Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Проект „**Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство**”” с рег. № К11-32-1/ 20.9.2011 г., осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет”

Проектът се финансира от Европейския социален фонд и от държавния бюджет на Република България

СЪЗДАВАНЕ НА УНИФИЦИРАНИ ИЗИСКВАНИЯ КЪМ ЦЕНТРОВЕТЕ ЗА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

ДОКЛАД С ПРИЛОЖЕНИЯ ЗА СВЕТОВНИЯ ОПИТ И ДОБРИТЕ ПРАКТИКИ ПРИ РАЗРАБОТВАНЕТО И ВЪВЕЖДАНЕТО НА СИСТЕМИ ОТ ЕДИННИ ИЗИСКВАНИЯ КЪМ ИЗГРАЖДАНЕТО И СЕРТИФИЦИРАНЕТО НА ЦЕНТРОВЕ ЗА СЪХРАНЕНИЕ НА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ ЗА НУЖДИТЕ НА ЦЕНТРАЛНА ДЪРЖАВНА АДМИНИСТРАЦИЯ В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2005.

Съдържание

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

ЕС	**Европейски съюз**
ЕАМИС	**Европейска агенция за мрежова и информационна сигурност**
ЕУИ	**Единни унифицирани изисквания**
ЕУИЦСОЧИ	**Единни унифицирани изисквания за Центровете за съхранение на особено чувствителна информация**
ИКТ	**Информационни и комуникационни технологии**
ИТ	**Информационни технологии**
КИИ	**Критични информационни инфраструктури**
КИКИ	**Критична информационна и комуникационна инфраструктура**
ЗОП	**Закон за обществените поръчки**
ПЧП	**Публично частно партньорство**
СУСИ	**Система за управление на информационната сигурност**
ЦСОЧИ	**Център за съхранение на особено чувствителна информация**
CIIP	**Critical Information Infrastructure Protection**
CERT	**Computer Emergency Response Team**
CSIR	**Computer Security and Incident Response Team**
ENISA	**European Network and Information Security Agency**
ISO	**International Standard Organization**

1. Единно европейско информационно пространство и възникващата необходимост от въвеждането на единни национални изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация.

Възникващата необходимост от въвеждането на единни национални, регионални или общностни стандарти в динамично развиващата се област като информационните технологии, се определя от обществения интерес както на социалните групи, които са потребители на информация, така и на целевите групи, които са носители на експертното знание да създават и развиват информационните системи и технологии.
Съвременните тенденции за консолидация на данните и визуализация на ресурсите за обработка на информацията в условията на непрекъснато разширяващ се като покритие и достъпност Интернет, поставят нови, по-високи изисквания към инфраструктурата за съхранение на информацията и осигуряване на достъп до приложения – по-високи изисквания към центровете за данни.

Лавинообразното навлизане на информационните и комуникационните технологии в практически всички сфери на социална активност поставя на дневен ред въпроса за изследване на зависимостта на съвременното общество от работоспособността на обслужващия го ИТ сектор и разглеждането на информационната и комуникационната инфраструктура, като неразделна част от критичната инфраструктура в национален и общностен мащаб.

В Единното европейско информационно пространство тази тенденция обективно се проявява с голяма амплитуда, поради спецификата на социалната структура, високия % на реално използващите е-технологии и политиките за насърчаване на прилагането и развитието на е-технологиите в обществения и държавните сектори.

Високият обществен интерес в страните-членки към рисковия потенциал на процеса за масово навлизане на информационните технологии се проявява активизиране на дейността на Европейската комисия в тази посока и дефинирането в началото на новия век на нова приоритетна област за стратегическо развитие и взаимодействие, наречена Европейско информационно общество (http://ec.europa.eu/information_society/index_en.htm) като ключов приоритет в тази област е разработването на Европейски политики за мрежова и информационна сигурност (http://ec.europa.eu/information_society/policy/nis/index_en.htm).
Още от създаването си работната група на ЕС развива активна дейност като свързващо звено между ЕС и Европейския парламент и по-специално Европейския икономически и социален комитети, Комитета на регионите, като първият програмен документ е публикуван през март 2001[1] и е озаглавен „Мрежова и информационна сигурност: Предложение на Европейски политически подход”. В този документ се очертава необходимостта от установяване на минимални и устойчиви изисквания, измерими критерии и нива на защита на информационната инфраструктура, като се подчертава, че в тази насока активностите е необходимо да се провеждат съгласувано, както на национално, така и на общоевропейско ниво. В Раздел IV от документа са определени и приоритетните области, които е необходимо да съсредоточат усилията при

разработването и прилагането на синхронизирани национални и общоевропейски политики. Като приоритетна област е определена мрежовата и информационната сигурност на ИКТ инфраструктурата на системи на държавната администрация (е-правителството): „Security in government use…"[1], както и определянето на единни критерии за сигурност и непрекъсната достъпност на тези системи и свързаните с тях вътрешни и външни (масови) услуги.

В изпълнение на програмният документ от Стокхолм[1] март'2001 в ЕС се създава и специализирана експертна група по въпросите на Защита на критичната информационна инфраструктура, известна като **CIIP** (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm) - **C**ritical **I**nformation **I**nfrastructure **P**rotection, която развива своята дейност и във връзка с Европейската директива за идентификация и обозначаване на Европейската критична инфраструктура. Актуалните документи, които към момента определят активностите на Експертната група на ЕС-CIIP са:

- СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ относно защитата на критичната информационна инфраструктура „Защита на Европа от широко мащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта", рег. № CM(2009) 149 окончателен [2] и по-специално Раздел 5.5, в който се определя необходимостта до края на 2010 да се разработят специфични критерии за класифициране на Европейската критична инфраструктура, приложими за ИКТ сектора.
- Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество за мрежова и информационна сигурност, рег.№ 2009 / C 321/01).
- СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ относно "Защита на критичната информационна инфраструктура: Постижения и следващи стъпки: към глобалната кибер-сигурност", рег.№ COM(2011) 163 окончателен[3].

Втората ключова стъпка, която се предприема в изпълнение на програмният документ от Стокхолм[1] март'2001 в ЕС е създаването през 2004 година на Европейската агенция за мрежова и информационна сигурност – ЕАМИС (European Network and Information Security Agency (ENISA)) с цел да гарантира високо ниво и ефективност на мрежовата и информационна сигурност в ЕС, съгласно РЕГЛАМЕНТ (ЕО) № 460/2004 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА НА ЕВРОПА. Като за срока си на функциониране (до март 2012) ЕС поставя пред агенцията следните цели[2]:

- Постигане на високо и ефективно ниво на мрежовата и информационната сигурност в рамките на Европейския съюз - мисията на Агенцията;

- Заедно с институциите на ЕС и държавите-членки да подпомага развиването на култура на мрежовата и информационната сигурност в полза на гражданите, потребителите, бизнеса и организациите от публичния сектор в Европейския съюз;
- Да помага на Европейската комисия, държавите-членки и бизнес общността за откриване, прекратяване и превенция на атаки, пробиви и потенциални рискове на мрежовата и информационна сигурност;
- Като орган на експертиза, създаден от ЕС, да изпълнява специфични технически и научни задачи в областта на информационната сигурност;
- Да подпомага Европейската комисия в техническата подготовка за актуализиране и разработване на законодателството на Общността в областта на мрежовата и информационната сигурност.

Като Агенция, създадена да подпомага разработването на синхронизирани национални стратегии за информационна сигурност, през май 2012 г. ENISA публикува мониторингов доклад[5] за състоянието на Единното европейско информационно пространство по отношение на обхвата и акцентите на възникващата необходимост от въвеждането на единни национални изисквания за мрежова и информационна сигурност. В Доклада[5] се прави анализ на текущото състояние на стратегии за информационна и кибер-сигурност в рамките на Европейския съюз. При анализа се идентифицират и се извеждат общи теми и различия при разработването на Национални стратегии и политики и се дават поредица от забележки и препоръки, свързани с обхвата и механизмите за хармонизиране и осигуряване на информационна съвместимост в Общността. Докладът[5] е практически въвеждащ документ, в който се дават предварителните констатации и анализи, във връзка с изведената от експертите на ENISA необходимост от разработване на Ръководство за добри практики за разработване, прилагане и поддържане на национална стратегия за информационна и кибер-сигурност [5]. В Доклада се определя и ролята на Ръководството за добри практики - да бъде полезен инструмент и да дава практически съвети за националните работни групи, отговорни за разработването и практическото прилагане на тези стратегии и политики.
На фиг.1 е представена информация за анализираните в Мониторинговия доклад на ENISA Национални стратегии за информационна и кибер-сигурност, като е представена и сравнителна информация за годините на публикуване на стратегиите.

*Фиг.1. Информация за годината на публикуване на Нациоанлна стратегия за информационна и кибер-сигурност за страните-членки на ЕС и в стравнение със САЩ, Канада и Япония *Източник [5]*

От представената информация и от анализите в доклада се вижда, че катализирането на необходимостта от разработване на такъв тип стратегии или политики е практически винаги свързано с реално събитие или инцидент, който извежда на преден план обществения интерес за разработването на такъв тип програмни документи в областта на информационната сигурност, съхранението и обработката на чувствителна информация. Например, събитията от 11 септември, е една от главните причини Националната стратегия на САЩ да се разработи от 5 до 8 години по-рано от подобни стратегии в останалите водещи индустриални държави, като Франция и Великобритания. И интересният акцент, е че САЩ публикуват "International Strategy for Cyber-space"[15], т.е.още в националният си програмен документ те показват, че практически информационното пространство няма граници и свързаните с него регулации е задължително да отчитат тази реалност, особено от гледна точка на постигане на съвместимост, непрекъсната и интегрирана сигурност.

Не случайно и Естония е сред първите страни-членки на ЕС, с разработена и публикувана стратегия за информационна сигурност[7]. След кибер-атаките от 27 април 2007 година, когато бяха засегнати ключови информационни системи, в т.ч. Естонския парламент, се предприеха спешни мерки за установяване на измеримо ниво

на защита на критична информационна инфраструктура, обслужваща държавната администрация, банковия, енергийния и транспортния сектори.

Един от основните изводи в анализа на ENISA[5] е необходимостта от проактивно разработване на национални програмни документи в областта на защитата и сигурността на критичната информационна инфраструктура, в които като приоритет да е заложена основа за международно взаимодействие, кооперирание и хармониране на активностите с цел осигуряване на непрекъснато като сигурност информационно пространство, както в рамките на Общността, така и по отношение на по-широк кръг международни алианси и споразумения за сътрудничество в тази стратегическа област.

Един от основните приноси в мониторинговия доклад на ENISA е опита да се дефинира един типичен обхват на дейности и области в една Национална стратегия за защита и сигурност на информационното пространство[5]:

- Да определи рамката и структурата за управление на сигурността в информационното пространство на национално ниво.
- Да дефинира подходящ механизъм (например, публично-частно партньорство или друг), който да позволява на всички заинтересовани страни да участват в обсъжданията и да се споразумеят за различни политически и регулаторни мерки и/или ограничения, свързани с въпросите на сигурността на критичната информационната инфраструктура.
- Да изведе необходимостта от политически и регулаторни мерки, при ясно определени роли, отговорности и права на частния и публичния сектор (нова правна рамка за борба с престъпленията в кибернетичното пространство, задължително докладване на инциденти, минимални мерки за сигурност и насоки, нови правила за възлагане на обществени поръчки). Например, стратегията на Словакия идентифицира необходимостта да се определи правна рамка за защита на критичната информационна инфраструктура.
- Да очертае цели и средства за разработване на национални приоритети и необходимата правна рамка, в национален мащаб и за ефективно включване в международните усилия за намаляване на последиците от престъпленията в информационното (кибер) пространство. В няколко стратегии има особен акцент върху престъпленията в кибер-пространство. Например, в Холандия се дават насоки за засилване на разследването и преследването срещу лица и групи с рисково поведение в информационното пространство [13], във Франция също се подчертава необходимостта от промени в националното законодателство и както и при международното съдебно кооперирание при разследването на такъв тип рисково или криминално поведение[9].
- Да определи критерии за идентифициране и категоризиране по степени на риск критичните информационни инфраструктури (КИИ), включително ключовите активи, услуги и взаимозависимости.
- Да определи обхвата и съдържанието на оперативните документи и процедури за подобряване готовността за превенция, реакция и възстановяване, както и разработване на планове и мерки за защита на КИКИ, например в Стратегията

на Литва е записано, че "За да се гарантира сигурността на кибер-пространството, е необходимо да се установи непрекъсната и правилно управлявана система, която обхваща всички фази на управление на инциденти, като например ранно предупреждение, предотвратяване, откриване, премахване и разследване"[11]. В тази насока могат да се разглеждат и дейностите по институционално развитие на интегрирани организационни структури, които се развиват, прилагат и изпробват плановете и мерките за подготовка, превенция, реагиране и възстановяване след рисково събитие.

