще спомогне за по-добрата осведоменост относно защитата на критичните инфраструктури в Европа и ще увеличи прекия обмен на информация между участниците.

CIWIN като сигурна и доброволна/с възможност за включване система за комуникация/тревога на няколко нива, съставена от две отделни функции: система за бърза тревога (RAS) и електронен форум за обмен на идеи и най-добри практики относно ЗКИ

Съгласно този вариант CIWIN ще се създаде като ИТ инструмент, способен да съхранява и препраща чувствителна информация, класифицирана до равнище „UE RESTREINT“. Системата ще разполага с две основни функции: 1) защитен форум за обмен на информация с акцент върху обмена на добри практики, диалог и изграждане на доверие на равнище ЕС; 2) система за бърза тревога за критичната инфраструктура. Държавите-членки ще имат възможност свободно да използват цялата система, да избират измежду предлаганите функции или изобщо да не използват системата.

CIWIN като задължителна система за комуникация/тревога на няколко нива, съставена от две отделни функции: система за бърза тревога (RAS) и електронен форум за обмен на идеи и най-добри практики относно ЗКИ

Съгласно този вариант CIWIN ще бъде задължителна система, като всяка държава-членка ще има задължението редовно да зарежда и актуализира съответната информация.

4. Ползи и недостатъци на вариантите на политиката

Варианти на политиката	Предимства	Недостатъци
Вариант 1: без промяна на политиката	Без допълнително законодателно предложение; държавите-членки имат пълната свобода да се справя с въпросите на ЗКИ както сметнат за добре	Диалогът и обменът на информация между държавите-членки ще остане без промяна. Няма да съществува съгласувана, сигурна и ефикасна ИТ система за обмен на информация по ЗКИ в Европа. Няма въздействие върху подобряването на сигурността на ЕС. Няма гаранции, че съответните участници в Европа ще имат достъп до тази информация по ЗКИ, която е от значение.
Вариант 2: усъвършенствана версия на съществуващите RAS	Създава се междусекторна система за бърза тревога (RAS).	Висока цена, за да се осигури съвместимостта на съществуващите RAS. Този вариант не позволява обмен на информация и на най-

		добри практики. Така или иначе ще се наложи създаването на нова платформа за обмен на информация.
Вариант 3: открита платформа за (незащитен) обмен на информация	Широк достъп до информация, свързана със ЗКИ. Частният сектор ще има възможност пряко да допринесе за платформата. След като информацията, въведена в системата вече е публично достъпна, CIWIN ще предложи ефикасен, координиран и лесен достъп до нея.	Въведената информация в системата се ограничава единствено до неклассифицирана информация. Тъй като такава информация вече е достъпна, добавената стойност на този вариант е ограничена. Няма възможности за обмен на сигнали за тревога.
Вариант 4: сигурна система на няколко равнища с възможност за включване	Системата ще осигури защитена среда за обмен на информация и ще има значителен принос за изграждането на доверие между участниците. Включената информация ще надвиши обема, който вече е публично достъпен. Системата ще позволи да се обменят сигнали за тревога. CIWIN ще предложи ефикасна ИТ система, която е лесна за използване. CIWIN ще допринесе за увеличаване на сигурността в ЕС. CIWIN ще спомогне за преодоляване на фрагментираните научноизследователски усилия по ЗКИ чрез подобрена координация и задълбочено сътрудничество.	Участниците от частния сектор няма да имат непосредствен достъп до CIWIN. Успехът на системата ще зависи от желанието на държавите-членки да я използват.

Вариант 5: сигурна система на няколко равнища със задължително включване	Всички държави-членки ще участват в системата. Включената информация ще надвиши обема, който вече е публично достъпен. Системата ще позволи да се обменят сигнали за тревога. CIWIN ще предложи ефикасна ИТ система, която е лесна за използване. CIWIN ще допринесе за увеличаване на сигурността в ЕС. CIWIN ще спомогне за преодоляване на фрагментираните научноизследователски усилия по ЗКИ чрез подобрена координация и задълбочено сътрудничество.	Държавите-членки няма да подкрепят предложението. Една задължителна система може и да не допринесе за изграждане на доверие, а може да има и обратен ефект. Системата може да се окаже в противоречие с принципа на пропорционалност.
---	--	--

5. ПРЕДПОЧИТАН ВАРИАНТ

След анализ на петте варианта Вариант 4 — CIWIN като сигурна и доброволна/с възможност за включване система за комуникация/тревога на няколко нива, съставена от две отделни функции: система за бърза тревога и електронен форум за обмен на идеи и най-добри практики относно ЗКИ — ясно показва най-благоприятното съотношение между ползи и недостатъци

Трябва да се наблегна на факта, че CIWIN няма да доведе до революционна промяна на сигурността на ЕС, а по-скоро трябва да се разглежда като една от многото стъпки към реализацията на EPCIP. CIWIN е ИТ инструмент, чиято цел е да улесни комуникацията по теми, свързани със защитата на критичната инфраструктура, и предоставя функции като табло за бюлетин с новини, дискуссионни групи, среда за сътрудничество, средства за управление на документооборота и работния процес, които са част от ежедневната употреба на интернет или на корпоративния интранет. Работата по CIWIN ще вземе предвид широка гама характеристики, като в същото време ще гарантира, че съществуването им може да бъде прекратено в случаите, в които се прецени, че вече не носят никаква добавена стойност или са в противоречие с установените практики.