- Да определи систематичен и интегриран подход на националното управление на риска (например надежден обмен на информация и национални регистри на рискове).

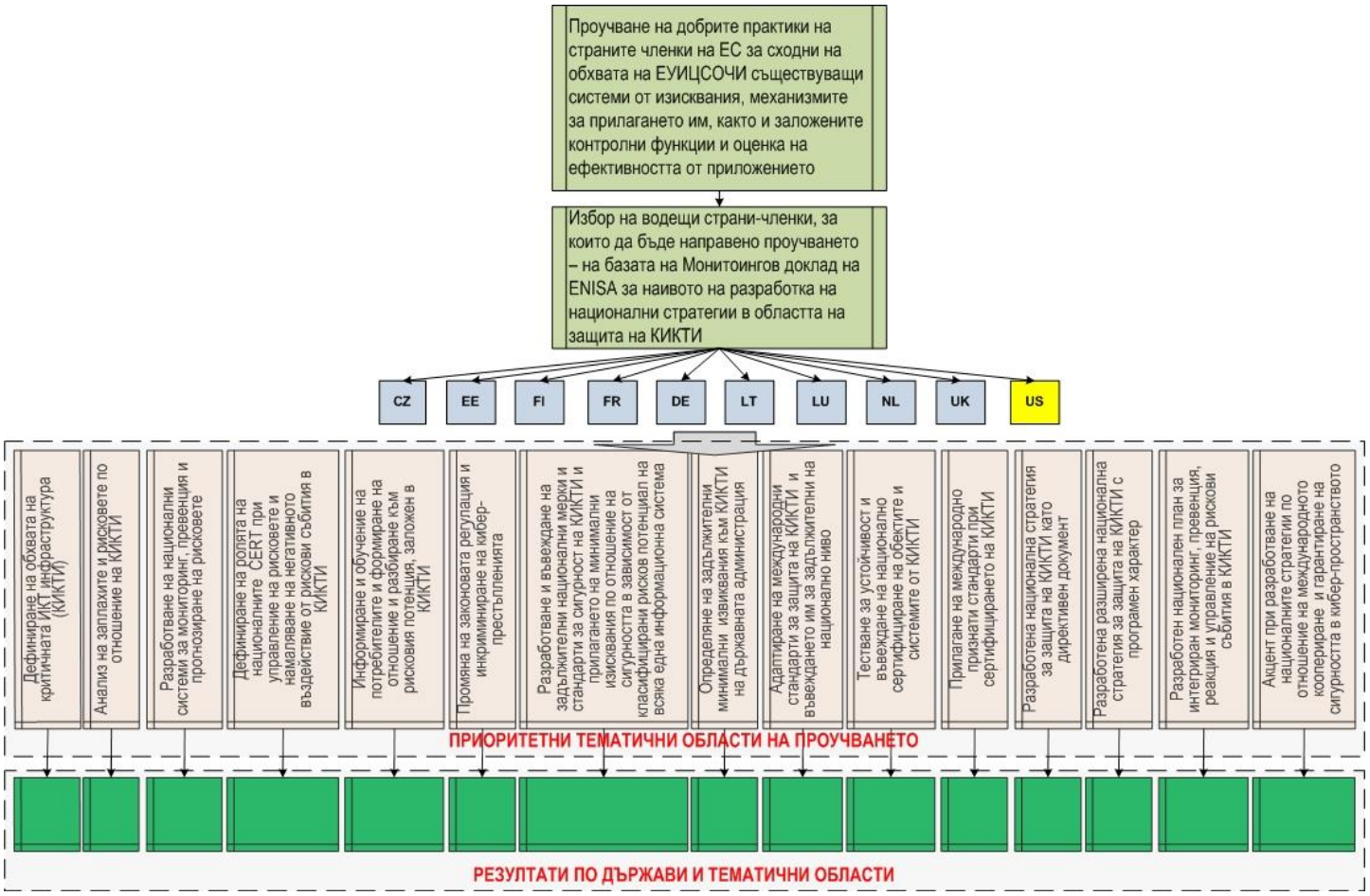
Представеният кратък обзор потвърждава факта, че в Единното европейско информационно пространство има ясно изградена позиция по отношение на обхвата и акцентите на възникващата необходимост от въвеждането на единни национални изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация от гледна точка на националните приоритети и европейския информационен обмен. Действията в тази посока, както се вижда и от информацията представена на фиг.1, са на фаза стратегическо планиране и разработване на оперативни национални програми, стандарти, планове и мерки за подготовка, превенция, реакция и ограничаване на негативните последици от рискови събития, възникнали в критичната информационна инфраструктура. В този смисъл, действията по разработването на Единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ) за нуждите на държавната администрация на Република България са навременни, необходими и отразяват общоевропейските цели и приоритети за осигуряване на ефективна защита на критичната информационна инфраструктура, особено тази част, функционираща за целите на държавното управление.

2. Представяне и избор на съществуващи системи от изисквания, механизмите за прилагането им, контролните функции и оценка на ефективността от приложението – акцент върху опита и добрите практики на страните – членки на ЕС.

За целите на обзора на добрите практики при осигуряването на ефективна защита на критичната информационна инфраструктура, осигуряваща приоритетно дейността на държавната администрация, е необходимо да бъдат дефинирани приоритетни теми, по които да бъде проведено проучването. От една страна е необходимо да се оценят общите изисквания и приоритетите по отношение на интеграцията на процеса за мониторинг, превенция, реакция и управление на рискови събития и кризисни ситуации по отношение на критичната информационна и комуникационна инфраструктура, като неразделна част от Европейската критична инфраструктура, съгласно ДИРЕКТИВА 2008/114/ЕО НА СЪВЕТА от 8 декември 2008 година относно „Установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита"[17]. От друга страна е съществено да се обобщи опита в тесния смисъл на практиките за въвеждане на единни национални изисквания, които да се прилагат в определен обхват в зависимост от класифицирания рисков потенциал на съответния център за съхранение и обработка на особено чувствителна информация, като част от КИКТИ.

На базата на тези две ограничения и във връзка с приоритетите, дефинирани в РЕЗОЛЮЦИЯ НА СЪВЕТА от 18 декември 2009 година относно „Европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност" (Рег.№ 2009/C 321/01)[18], могат да се дефинират следните базови показатели за провеждане на обзорното проучване, представени на фиг.2. На фиг.2 е представен и в най-общ вид модел на провеждане на проучването. Критериите за избор на страни, чиито опит да бъде проучен е на базата на Мониторинговия доклад на ENISA [5], като към тези страни е добавена за сравнение и САЩ. Допълнителна информация за проучването е натрупана на базата на публикациите във връзка с изпълнението на поетите от страните-членки ангажименти по Европейска инициатива за защита на критичната информационна инфраструктура (*http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm*) както и съвместните публикации на ENISA и CIIP във връзка с хода на разработването на националните планове за защита на критичната информационна и комуникационна инфраструктура (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/national-contingency-plans).

При проучването са подложени на анализ Националните стратегии на избраните държави [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], както и свързаните с тези документи приложения, национални планове и доклади за напредъка на страните-членки[20] и САЩ[19].



фиг.2. Базови показатели за провеждане на обзорното проучване

На базата на модела за провеждане на проучването и информацията от цитираните източници, са изведени обобщени резултати за приложимите добри практики в Таблица 1. Анализът е проведен по 15-те приоритетни тематични области, като целта е да се изведат тематичните области, по които има практически постигната консенсусна позиция и да се анализират областите, в които има различия, както и до колко областите, по които тече дискусия имат проекция към спецификата на националните традиции и особености на българското информационно пространство.

От представената информация се вижда, че в общоевропейски план все още е отворена дискусията за обхвата на т.нар. критична информационна и комуникационна инфраструктура (КИКИ). Прави впечатление, че в Бенелюкс, понятието КИКИ е трайно подменено от т.нар. „Чувствителни системи и данни", като разликата в двете понятия се състои в приоритета на оценката на риска. Ако в контекста на CIIP критичната инфраструктура се разглежда от технологичната страна за осигуряване на защитата на ключови информационни ресурси, то фокуса при „Чувствителните системи и данни" е човека, услугите, които се осигуряват чрез опериране с чувствителни данни, достъпността до чувствителни услуги и т.н. В този смисъл, за различните социални групи, могат да бъдат дефинирани различни като обхват, съдържание и функционалност „Чувствителни системи и данни", докато КИКИ (в аспекта на CIIP)

обективно съществува, маркира се, наблюдава се и работи, независимо от субективната необходимост. И тъй като целта на обзора е по дискусионните теми да се определи към коя от алтернативите е по-близо националната специфика на България, но определено за българското информационно пространство е по-приложима базовата дефиниция на CIIP за критична информационна инфраструктура.

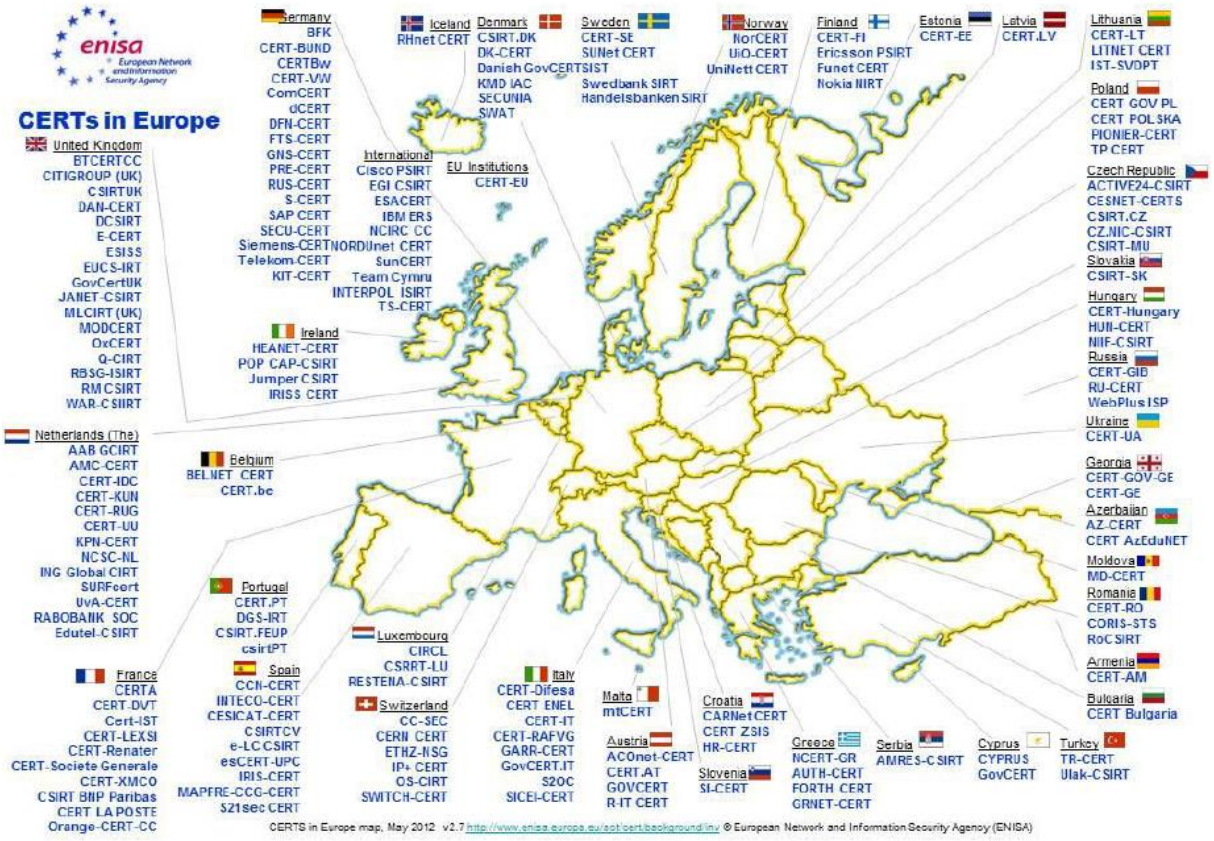
Таблица 1. Обобщени резултати от проучването на приложимите добри практики

	Приоритетни направления, политики и добри практики в Националните стратегии и планове на страните членки на ЕС при осигуряването на ефективен мониторинг, превенция и реакция на рискови събития за критичната информационна и комуникационна инфраструктура (КИКИ)	CZ*	EE	FI	FR	DE	LT	LU	NL	UK	US
1	Дефиниране на обхвата на критичната ИК инфраструктура (КИКИ)		■		■	■	■				
2	Анализ на заплахите и рисковете по отношение на КИКТИ	■	■	■	■	■	■	■	■	■	■
3	Разработване на национални системи за мониторинг, превенция и прогнозиране на рисковете за КИКИ	■	■							■	■
4	Дефиниране на ролята на националните CERT при управление на рисковете и намаляване на негативното въздействие от рискови събития в КИКИ	■	■	■	■	■	■	■	■	■	■
5	Информиране и обучение на потребителите и формиране на отношение и разбиране към рисковия потенциал, заложен в КИКИ	■	■	■	■	■	■	■	■	■	■
6	Промяна на законовата регулация и инкриминиране на кибер-престъпленията	■	■	■	■	■	■	■	■	■	■
7	Разработване и въвеждане на задължителни национални мерки и стандарти за сигурност на КИКИ и прилагането на минимални изисквания по отношение на сигурността в зависимост от класифицирания рисков потенциал на всяка една информационна система	■	■			■		■	■	■	■
8	Определяне на задължителни минимални извиквания към КИКИ на държавната администрация		■	■	■	■				■	■
9	Адаптиране на международни стандарти за защита на КИКИ и въвеждането им за задължителни на национално ниво		■				■				
10	Тестване за устойчивост и въвеждане на национално сертифициране на обектите и системите от КИКИ			■							■
11	Прилагане на международно признати стандарти при сертифицирането на КИКИ	■	■		■	■	■	■	■	■	
12	Разработена национална стратегия за защита на КИКИ като директивен документ	■				■		■	■		
13	Разработена разширена национална стратегия за защита на КИКИ с програмен характер		■	■	■		■			■	■
14	Разработен национален план за интегриран мониторинг, превенция, реакция и управление на рискови събития в КИКИ		■			■					■
15	Акцент при разработване на националните стратегии по отношение на международното кооперирание и гарантиране на сигурността в кибер-пространството	■	■	■	■	■	■	■	■	■	■

**Използвани съкращения на държавите съгласно ISO 3166 alpha-2*

Въпреки че в заглавната част на проекта фигурира определението „чувствителна” по отношение на информация, приложимостта на CIIP подхода за България е по-ефективен, тъй като дава възможност за допълнително вторично класифициране на КИКИ в зависимост от рисковия потенциал и прилагане на мерки, адекватни на проектна заплаха.

Другият дискусионен въпрос е свързан с обхвата на националните CERT структури и до колко те могат да изпълняват функциите на национални центрове за мониторинг, превенция и прогнозиране на рискови събития за КИКИ. И ако от края на 90-те години двете абревиатури CERT (Computer Emergency Response Team) и CSIR (Computer Security and Incident Response Team), практически обозначават един и същ набор от активности, то ако сравним съвременните разбирания за ролята на CERT, CERT е „…организация за проучвания и изследване на компютърна и мрежова сигурност с цел предоставяне на услуги за реагиране при инциденти, подпомагане на „жертвите” на атаките, която публикува предупреждения за уязвимости и заплахи, както и предлага друга информация, за да помогне за подобряване на компютърна и мрежова сигурност”[21] с тематична област 3: ”Разработване на национални системи за мониторинг, превенция и прогнозиране на рисковете за КИКИ”, се наблюдава определено припокриване на функции. Картата на покритие на CERT мрежата, дава основание да се смята, че от гледна точка на осигуряване на непрекъснатост на защитата на информационното пространство, интегрирането на националните CERT е значително по-успешен подход, отколкото разбиването на паралелни контролни структури – фиг.3.



фиг.3. Карта на покритите на Европейската мрежа на CERT\CSIRT

На територията на България ефективно работи националната структура на CERT\CSIRT (https://govcert.bg/BG/Pages/default.aspx), като от гледна точка на добрите практики ще е необходимо тази структура да се интегрира по-пълно, като елемент на една бъдеща Национална стратегия за защита на КИКИ. От гледна точка на обхвата на ЕУИЦСОЧИ, връзките с националния CERT\CSIRT могат да бъдат реализирани на етапите, свързани с установяването на съответствието с вече дефинираните изисквания и оценка на ефективността на защитата, развита чрез прилагането в практиката на ЕУИЦСОЧИ.

Съзнателно в приоритетните теми на проучването специфично се разделя *разработването и въвеждането на задължителни национални мерки и стандарти за сигурност на КИКИ и прилагането на минимални изисквания по отношение на сигурността в зависимост от класифицирания рисков потенциал на всяка една информационна система* (приоритетна тематична област 7-Таблица 1) от определянето на задължителни минимални извиквания към КИКИ на държавната администрация (приоритетна тематична област 8-Таблица 1). От представените резултати на Таблица 1 се вижда, че се наблюдава тенденцията, че в по-голяма част от включените в проучването държави се планира установяване на въвеждането на задължителни национални стандарти и минимални изисквания към обектите и системите на КИКИ. За една част от държавите наред с общите национални стандарти и минимални изисквания се конкретизират и адаптират за спецификата на информационното обслужване на държавната администрация – такъв е случая при Естония, Германия, Великобритания и САЩ. Има и страни, в които се предвижда въвеждане на общи национални стандарти и минимални изисквания за обектите и системите на КИКИ, без да се конкретизира за определена област, като е достатъчно обектът и/ или системата да отговарят на критериите и да са “маркирани” като КИКИ - Чехия, Люксембург и Холандия. За Франция и Финландия е характерно, че се предвижда въвеждането на национални стандарти и минимални изисквания за обектите и системите на КИКИ, които да са задължителни за държавната администрация и препоръчителни или подусловие за останалите сектори. В тези разглеждания, прецедент е Литва, като в националната й стратегия е акцентирано върху пълното адаптиране и приемане на международно признати стандарти като ISO27001 и други, като задължителни, без да се налага изобщо да бъдат разработвани национални стандарти, критерии или изисквания във връзка със защитата на КИКИ. Къде е мястото на България? Ако се базираме на идеята за това, че времето е факторът, доказващ добрите практики, то в страните с най-дълъг стаж в прилагането на национални стратегии за защита на КИКИ – Естония и САЩ (фиг.1) се прилага комбинирания подход, т.е разработване на единен национален стандарт и минимални изисквания по отношение на обектите и системите на КИКИ и специфични или адаптирани изисквания, като следствие на общите, но при отчетена специфика на процесите, функционалността и мащаба на информационно обслужване за целите на държавната администрация. Един такъв подход предполага съсредоточаването на повече експертиза и административен капацитет за създаване на нормативна база, методическо осигуряване и практически указания за въвеждане и поддържане на

съответствието с общите и специфични изисквания. Предимството е, че ако при общия анализ на риска по отношение на КИКИ, допустимият праг на нанесените щети може да бъде съобразен с особеностите на сектора, то тогава допълнителни ограничения се налагат само за случаите, които са извън бизнес логиката за поемане на "измерим" риск и се свързват устойчиво с обслужването на обществения интерес (за който тази логика не е приложима) – такъв сектор е Държавната администрация. При наличието на концентрация на експертно знание в областта у нас и възможността да бъде съсредоточен достатъчен административен капацитет, опита на Естония изглежда, че стои най-близо до реалностите в българското информационно общество. В този смисъл, при разработването на ЕУИЦСОЧИ, е важно да бъдат изведени и дефинирани в голяма степен онези съдържателни части, които биха послужили като изходна база за разработване на обобщения единен национален стандарт и минимални изисквания на обектите и системите от КИКИ за всички сектори.

Правейки паралел между резултатите от проучването по приоритетни теми 11 и 15 (съответно: „*Прилагане на международно признати стандарти при сертифицирането на КИКИ*" и „*Акцент при разработване на националните стратегии по отношение на международното кооперирание и гарантиране на сигурността в кибер-пространството" – Таблица1*), се вижда консенсусната позиция на преобладаващата част от наблюдаваните страни, че естествения път за постигане на взаимодействие и непрекъсната защита на глобалната критична информационна инфраструктура е постигането на съответствие с общопризнати международни стандарти в областта на защита на информацията и информационните системи като например групата стандарти ISO27000. От тази обща тенденция типичното изключение е САЩ, като причината е преди всичко в силната позиция на територията на САЩ на Националния институт за стандарти и технологии (National Institute of Standards and Technology (NIST)), който публикува през май 2010 година програмен документ[22] (публично достъпна е само "draft" версията), който при оценката на риска на критичната ИТ инфраструктура се определя като водеща методиката на HIPPA[23]. Франция, също прави изключение от общата тенденция, тъй като за Франция е характерно, че проблемите за защита на критичната информационна инфраструктура се решават традиционно (повече от 10 години) по линията на публично-частното партньорство, като двигател да тези дейности е CLUSIF (Клуб за информационна сигурност на Франция), който през 2008 публикува програмен документ[24], чрез който се установява методиката за национално сертифициране и селективно прилагане на международните стандарти в областта за защита на информацията и информационните системи. И двете типични изключения, всъщност, потвърждават основната тенденция за неотменната необходимост при разработването на единни национални изисквания към обектите и системите на КИКИ да се търси възможност за прилагане на утвърдени международни стандарти, което е условие и гаранция за взаимодействие и осигуряване на непрекъсната сигурност в глобалното информационно пространство, част от което са националните КИКИ.

Проучването на добрите практики по отношение на приоритетни теми 12, 13, 14 – Таблица 1 има за цел да очертае характерната последователност и обхват на

различните типове програмни документи, които се разработват в национален мащаб по отношение на защита на КИКИ. Както се вижда от представените резултати, а при един по-детайлен преглед може да се направи извод, че пътя на всяка страна-членка е специфичен и няма ясно очертаваща се тенденция кой подход е по-успешен. Дали подхода от долу-нагоре, т.е от секторните стандарти и единни изисквания към национална стратегия (Германия, Естония) или обратния път – от национална стратегия, към програма и оперативни планове и секторни минимални изниквания (Холандия, Чехия). Великобритания е пример за подхода от средното ниво към националното и секторните нива. Тази тенденция се обуславя от силната национална стандартизационна практика в областта, чиито традиции датират от повече от 15 години, т.е не е необходим стратегически етап. За нашите условия, въпреки че България няма разработена самостоятелна стратегия за защита на КИКИ, според годишния доклад на ENISA за нашата страна за 2011 година[28], България има ясно дефинирани стратегически и програмни цели в областта на защита на критичната информационна инфраструктура, като водеща роля има държавната администрация, чрез разработените два програмни документа – Обща стратегия за електронно управление на Република България 2011-2015[26] и Национална програма за ускорено развитие на информационното общество в Република България (2008-2010г.)[27]. В този смисъл и от гледната точка на независимата европейска институция ENISA, България е готова за разработка на секторни стандарти в приоритет по отношение на обекти и системи от КИКИ, обслужващи държавната администрация и информационните масиви в обхвата на е-правителството.

На базата на проведеното проучване, могат да бъдат изведени следните приложими добри практики на страните членки на ЕС за сходни на обхвата на ЕУИЦСОЧИ съществуващи системи от изисквания, механизмите за прилагането им, както и заложените контролни функции и оценка на ефективността от приложението:

- (1) Разработване в рамките на националните програмни документи на специфични единни изисквания за КИКИ (ЦСОЧИ) за държавната администрация (*Естония, Финландия, Франция, Германия, Великобритания*);
- (2) Въвеждане на единни унифицирани изисквания към проектирането, техническите решения и програмно осигуряване на обектите и системите на КИКИ (ЦСОЧИ) за държавната администрация, съвместими с международно признатите стандарти от серията ISO27000 (*Чехия, Естония, Франция, Германия, Латвия, Люксембург*);
- (3) Разработване на методика за въвеждане на единните унифицирани изисквания за съществуващи и новоизграждащи се обекти и системи на КИКИ (ЦСОЧИ) (*Естония и Германия*);
- (4) Въвеждане на минимални изисквания за техническите решения и програмно осигуряване, които да се прилагат при конкурсите за избор на изпълнители на обекти и системи на КИКИ (ЦСОЧИ) за държавната администрация (*Финландия и Естония*);

- (5) Разработване на процедура за обмен на информация между ЦСОЧИ и националния офис на CERT с цел осигуряване на ефективна интеграция с Европейската и глобалната система за защита на критичната информационна инфраструктура (*всички страни от проучването – Таблица 1*).

Прилагането на тези добри практики и следването на успешната национална експертиза и постижения в областта са необходимите условия за качеството на разработването и ефективността на въвеждането на Единните държавни изисквания към ЦСОЧИ в реалната практика при осигуряването на необходимата измерима и прогнозируема степен на защита на критичната информационна инфраструктура на държавната администрация (е-правителството) на Република България.

3. Специфика на приложението на ISO/IEC 27001:2005 при изграждането на центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация.

Спецификата на приложението на **ISO/IEC27001:2006** при изграждането на центрове за съхранение на особено чувствителна информация за нуждите на държавната администрация се свърза с факта, че стандартът на практика съдържа най-добрите международни практики в сигурността на информацията за настоящия момент. Той предоставя на всяка организация, агенция или ведомство надеждна и ефективна рамка за въвеждането на система за управление на сигурността на информацията, която да защити активите й, да осигури устойчивост на процесите на обслужване и да гарантира обществения интерес при развитие и цялостна реализация на концепцията за е-правителството и свързаните с нея публични и вътрешни информационни процеси, услуги, структури от данни и функционални връзки.

Целта на настоящия обзор е да се обобщят и анализират основните изисквания и дейностите по създаване, внедряване, използване, наблюдение и подобряване на система за управление на сигурността на информацията в ЦСОЧИ, обслужващи централната държавна администрация, в съответствие с изискванията на международния стандарт БДС ISO/IEC27001:2006 и по-конкретно:

- Да се изясни същността, особеностите и спецификата от гледна точка на конкретния обект на приложение (ЦСОЧИ) на стандартите за управление на сигурността на информацията и по-специално на БДС ISO/IEC27001:2006;
- Да се анализират специфичните изисквания и начините за внедряване на системи за управление на сигурността на информацията (СУСИ) като интегриран елемент от процеса на **въвеждането на единни национални изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация от гледна точка на националните приоритети и европейския информационен обмен**;
- Да се посочат конкретни насоки и практики за разработването и внедряването на СУСИ в контекста на бъдещото разработване на Методика за изграждане и сертифициране на центрове за съхранение на особено чувствителна информация за нуждите на централната държавна администрация.

От приложна гледна точка ISO27001 „определя изискванията за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на документирана СУСИ. Този международен стандарт може да бъде използван за оценяване на съответствието от вътрешни и външни заинтересовани страни.”[29]. С други думи той е конкретният документ, спрямо който една СУСИ може да бъде оценявана. Необходимостта от въвеждане на СУСИ като структурен елемент от Единните унифицирани изисквания към ЦСОЧИ се свързва с факта, че

самостоятелното прилагане на технически мерки не е достатъчно, за да се осигури и поддържа устойчива на риск критична информационна инфраструктура. От друга страна, осигуряването чрез ЕУИ на среда за прилагане на СУСИ и сертифицирането на ЦСОЧИ в съответствие с ISO27001 е измеримо условие и доказателство за всички заинтересовани страни за нивото на защитеност на критичната информационна инфраструктура на централната държавна администрация на Република България.

По тази причина, при разработване на Единните унифицирани изисквания и методиката за тяхното прилагане в ЦСОЧИ, е важно да се отдели значително внимание на процесите за управление на информационната сигурност. В контекста на ЕУИСОЧИ, управлението на сигурността на информацията се разглежда като базов работен процес, който включва следните основни компоненти:

- Технологии и дейности за мониторинг и управление на риска;
- Класификация на информацията и информационните активи;
- Политика за сигурност на информацията - процедури, стандарти, указания;
- Организация на сигурността - обучение, измерване ефективността и непрекъснато подобряване.

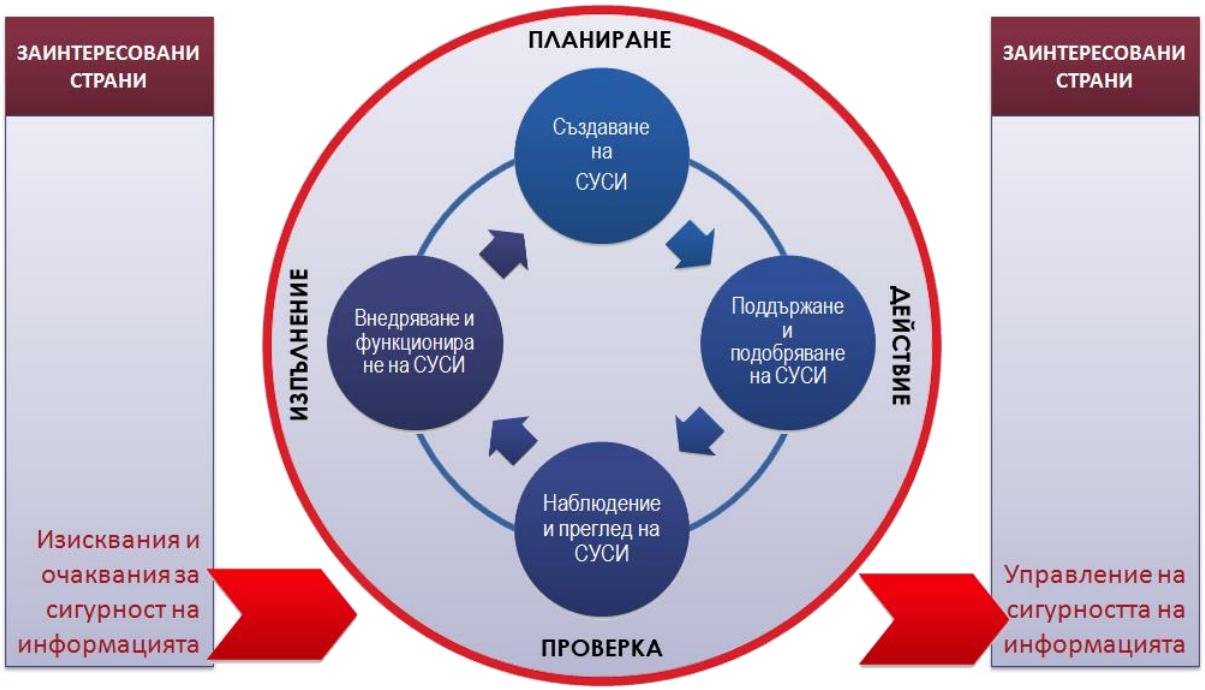
Тези основни компоненти служат като основа на програмата за сигурност, която е необходимо да се разглежда като неразделна част от системата на ЕУИЦСОЧИ. Същността на сигурността и програмата за сигурност е да бъдат защитени специфичната критична информация и (в по-общ план) критичните информационни активи на територията на всеки един ЦСОЧИ. Анализът на риска идентифицира тези активи, открива заплахите, които ги излагат на риск и изчислява (прогнозира) възможните щети и потенциалните загуби, ако тези заплахи се осъществят на практика. Резултатите от анализа на риска подпомагат планирането на дейностите и технологичните средства за осигуряване защитата на идентифицираните активи от релевантните им заплахи и за разработване на приложими политики за сигурност, които да предоставят насоки за дейностите по сигурността. Обучението разпространява тази информация до всеки един служител на ЦСОЧИ, така че всеки да е пълно и навременно информиран и да е в състояние да допринесе за постигане поставените цели по сигурността.

ISO27001 е система от стандарти, като с ISO/IEC27002:2006[30] се очертава важната за ЕУИЦСОЧИ рамка за най-добрите приложими международни правила в управлението на сигурността на информацията и взаимодействието на системите.

На базата на добрите практики за прилагане на ISO/IEC27002:2006[30], като ефективна база за управлението на сигурността на информацията и взаимодействието на системите, могат да бъдат изведени базов модел (фиг.4) и индикативна програма (фиг.5) за разработване и внедряване на СУСИ, като елемент от ЕУИЦСОЧИ.

С версията на ISO/IEC27002:2006 се въвежда т.нар. процесно-ориентиран подход при проектирането и проектиране и развитие на СУСИ, което е съпосочно с развиваната цялостна концепция за ориентирана към процесите защита на критичната

информационна инфраструктура в Европейския контекст, заложен в програмните документи на ENISA[5]в голяма степен.



Фиг.4. Процесно-ориентиран подход при проектирането и проектиране и развитие на СУСИ

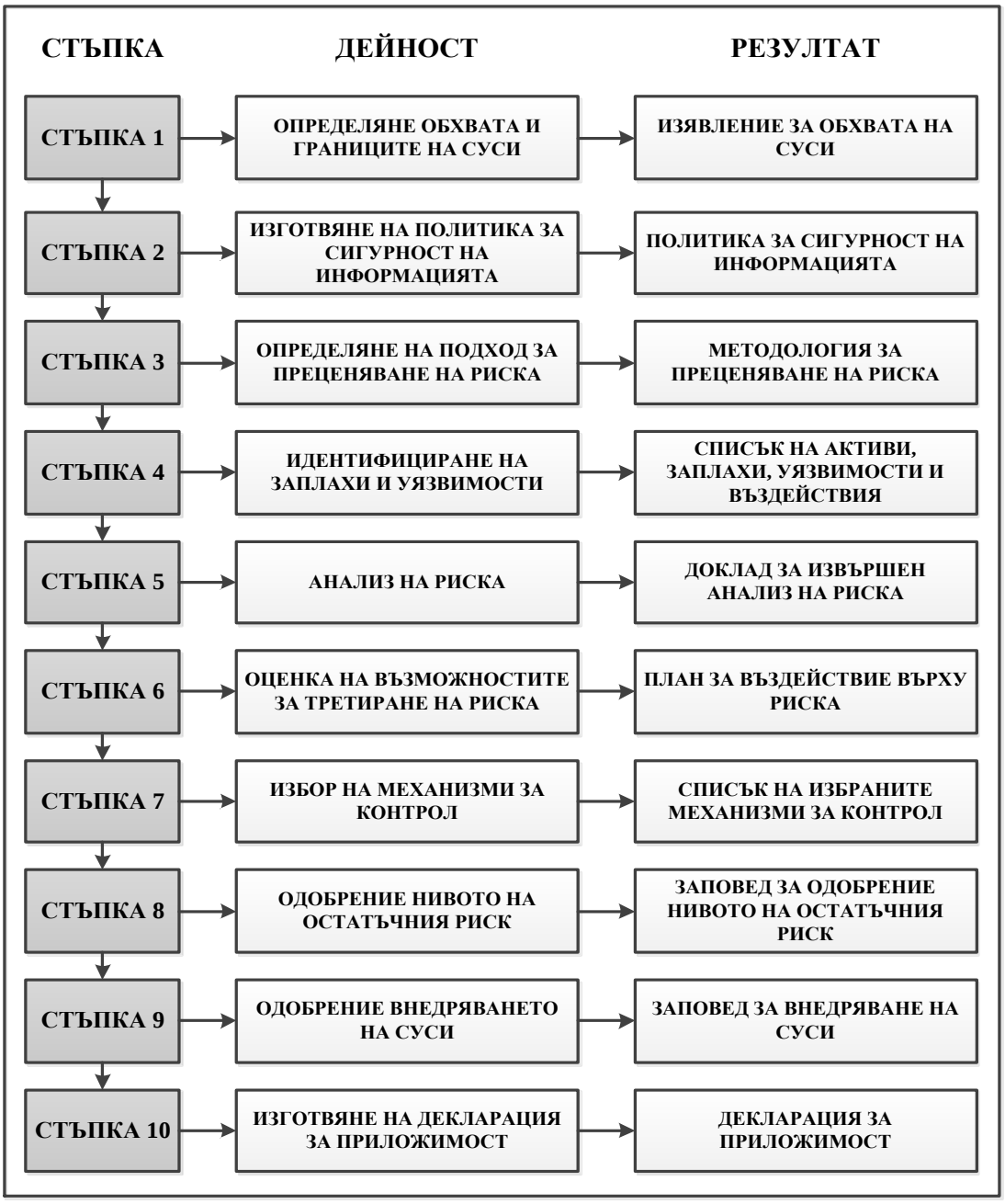
Въведението към ISO27002 описва този модел и посочва как да се прилага в контекста на сигурността на информацията, съгласно Приложение В към ISO27001 се представя и подхода за прилагане на модел, от фиг.4 при разработването на специфична СУСИ[31]. В този смисъл Приложение В към ISO27001 е отправната методическа база за интеграция на моделът и процедурата (фиг.4 и фиг.5) в общата Методика за установяване и поддържане на съответствие с ЕУИЦСОЧИ.

Постигането на процесно-ориентиран подход при проектирането и развитието на СУСИ се свързва с разработването и внедряването на програма за сигурност, съгласно процедурата, представена на фиг.5. Процедурата обхваща и адресира комплекс от аспекти на сигурността – технологични, организационни и аспекти на влиянието на субективния фактор - специфично ниво на компетентност, умения, мотивация и др.

Стъпки 1 и 2 от процедурата са свързани с установяването на обхвата и границите на СУСИ[31], които се дефинират от специфичните характеристики на дадената ЦСОЧИ - мащаб, информационни активи и типове и критичност на информационни системи, класифицирани от гледна точка на функционалност, област на приложение и характеристики (профил) на обслужването, норми, регулации и други специфични изисквания на централната държавна администрация. Добрата практика при провеждане на стъпки 1 и 2 от процедурата (фиг.4) предполага активното участие на управляващия екип на ЦСОЧИ, тъй като тези фази са ключови за успешното имплементиране на СУСИ, като елемент от ЕУИЦСОЧИ.

Стъпки от 3 до 5 са свързани с мониторинга и анализа на рисковете за критичната информационна инфраструктура в дадената организация, като за тази цел

стандарта дава повече свобода за избора на методика, тъй като спецификата на информационните активи и класификацията на рисковия им потенциал ги отличава от широкото разбиране за оценка на риска, т.е необходимо е да се разработи конкретен подход и методология за целите на ЦСОЧИ.



Фиг.5 Процедура на разработване и внедряване на СУСИ

Стъпки 6 и 7 от процедурата дават оценка на възможностите за въздействие на идентифицираните рискове, селектиране на релевантни контроли и определяне на техните цели. Съгласно добрите пратки за прилагане на стандарта за рискове, дефинирани като неприемливи в Методиката за прилагане и поддържане на съответствие с ЕУИ е необходимо да се дефинират механизми за управление на този тип рискове като част от общ план за третиране на риска. Този план включва

прилагането на подходящи механизми за контрол, приемане или трансфериране на рисковете към трети страни. Друга възможност е предприемане на дейности за избягването им. В съответствие с решението как да бъдат третирани рисковете, задължително се избират защитни контроли от описаните в Приложение А на стандарта, като е възможно добавянето и на допълнителни такива с цел адресиране специфични за ЦСОЧИ рискове.

Стъпки 8 и 9 от процедурата (фиг.5) имат отношение към определянето на праговете на остатъчния рисков потенциал. Тези прагове е необходимо да бъдат опредени в Единните унифицирани изисквания, както и съответствието на тези прагове по отношение на класификацията на конкретния ЦСОЧИ като част от критичната информационна инфраструктура. Обикновено тези прагове са отговорност на екипа, управляващ организацията, в която се внедрява СУСИ, но от гледна точка на коректното множество обекти (ЦСОЧИ) е по-ефективно и приложимо праговете на остатъчните рискове да бъдат „изведени" от компетенциите на управляващия екип и да бъдат определени в Единните унифицирани изисквания. По този начин ще се осигури съпоставимост по отношение, както на мерките (технически и организационни), така и на потенциала на рисковете и евентуални щети, чието преодоляване би било свързано с твърде много разходи, в условията на бюджетни и други ограничения, характерни за държавната администрация.

Стъпка 10 от процедурата се отнася до изготвянето на т.нар. Декларация за приложимост[31]. Декларацията за приложимост на СУСИ е част от общата система от контроли за поддържане на съответствие с ЕУИ за всяка конкретна реализация на ЦСОЧИ. Подмножеството на СУСИ контролите е важно да бъдат синхронизирани като цели, причини за избора и обективната възможност за приложение с общите контроли на прилагане на ЕУИ, тъй като информационната сигурност е ключов, но не единствен елемент от системата за осигуряване на ефективна защита на критичната информационна инфраструктура.

От анализа е видно, че взаимодействието ЕУИ – СУСИ на територията на всеки един ЦСОЧИ е ключово за постигане на реална и измерима защита на активите на критичната информационна инфраструктура. От една страна, постигането на съответствие с ЕУИ е необходимо условие за внедряване на СУСИ и сертифициране на конкретния център за постигнато съответствие с ISO27001. От друга страна, въведената в действие СУСИ и сертифицирането съгласно ISO27001 е видимата, разпознаваемата гаранция, че в конкретния ЦСОЧИ е въведен надежден механизъм за мониторинг и контрол и управление на риска в критичната информационна инфраструктура на базата на инвестицията, реализирана при осигуряване за покриване на ЕУИ. Ако в една организация, отговорност на ръководството е да определи допустимото ниво на риск и да планира или не изпълнението на плановете за превенция, то чрез ЕУИ се въвежда за определен клас критична информационна инфраструктура, а именно ЦСОЧИ, единни изходни прагове за допустимото ниво на рисковете, чрез предефиниране на тези прагове (трансформиране) в минимални технически и организационни изисквания. При типичните бизнес-ориентирани приложения на СУСИ (ISO27001) е заложен механизма на оптимизация, т.е дефинирана е задача за линейно програмиране и минимизиране на

целева функция – векторно произведение на вектора на загубите от „консумирани" рискове в информационните активи и вектора на инвестициите за влияние (потискане в определена степен) на съответстващите рискове. В тази логика за сумарно по-малки общи разходи, ръководството може да поема управленския риск за по-малко инвестиции за превенция. При приложения на СУСИ (ISO27001) за критична информационна инфраструктура от клас ЦСОЧИ за Централната държавна администрация, въпреки ограниченията на инвестиционния портфейл, обективно възниква необходимостта от определяне на минималните допустими прагове на рисковия потенциал по отношение на критични информационни активи. В контекста на спецификата на приложението на ISO/IEC27001:2006 при изграждането на центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация, Единните унифицирани изисквания са инструмента за регулиране на минималните прагове на остатъчните рискове от гледна точка на националния интерес и поетите от Република България ангажименти в европейски и международен план. Приложимостта на ISO/IEC27001:2009 може да бъде разглеждана и в контекста на решаването на задачата за определяне на минималния обхват на Единните унифицирани изисквания към ЦСОЧИ. Свободно определяне на обхвата на Единните унифицирани изисквания към ЦСОЧИ е проблем за приложимостта на тези изисквания. Ограничаването на обема на наблюдаваните рискове, до тези, определени чрез ISO27001, е добра практика. В този смисъл, подходът за прилагане на СУСИ, определен чрез ISO27001, може да послужи като отправна точка и определянето на обхвата и дефинирането на Единните унифицирани изисквания към ЦСОЧИ. В клауза 4.2.1[29] Стандартът (ISO27001) урежда, необходимия структурен подход към изграждането на една СУСИ, като за целите на дефиниране на Единните унифицирани изисквания към ЦСОЧИ, особено важен е етапът „Планиране", който включва шест подетапа, които могат да бъдат разглеждани и като обобщение на процедурата, представена на фиг.5:

- Определяне обхвата и границите на СУСИ.
- Определяне на политиката за сигурност на информацията, свързана със СУСИ.
- Определяне подхода за преценяване на риска на организацията и критериите за приемане на риска.
- Идентифициране, анализ и оценка на рисковете.
- Идентифициране и преценка на възможностите за въздействие върху тези рискове, избирайки, където е необходимо, цели по контрола и механизми за контрол, които да бъдат приложени.
- Изготвяне на Декларация за приложимост.

Ако е необходимо да бъдат дефинирани особеностите, които е важно да се отчитат при оценката на приложимостта на този подход, като методическа база за дефиниране на Единните унифицирани изисквания към ЦСОЧИ, то те са в дефиницията на обекта на защита – информацията въобще (СУСИ) и специфичния клас критична информационна инфраструктура – ЦСОЧИ (ЕУИ). И ако СУСИ (ISO27001),

могат да бъдат разглеждани като множество от организационни и технически активности с акцент на организационните, то ЕУИ са по-скоро технически и организационни норми, съответствието, с които гарантира функционирането на критичната информационна инфраструктура от клас ЦСОЧИ с измеримо ниво на риск, наблюдавано, оценявано и управлявано чрез СУСИ (ISO27001).

В потвърждение на това на етапа „Изпълни" стандартът (ISO27001) определя СУСИ като „част от общата система за управление, основана на подхода за риска, свързан с организацията за изграждане, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на сигурността на информацията" [29].

Важно е да се отбележи, че по отношение на дефинирането и въвеждането в действие на Единните унифицирани изисквания към ЦСОЧИ, ISO27001 като стандартизационна практика има алтернативи. В публикациите на NIST и HIPPA могат да бъдат открити редица сходства и по-детайлни трактовки на част от разглежданите проблеми, особено от гледна точка на методическата база на риск-анализа (HIPPA). Но предимството на ISO27001 е не само във факта, че е международно признатия стандарт в областта на защитата на информацията, а и в завършения характер, систематичността и изчерпателността на пакета от стандарти.

4. Сравнителен анализ на конкретни добри практики и развити системи от критерии и изисквания – примерни реализации, сравнения на подходите за прилагане и контрол, анализ на данни за постигнат ефект по отношение на измеримо ниво на защита и оперативна съвместимост на информация.

На оценка по методологията SWOT анализ се подлагат изведените в т.1.2. приложими добри практики на страните членки на ЕС за сходни на обхвата на ЕУИЦСОЧИ съществуващи системи от изисквания, механизмите за прилагането им, както и заложените контролни функции и оценка на ефективността от приложението:

- (1) Разработване в рамките на националните програмни документи на специфични единни изисквания за КИКИ (ЦСОЧИ) за държавната администрация - Таблица2.

Таблица 2. SWOT анализ (1).

SWOT Анализ	Положителни	Отрицателни
Вътрешни фактори ОРГАНИЗАЦИЯТА	**Силни страни (Strengths)**	**Слаби страни (Weaknesses)**
	1. Продължаване на националната традиция и положителен опит. 2. Минимизиране на инвестициите, чрез осигуряване на възможност за базата за надграждане на съществуваща инфраструктура. 3. Постигане на съответствие с действащите национални регулации и законова уредба. 4. Адаптиране на изискванията към установената практика за категоризиране на ЦСОЧИ.	1. Мултиплициране на традиционни практики и политики без доказан позитивен ефект. 2. Отдалечаване от възможността за интеграция в европейските и международни инициативи. 3. Не ефективно категоризиране на КИКИ (ЦСОЧИ). 4. Провеждане и налагане на политики, които обслужват частни, а не обществените интереси.
Външни фактори СРЕДАТА	**Възможности (Opportunities)**	**Заплахи (Treats)**
	1. Постигане на лидерска позиция в прилагането на добри практики за защита на критичната информационна инфраструктура в регионален и европейски мащаб. 2. Развиване на експертен и административен капацитет в областта на защита на КИКИ. 3. Възможност за трансфер на „know how" в регионален, европейски мащаб и привличане на инвестиции за осигуряване на този трансфер чрез механизма на ПЧП. 4. Създаване на условия за задържане в България на млади специалисти в областта на информационните технологии и създаване на дългосрочна перспектива за тяхната реализация в рамките на проекти за внедряване на националните изисквания и консултиране в областта за защита на КИКИ.	1. Капсулиране на национално ниво и отдалечаване от добрите европейски и световни практики за развиване и внедряване на системи и решение за защита на КИКИ на държавната администрация и е-правителството. 2. Несъответствие и необходимост от преработване на изискванията предвид изпълнение на ангажименти, свързани с членството на България в ЕС и други международни спогодби за информационен обмен и защита на критична инфраструктура. 3. Загуба на влияние и авторитет в европейските структури, работещи в областта на защита на КИКИ в резултат на провеждане на независима национална политика в областта.

- (2) Въвеждане на единни унифицирани изисквания към проектирането, техническите решения и програмно осигуряване на обектите и системите на КИКИ (ЦСОЧИ) за държавната администрация, съвместими с международно признатите стандарти от серията ISO27000.

Таблица 3. SWOT анализ (2).

SWOT Анализ	Положителни	Отрицателни
Вътрешни фактори ОРГАНИЗАЦИЯТА	**Силни страни (Strengths)**	**Слаби страни (Weaknesses)**
	1. Разработване на ЕИУ, осигуряващи ефективна интеграция на националната КИКИ в международни структури за информационен обмен с внедрени СУСИ, съгласно ISO27001. 2. Превенция от методологични грешки при определяне на обхвата и съдържанието на ЕУИ към ЦСОЧИ. 3. Постигане на ефективни механизми за мониторинг, превенция и управление на риска за информационните активи на КИКИ. 4. Осигуряване на непрекъснат контрол за съответствие към ЕУИ на базата на разработена и въведена СУСИ за ЦСОЧИ.	1. Механично прилагане на стандарта без отчитане на спецификата на обекта за приложение, националните традиции, добри практики и опит в областта. 2. Изместване на акцента към организационните мерки и риск от неефективно бюджетиране на инвестиционните разходи за защита на КИКИ. 3. Разработване на „документални" ЕУИ, осигуряване на готовност за сертифициране за съответствие с ISO27001, без постигане на измерима степен на защита на КИКИ.
Външни фактори СРЕДАТА	**Възможности (Opportunities)**	**Заплахи (Treats)**
	1. Институционално международно признаване на мерките за защита на КИКИ, когато те са разработени на базата на признат стандарт. 2. Осигуряване на възможност за присъединяване на обекти от националната КИКИ – ЦСОЧИ към международни системи и структури за съхранение, обмен и обработка на особено чувствителна информация (покриване на изискване за въведена СУСИ и сертифициране по ISO27001). 3. Изграждане на доверие и усещане за адекватност към обществения интерес на предприеманите мерки за защита на особено чувствителна информация, съхранявана и обработвана в центровете за данни на държавната администрация и е-правителството. 4. Постигане на международно разпознаваемо ниво на сигурност при предоставянето и оперирането с особено чувствителна информация в рамките на е-правителството и свързаните с него е-услуги.	1. Отклоняване от Европейски политики за мрежова и информационна сигурност и европейската инициатива за защита на КИКИ, доколкото ISO27001 не е единствен източник на добри практики и методическо осигуряване и е с практически еднакъв приоритет с националните стратегии и разработките на ENISA. 2. Формиране на конфликтни точки при дефинирането на ЕУИ към ЦСОЧИ на базата на бизнес-ориентираната логика на стандарта ISO27001 и прилагането му за целите на обслужването на обществения интерес при защита на особено чувствителна информация, съхранявана и обработвана в центровете за данни на държавната администрация и е-правителството. 3. Непълнота в обхвата на ЕУИ към ЦРОЧИ, тъй като ISO27001 е общо приложим стандарт и не отчита особеностите при международния обмен на особено чувствителна информация и стратегическите приоритети в защитата на европейската КИКИ.

- (3) Разработване на методика за въвеждане на единните унифицирани изисквания за съществуващи и новоизграждащи се обекти и системи на КИКИ (ЦСОЧИ).

Таблица 4. SWOT анализ (3).

SWOT Анализ	Положителни	Отрицателни
Вътрешни фактори ОРГАНИЗАЦИЯТА	**Силни страни (Strengths)**	**Слаби страни (Weaknesses)**
	1. Осигуряване на единен стандарт за защита на всички центровете за данни, съхраняващи и/или обработващи особено чувствителната информация в държавната администрация и е-правителството. 2. Устойчиво постигане на очакваните изходни резултати чрез прилагане на единна и универсална методика, независимо от степента на изграденост на ИТ инфраструктурата, обема и обхвата на обработваната информация в центъра за данни. 3. Минимизиране на влиянието на субективния фактор при прилагане на ЕУИ с цел постигане на устойчива защита на КИКИ от клас ЦСОЧИ.	1. Неефективност при прилагането на една и съща обща методика за нови и за вече функциониращи центрове. 2. Риск при провеждането на миграцията към ЕУИ на съществуващи центрове за данни. 3. Неподготвеност и липса на мотивация на субективния фактор при прилагането на ЕУИ.
Външни фактори СРЕДАТА	**Възможности (Opportunities)**	**Заплахи (Treats)**
	1. Катализиране на процеса по въвеждане на национална нормативна уредба за класифициране и етикиране на КИКИ и прилагане на минимални извиквания за защита на критичните информационни активи в съответствие с Резолюция на Съвета от 18 декември 2009г. относно европейски подход на сътрудничество за мрежова и информационна сигурност, рег.№ 2009 / C 321/01. 2. Осигуряване на възможност за ефективен междуведомствен обмен на добри практики за развитието и усъвършенстването на методиката за въвеждане на единните унифицирани изисквания за съществуващи и новоизграждащи се обекти и системи на КИКИ (ЦСОЧИ). 3. Привеждане на вътрешноведомствени политики и/или регулации за защита на КИКИ за съхранение и обработка на особено чувствителна информация в съответствие с ЕУИ и методиката за тяхното прилагане и устойчиво осигуряване във времето.	1. Липса на нормативна уредба, която да регламентира прилагането на ЕУИ по отношение на съществуващи и/или нови ЦСОЧИ. 2. Недефиниран към момента обхват на приложение на ЕУИ за ЦСОЧИ при отсъствието на утвърдена национална класификация и „етикиране" на КИКИ съгласно Резолюция на Съвета от 18 декември 2009г. относно европейски подход на сътрудничество за мрежова и информационна сигурност, рег.№ 2009 / C 321/01. 3. Временна невъзможност за приложение на ЕУИ по отношение на съществуващи и/или нови ЦСОЧИ поради възникнали противоречия или несъответствия с вътрешноведомствени политики и/или регулации за защита на КИКИ за особено чувствителна информация.

- (4) Въвеждане на минимални изисквания за техническите решения и програмно осигуряване, които да се прилагат при конкурсите за избор на изпълнители на обекти и системи на КИКИ (ЦСОЧИ) за държавната администрация.

Таблица 5. SWOT анализ (4).

SWOT Анализ	Положителни	Отрицателни
Вътрешни фактори ОРГАНИЗАЦИЯТА	**Силни страни (Strengths)**	**Слаби страни (Weaknesses)**
	1. Разработване на единни критерии за качество и оперативна съвместимост при избор на технически решения и изпълнителни на дейности (проекти) за изграждане или модернизация на ЦСОЧИ. 2. Ефективно и цялостно дефиниране на обхвата на дейностите при планиране на бюджетите и обявяване на конкурсите за избор на изпълнители на обекти и системи на КИКИ (ЦСОЧИ) за държавната администрация – така че да покриват всички етапи от Методиката за прилагане на ЕУИ, т.е в проектите да не остават не финансирани дейности и по този начин да се повлияе пряко или косвено върху нивото на защита на критичните информационни активи. 3. Защита на бюджетната инвестиция от гледа точна на нейната ефективност по отношение на осигуряване на ЕУИ за ЦСОЧИ.	1. Тъй като ЕУИ е необходимо да отразяват текущото ниво на технологиите за защита на КИКИ, то от гледна точка на ЗОП и свързаните с него регулации, е възможно да се появят противоречия между дефинираните чрез ЕУИ функционални параметри и приложимостта им под формата на минимални технически изисквания при обявяване на обществена поръчка. 2. Пречки при формулирането на част от изискванията на ЕУИ под формата на минимални технически изисквания съгласно ЗОП. 3. Липса на опит и създаване на условия за разработване на методики за оценка на конкурсните предложения, които не осигуряват обективност от гледна точка на действителното съответствие на предлаганото решение (я) към ЕУИ.
Външни фактори СРЕДАТА	**Възможности (Opportunities)**	**Заплахи (Treats)**
	1. Привличане на технологични лидери при за участие в проектите за изграждане и модернизация на ЦСОЧИ – гаранция на качеството на изпълнение на дейностите за постигане на съответствие с ЕУИ. 2. Постигане на ясна и прозрачна комуникационна среда с потенциалните изпълнители, на базата на устойчиви изисквания и очаквания на Възложителя. 3. Възможност за ефективно прилагане на механизма за публикуване на предварителните обявления – предоставяне на възможност във времето на водещите доставчици на решения да подготвят своите предложения, така че в най-голяма степен да удовлетворяват ЕУИ за конкретния ЦСОЧИ.	1. Създаване на условия за обжалване и ненужно удължаване на процедурите за избор на изпълнител на защитената ИТ инфраструктура на ЦСОЧИ, съответстваща на ЕУИ. 2. Обективна възможност за преформулиране на изискванията от гледна точка на законовата регулация, при което да бъдат допуснати до оценяване и изпълнение решения, които да отговорят частично на ЕУИ. 3. Липса на механизъм за ефективен централизиран контрол за прилагането на подобни практики при обявяването на ЗОП за изграждане на защитена КИКИ от клас ЦСОЧИ.

- (5) Разработване на процедура за обмен на информация между ЦСОЧИ и националния офис на CERT, с цел осигуряване на ефективна интеграция с Европейската и глобалната система за защита на критичната информационна инфраструктура.

Таблица 6. SWOT анализ (5).

SWOT Анализ	Положителни	Отрицателни
Вътрешни фактори ОРГАНИЗАЦИЯТА	**Силни страни (Strengths)**	**Слаби страни (Weaknesses)**
	1. Синергия при дейностите на CERT и екипите за обслужване на ЦСОЧИ при осигуряването на ефективна интеграция с Европейската и глобалната система за защита на критичната информационна инфраструктура. 2. Ефективно включване на националния CERT при развитието и усъвършенстването на процедурите за мониторинг и превенция на риска в ЦСОЧИ. 3. Създаване на канали за трансфер на експертно знание от CERT към екипите за обслужване на ЦСОЧИ при управлението на инциденти и минимизиране на негативните последици от рискови събития в условията на вече приложени ЕУИ към ЦСОЧИ.	1. Отсъствие на мотивация и разбиране в екипите за управление и обслужване на ЦСОЧИ за необходимостта от взаимодействие с външни екипи със сходни приоритети и активности (CERT). 2. Недостатъчна оценка на потенциала и резултатите от взаимодействието с CERT в резултата на разбирането, че рапортуването на инцидент е признак за неадекватност на системата за защита на КИКИ. 3. Подценяване на необходимостта от актуална информация за външния рисков потенциал и от там ролята на CERT/CSIR при адаптирането на политиките за превенция като част от ЕУИ към ЦСОЧИ.
Външни фактори СРЕДАТА	**Възможности (Opportunities)**	**Заплахи (Treats)**
	1. Обмен на добри практики между екипите за обслужване на ЦСОЧИ и CERT и при развитието на приоритетите и политиките на CERT/CSIR за засилване на ефективността на превенцията като механизъм за ефективна защита на ИТ инфраструктурата (във всяка приложна сфера) от гледна точка на заявената степен на критичност. 2. Усъвършенстване на организационната структура на CERT чрез прилагане на диференциран подход в зависимост от степента на критичност на информационните активи в организацията. 3. Създаване на специализирани групи в националните CERT, за взаимодействие с обектите на Европейската КИКИ и по-специално с ЦСОЧИ.	1. Отсъствие на мотивация и формална регулация, която да осигури включването на националния CERT в процеса на въвеждане на ЕУИ към ЦСОЧИ. 2. Възникващото противоречие и разминаване в приоритетите между характер на целите и активностите на CERT и ограничената област на приложение на ЕУИ – за ЦСОЧИ. 3. Невъзможност за привличане на ресурси в рамките на CERT за съвместна активност и екипите на ЦСОЧИ поради бюджетни ограничения и свързаните с тях ресурси и планирани дейности.

Резултатите от SWOT анализа потвърждават необходимостта от разработка на ЕУИ към ЦСОЧИ при следните ограничения и особености:

- **(1)** Като изходна база за разработване на ЕУИ за ЦСОЧИ и Методиката за тяхното прилагане се разглеждат:
    - Групата стандарти за информационна сигурност ISO27K;
    - Програмните документи, свързани с Европейската инициатива за защита на критичната информационна инфраструктура;
    - Добрите европейски практики в областта на защита на информацията и информационната инфраструктура, обобщение чрез дейността, мониторинговите доклади и анализи на ENISA;
    - Дългогодишната национална традиция в областта на защита на информацията и постиганите резултати и натрупан опит у нас;
    - Дългосрочната перспектива за изграждане на защита и превенция на риска в общоевропейската критична инфраструктура, неразделна част, от която са и националните КИКИ.

- **(2)** ЕУИ за ЦСОЧИ е необходимо да бъдат разработени така, че да позволяват мащабиране и адаптивно приложение в зависимост от степента на критичност на информационните активи, осигуряващи съхранение и централизирана обработка на особено чувствителна информация. На етапа на оценка на риска към информационните активи е важно бъдат инвентаризирани характерните типове информационни активи с акцент към мащаба, обхвата и съдържанието на чувствителната информация, която се съхранява и/или обработва. По този начин ще се осигури възможност за гъвкаво прилагане на ЕУИ за ЦСОЧИ в зависимост от спецификата на конкретния център, без да се нарушава общата идеология на въвеждането на изискванията и при ефективно управление на бюджетите за постигане на съответствие с тези изисквания.

- **(3)** Паралелно с разработването на ЕУИ за ЦСОЧИ е задължително да протече процес за нормативно регулиране на приложението на тези изисквания. В този процес е необходимо да бъдат включени всички ведомства и структури на държавната администрация от гледна точка на навременното планиране на бюджетите и реалните активности във връзка с въвеждането на ЕУИ за ЦСОЧИ:
    - Инвентаризация и етикиране на КИКИ в държавната администрация;
    - Оценка на рисковия потенциал и избор на модел за прилагане на ЕУСОЧИ за всеки конкретен ЦСОЧИ;
    - Планиране и управление на проектите за модернизация на съществуващите и изграждане на нови ЦСОЧИ в съответствие с ЕУИ:
        - Предварителна оценка и планиране на бюджета за миграция към ЕУИ;
        - Подготовка и обявяване на конкурсите за избор на изпълнител на инженеринговите дейности по миграцията към ЕУИ;

        - Организационно и кадрово преструктуриране и осигуряване на етикираните ЦСОЧИ;
        - Изпълнение на проектите за миграция и привеждане в съответствие с ЕУИ;
        - Поддържане на съответствието с ЕУИ в среда на развитие на услугите и обмена обработвана чувствителна информация от конкретния център.
    - Установяване на междуведомствено координационно звено за методическо подпомагане, мониторинг и контрол на въвеждането и поддържането на съответствие с ЕУИ за ЦСОЧИ. Това звено може да изпълнява и представителни функции по отношение на изпълнението на националните ангажименти за включване в Европейската инициатива за защита на критичната информационна инфраструктура и участие в работни групи на очакваната нова Агенция (наследник на ENISA), която ще координира общоевропейските действия по отношение на CIIP.

- **(4)** Ключов въпрос при осигуряване на измерим ефект от въвеждането на ЕУИ за ЦСОЧИ е методическото и кадрово осигуряване на процеса на миграция на КИКИ към ЕУИ. Методическото и кадрово осигуряване на процеса на миграция имат роля при конкретното адаптиране на ЕУИ към мащаба, структурата и профилите на обработка на особено чувствителната информация за всеки център. ЕУИ малко или много представят един обобщен възглед по въпроса за постигане на измеримо и прогнозируемо ниво на риска в КИКИ. Обучението на екипите, които ще въвеждат ЕУИ за ЦСОЧИ и, особено, ефективното комуникиране с тези екипи на методическите аспекти на процеса, ще играе ключова роля, както при успешното сертифициране на центовете от гледна точка на ISO27001, така и за ежедневното практическо поддържане на съответствието чрез механизмите на СУСИ и процедурите за мониторинг и контрол от Методиката за въвеждане на ЕУИ.

- **(5)** В съдържанието на Указанието за прилагане на ЕУИ за ЦСОЧИ е важно да бъде включен раздел за прилагане на минималните изисквания по отношение на технологията и решенията за защита на КИКИ при обявяване на конкурсите за избор на доставчици/изпълнители. От гледна точка на опита у нас, като и практиките в останалите страни-членки, се вижда, че при по-голямата част от случаите са приложими т.нар. специални обществени поръчки или двуфазни конкурси с предварителна селекция. От друга страна, поради интегрирания характер на мерките за защита на КИКИ, е важно правилно да бъде дефиниран обекта на конкурса, като добрите практики сочат, че за такъв тип обекти е характерно да се възлага изпълнение под формата на инженеринг (проектиране, доставка, изпълнение, обучение, гаранционно и следгаранционно обслужване).

Разработването на ЕУИ за ЦСОЧИ не е изолиран процес и е необходимо да се разглежда като стъпка в разработването на национална стратегия за защита на КИКИ в контекста на Европейската CIIP инициатива. В този смисъл при разработването на изискванията е важно да бъде разгледан контекста на тяхната бъдеща интеграция в националната CIIP стратегия. Въпреки, че този подход – отдолу-нагоре е характерен за по-малко държави от ЕС (Германия, Естония), то се вижда, че в точно тези държави са постигани най-съществени резултати и се сочат като добри примери по отношение на постигане на целите на CIIP инициативата. В този смисъл, с въвеждането на ЕУИ за ЦСОЧИ, е необходимо да бъдат преминати и част от по-глобалните активности, свързани с избора на подход за етикиране на КИКИ (CIIP) в нашите условия и специфики, тъй като ЦСОЧИ са част от КИКИ и, ако за тях бъде приложена изолирана система от правила за класифициране на рисковия потенциал, то на по-късен етап всяко едно „преетикиране" ще доведе до необходимост от преработка на документалната база за внедряване на ЕУИ за ЦСОЧИ. От друга страна, с разработването на ЕУИ за ЦСОЧИ ще се даде практическа насока и ще се визуализира взаимодействието „CIIP – ISO27K". В приоритетите на CIIP този въпрос е ключов и неговото практическо решаване ще очертае пътя на синергията на CIIP и ISO27K действията. Както вече беше разгледано в т.1.3., този въпрос изисква детайлен анализ и очертаване на зоните на „припокриване" и зоните за взаимодействие, но без практическо апробиране, избора на успешна политика за синергия, е невъзможен. В този смисъл, разработването и въвеждането на ЕУИ за ЦСОЧИ с основание може да се разглежда като подготвителна (пилотна) фаза от процеса за разработване на национална Стратегия и план за действие във връзка с Европейката CIIP инициатива.

От друга страна обзорът на добрите европейски практики при разработването на ЕУИ за ЦСОЧИ е необходимо да бъде разгледан и в контекста на проблемите, свързани със защита на личните данни при поддържане и предоставяне на е-услуги. Този контекст е съществен, тъй като личните данни, тяхното „събиране", съхранение, обработка и обмен попадат директно в обхвата на класа информационни обекти - особено чувствителна информация (ОЧИ).

Анализирането на ефективните методи и подходи за защита на личните данни в средата на напрекъснато развиващ се и разширяващ се обхват на електонните услуги, предоставяни от държавата администрация и частни регистрирани оператори на лични данни, е във фокуса на дейностите на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA), съгласно чл.4 от Регламент ЕС No 460/2004 [4]. Съгласно разпоредбите на чл.4 Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) има приоритетна област на активност за организацията за дейностите, мониторинг и осигуряване изпълнението на ДИРЕКТИВА 2002/21/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 7 март 2002 година относно общата регулаторна рамка за електронните съобщителни мрежи и услуги[32]. В тази връзка Техническия комитет на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA), създаде работна група в тази приоритетна област, която взема дейно участие при разработка на допълнението към ДИРЕКТИВА 2002/21/ЕО, а именно ДИРЕКТИВА 2009/136/ЕО на Европейския парламент и на Съвета от

25 ноември 2009 година за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите[33]. В тази връзка Техническия комитет на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) разработи и представи на страните-членки и два програмни документа:

1. Обзорен доклад за оценка на необходимостта от въвеждане на Общоевропейска система за уведомяване при нарушения по отношение на съхранението, предавнето и досъпа до лични данни [34] – май 2011.

2. Изследване на добрите практики за събиране и съхраняване на данни в ЕС [35] – февруари 2012

В обзорният доклад[34] е проучен и представен опита при осигуряването на непрекъсната верига и процес на защита на личните данни в информатионните системи и електронните услуги във всички държави-членки на ЕС, Норвегия, Турция и САЩ, като са изведени два основни приоритета или т.н. приоритетни зони за действие при осигуряването на ефективна защита на личните данни:

-*Публична приоритетна зон*а (privacy front office) - развита в зоната за отговорност на публичните телекомункационни оператори и мрежите са обмен на данни на държавните администрации;

-*Вътрешна зона* (privacy back office) – разгледана в контекста на критичната информационна инфраструктура за съхранение и постобработка на лични данни, т.е от гледна точка на настоящия обзор във втората приоритетна зона попадат и ЕУИ за ЦСОЧИ.

По отношение на избора на мерки и подходи за защита на „вътрешната зона“ в доклада се прави обобщението на базата на обзора на добрите практики, че адекватността на прилаганите мерки е задължително да се верифицира чрез анализ на рисковете и ефективна оценка на рисковия потенциал на базата на 4 базови критерия:

- Броя на засегнатите хора при загуба или неправомерен достъп;
- Естество на данни, които биха попаднали в обхвата на нарушението (финансови, здравеопазване, национална сигурност и т.н.);
- Характера на нарушението (планирана, систематична атака, или изолиран инцидент);
- Моментното ниво на защита (резервираност, физическа защита, криптиране).

По-конкретни препоръки във връзка със съхранеието на чувствителна информация, носители, резервираност, процедури, брой копия и архивиране са представени в Изледването на добрите практики за събиране и съхраняване на данни в ЕС[35] на Техническия комитет на Европейската Агенция за Мрежова и Информационна

Сигурност (ENISA). Изследването [35] е направено на базата на опита в страните-членки на ЕС, Австралия, Канада и САЩ. В т.5.2.4.2 от изследването[35] е направен детайлен анализ на проблемите, свързани със сроковете за съхранение на чувствителната информация, като ясно е определена добрата практика за диференциране на срока, в зависимост от съдържанието на информацията. Ясно са очертани недостатъците на т.нар. „плоска“ схема за срокове за съхранение (един срок независимо от типа и характера на информацията), като се показва, че срокът за съхранение е задължителна функция на система от външни регулации, имащи отношение към съдържнието на информацията и свързаните със съдържанието потенциални последици от „просрочване“ и последващо използване. В изследването са определени и препоръчителни и задължителни (регулаторно определени) срокове за съхранение и/или актуализиране на характерни типове информация, като например:

- До 30 дни за видеоинформация, придобита от камери за обзорно (охранително) наблюдение на зони с публичен достъп;
- До 6 месеца за данни, свързани със регистрирано присъствие на лице в публично учреждение, хотел, транспортно средство за превоз на пътници и т.н.
- До 12 месеца за информация, която съдържа преки или косвени доказателства за извършено престъпление.

Ясно се подчертава, че ако има регулаторни условия определен тип лични данни да се съхраняват трайно за по-дълго време от указаните срокове, то добрите практики предполагат разработване на публичен регистър на операторите, процедура за сертифициране и одитиране на мерките за защита и достъп до личните данни. В доклада се дава информация и оценка, че България е страна с положителен опит в това направление, като препоръките за всички „нови“ страни-членки е да насочат усилията в техническото осигуряване на процесите и процедурите, тъй като регулаторно изискванията са покрити.

В изследването[35] се прави и анализа на отношението между обема на регисираните лични данни, механизмите за съхранение и времето за съхранение, като това отношение се поставя и в контекста на необходимостта при различни стуктурни отношения да се прилагат диференцирани организационни и технически мерки за защита на информацията.

За групата държави, попадащи в обхвата на проучването е представена интересна съпоставка между Минимален Обем лични данни при заявяване на електронна услуга (Таблица 2[35]) и времето за съхранение на Данни за трафика (регистрираните номера на МПС, списъци с пътниците, тахографска информация и т.н. – Таблица 3[35]). Наблюдава се тендецията, че в държави с висок рисков потенциал като Ирландия се регистрира по-голям обем лични данни при заявка за електронна услуга (в т.ч. и актуален адрес на местоживеене) и две годишен период за съхранение на данните от системите за мониторинг и регистрация на трафика и пътникопотока. В това отношение България е посочена като страна с балансирана политика, както по отношение на

значителното ограничаване на обема на личните данни, необходими за представяне на електронни услуги, така и прилагане на най-често срещания срок за съхранение на трафични данни - до една година.

В заключение в изследването [35] след обобщаване на добрите практики се правят шест основни препоръки към страните-членки на ЕС, в т.ч. и към България[35]:

Препоръка 1. Националните органи за защита на личните данни в координацията на Работната група за защита на данните към ЕС да дефинират ясни насоки за прилагане на мерки за защита на информацията към администраторите на лични данни, чрез балансиране на интересите на риск във всеки конкретен контекст и технология, като се вземат предвид особеностите на националните законодателства.

Препоръка 2. Практическото приложение на принципите за минимизиране на данните и на опазване в конкретни случаи от страна на администраторите на лични данни, трябва да бъдат оценени (например под формата на одити) и да бъдат определени ясни санкции и механизми за прилагането им в случаи на нарушения.

Препоръка 3. На европейско равнище да се създаде Европейският надзорен орган по защита на данните, който съвместно с Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) да разработи ясни насоки относно специфични области на обработката на лични данни с общоевропейско въздействие, и по-специално относно тълкуването на принципите за минимизиране на данните и тяхната защита, отнасящи се до събирането и съхранението на лични данни.

Препоръка 4. Като се има предвид факта, че събирането и съхранението на лични данни не винаги е регулирана само от законодателството за защита на данните, държавите-членки следва да предприемат действия за установяване и премахване на противоречиви регулаторни разпоредби, отнасящи се до събирането и съхранението на лични данни.

Препоръка 5. Европейската комисия да гарантира, че всички разпоредби в бъдещите европейски правни инструменти във връзка със защита на данни ще са съгласувани и целенасочени към минимизиране на рисковете при предоставяне на електронни услуги.

Препоръка 6. Националните органи за защита на данните трябва да работят за подобряване на осведомеността на потребителите относно техните права, произтичащи от законодателството за защита на данните, както и за възможностите, които им се предлагат от правната система, за да упражняват тези права.

Дадените в Изследването на Техническият комитет на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA)[35] препоръки са приоритетно с организационен характер и от тях не произтичат пряко технически мерки и ограничения. Видима е тенденцията за унификация и непрекъснатост на процеса за защита на чувствителната информация в Европейското информационно пространство и България е необходимо да бъде активна в този процес, за да се избегне изоставане и невъзможност за достъп до общоевропейски електронни услуги поради несъответствие или не достатъчна степен на защита на националните информационни ресурси, част от общата Европейска критична информационна инфрастуктура.

На базата на обзора на добрите практики може да бъде направено заключение, че разработването на ЕУИ за ЦСОЧИ в този конкретен момент и от гледна точка на националната специфика, традиция и натрупания опит, е навременно и в синхрон с очакванията и ангажиментите, поети към нашите европейски партньори. Процеса на въвеждане на ЕУИ за ЦСОЧИ у нас ще има смисъла на миграция към единна система изисквания, което означава, че и до този момент към ЦСОЧИ са осигурени и се осигуряват ефективни мерки за защита на критичните информационни активи, но е необходимо те да бъдат стандартизирани технологично и методически, като подход и процедурите за мониторинг и поддържане на съответствието.

От гледна точка на интеграция на българската критична информационна инфраструктура в европейското CIIP пространство, е важно, разработените ЕУИ за ЦСОЧИ да бъдат представени и визуализирани пред европейските партньори по подходящ начин и чрез верифицирането им в средата на международно призната стандартизационна практика в областта на защитата на информацията – серията стандарти ISO27001. Това ще осигури ефективно участие на всеки един обект или структурна единица от национална критична инфраструктура в общоевропейски проекти за информационен обмен на чувствителна информация, без да се налага вторично одитиране и допълнителен мониторинг от проектните контролни органи. Така ще се утвърди авторитета и престижа на България като една от водещите държави-членки в областта на прилагане на информационните технологии в държавното управление и развитие на е-правителството, на базата на информационна инфраструктура, измеримо защитена от рискове.

Разработването и въвеждането на ЕУИ за ЦСОЧИ ще демонстрира и готовността, и мотивацията, и разбирането да се въвеждат единни национални ИТ стандарти за държавната администрация, тъй като през последните 10 години са се наблюдавали и прояви на „затваряне” на ниво ведомство и провеждане на независими политики в контекста на извеждане на определени специфики на ведомственото информационно обслужване, които правят неприложими единните национални стандарти. Целта е с разработването на ЕУИ за ЦСОЧИ да се постигне такава степен на адаптивност и гъвкавост, която да осигури приложимост, независимо от „традиционните” пречки по отношение на ведомствени специфики. Това е обусловено от заложената в ЕУИ за ЦСОЧИ идея за одитиране на критичните информационни активи и въвеждане на единна система за класифициране в зависимост от степента на риска при съхранение, обработка или достъп до особено чувствителна информация. Този подход със сигурност е универсален (опита на Естония и Германия го показва). Прилагането на единна схема за етикиране на критичните информационни активи, съобразена с CIIP дефинициите, ще осигури необходимата дълбочина и универсалност при приложението на ЕУИ за ЦСОЧИ.

Библиографска справка:

1. Официална публикация на Европейската комисия, до Европейския парламент и Икономическия и социалния комитет и Комитета на регионите, представяща основите на общоевропейския подход при осигуряването на мрежова и информационна сигурност: http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf;
2. Официална публикация на Европейската комисия, до Европейския парламент и Икономическия и социалния комитет и Комитета на регионите, относно защитата на критичната информационна инфраструктура: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:BG:PDF;
3. Официална публикация на Европейската комисия, до Европейския парламент и Икономическия и социалния комитет и Комитета на регионите, относно защитата на критичната информационна инфраструктура срещу широко мащабни кибер-атаки: http://ec.europa.eu/information_society/policy/nis/docs/comm_2011/comm_163_en.pdf;
4. РЕГЛАМЕНТ (ЕО) № 460/2004 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА НА ЕВРОПА за създаване на Европейска агенция за мрежова и информационна сигурност: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:EN:PDF;
5. Доклад на Европейската Агенция за Мрежова и Информационна Сигурност (ЕАМИС) за „Посоката на националните усилия за укрепване на сигурността в киберпространството”: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport;
6. Кибернетичната сигурност СТРАТЕГИЯ НА ЧЕШКАТА РЕПУБЛИКА за периода 2011 – 2015 **:** http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF;
7. Стратегия за информационна сигурност, разработена от Комитета по информационна сигурност на Министерството на отбраната на Естония : http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf;
8. РЕЗОЛЮЦИЯ НА ФИНЛАНДСКОТО ПРАВИТЕЛСТВОТО ЗА НАЦИОНАЛНА СТРАТЕГИЯ ЗА ИНФОРМАЦИОННА СИГУРНОСТ **:** http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20periaatep%C3%A4%C3%A4t%C3%B6s%20kansallisek si%20tietoturvastrategiaksi%20%28su/ru/eng%20LVM62/2008%29;
9. Стратегия на Франция, разработена от Националната агенция за сигурност на информационните системи **:** http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011;
10. Стратегия на Германия за информационна сигурност : http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1;
11. Програма за развитие на електронна информационна сигурност на **Литва**: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf;
12. Национална стратегия за кибер сигурност на **Люксенбург**: http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf (in French);

13. Националната стратегия за сигурност на информационното пространство на **Холандия**: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011;
14. Стратегия за информационна сигурност на **Англия**: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf;
15. Международната стратегия за киберпространството **на САЩ:** http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf;
16. РЕЗОЛЮЦИЯ НА СЪВЕТА от 18 декември 2009 г. За европейския подход на сътрудничество за мрежова и информационна сигурност: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF;
17. ДИРЕКТИВА 2008/114/ЕО НА СЪВЕТА от 8 декември 2008 година относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:BG:PDF;
18. РЕЗОЛЮЦИЯ НА СЪВЕТА от 18 декември 2009 година относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:BG:PDF;
19. Федералния план за киберсигурността и информационно осигуряване – изследвания и развитие: http://www.cyber.st.dhs.gov/docs/Federal%20R&D%20Plan%202006.pdf;
20. Документален, интернет базиран архив, на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) с годишни доклади за напредъка на страните-членки в областта на мрежовата и информационната сигурност: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/;
21. Обзорен доклад за дейността на центъра за реагиране при компютърни инциденти (CERT), разработен от експерта група на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA). Inventory of CERT activities in Europe Publicly listed teams, co-operation, support and standardisation activities, ENISA, Version 2.7, May2012.
22. Практическо указание за прилагане на система от правила за оценка на риска: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf;
23. Система от правила, прилагана във фармацевтичната индустрия: The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
24. "Информационни системи. Заплахи и добри практики в информационната сигурност във Франция '2008": http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008-en.pdf;
25. Годишен доклад за на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) за напредъка на България в дейностите, свързани с осигуряването на информационната сигурност за 2010 година, публикуван през месец май 2011 година: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Bulgaria.pdf;

26. ОБЩА СТРАТЕГИЯ ЗА ЕЛЕКТРОННО УПРАВЛЕНИЕ В РЕПУБЛИКА БЪЛГАРИЯ 2011-2015 http://www.strategy.bg/FileHandler.ashx?fileId=1351;
27. Национална програма за ускорено развитие на информационното общество в Република България (2008-2010г.) http://www.mtitc.government.bg/page.php?category=492&id=3585;
28. Годишен доклад на Европейската Агенция за Мрежова и Информационна Сигурност (ENISA) за напредъка на България в дейностите, свързани с осигуряването на информационната сигурност за 2010 година, публикуван през месец май 2011 година: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Bulgaria.pdf;
29. БДС ISO/IEC27001:2006. Българският институт за стандартизация, 2008. Приложение А, стр. 5; http://www.bds-bg.org/standard/info.php?standard_id=34103;
30. Добри практики на работната група на Британския институт по стандарти - прилагането на стандарта за информационна сигурност и спецификата при разработването на системи за управление на информационната сигурност: Information Security ISO/IEC27001 - WLA - Frequently Asked Questions. British Standards Institution. bsi-emea.com - 18.06.2010 < http://www.bsi-emea.com>;
31. БДС ISO/IEC27001:2006. Българският институт за стандартизация, 2008. Приложение В, с. 37: http://www.bds-bg.org/standard/info.php?standard_id=34103.
32. ДИРЕКТИВА 2002/21/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 7 март 2002 година относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива) - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:35:32002L0021:BG:PDF;
33. Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:BG:HTML
34. Обзорен доклад за оценка на необходимостта от въвеждане на Общоевропейска система за уведомяване при нарушения при съхранението, предаването и досъпа до лични данни http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn/at_download/fullReport;
35. Изследване на добрите практики за събиране и съхраняване на данни в ЕС http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection/at_download/fullReport