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

ЕДИННИ ДЪРЖАВНИ 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

АИС	**Автоматизирани информационни системи**
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**
ИО	**Информационно обслужване**
ИТ	**Информационни технологии**
КИИ	**Критични информационни инфраструктури**
КИКИ	**Критична информационна и комуникационна инфраструктура**
НКПД	**Национален класификатор на професиите и длъжностите**
ОЧИ	**Особено чувствителна информация**
ЗОП	**Закон за обществените поръчки**
ПЧП	**Публично частно партньорство**
СУСИ	**Система за управление на информационната сигурност**
ЦСОЧИ	**Център за съхранение на особено чувствителна информация**
ЦДА	**Централна държавна администрация**
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**
IETF	**Internet Engineering Task Force**
OASIS	**Organization for the Advancement of Structured Information Standards**

1. Анализ на текущото състояние на системите и технологии, прилагани с цел защита на информацията и осигуряване на оперативна съвместимост в центровете за съхранение на особено чувствителна информация на държавна администрация в Република България.

В редица национални нормативни документи в последните 3 години е поставен акцент на проблемите за защита на информацията и информационната инфраструктура в контекста на осигуряване на оперативна съвместимост на ниво данни и приложения, както в национален, така и в европейски план.

Възникващата необходимост от единна национална и съвместима с добрите европейски практики политика за осигуряване на стабилната и непрекъсната работа на електронното управление и информационните системи на централната държавна администрация (ЦДА), намиращи се в експлоатация, се очертава от факта, че към настоящия момент не са дефинирани унифицирани изисквания към центровете за съхранение на особено чувствителна информация, обслужващи ЦДА на Р България, в съответствие със система от критерии за оперативна съвместимост и информационна сигурност на национално и общностно ниво. В настоящият момент процесите на надеждната и безотказна работа на информационните системи на ЦДА, намиращи се в експлоатация, са в пряка зависимост от информационните технологии и в непряка зависимост от ИТ инфраструктурата, изискват безотказност и непрекъсваемост на работата на информационните системи.

Практиката при експлоатация на центровете за съхранение на особено чувствителна информация на ЦДА и предоставянето на административни услуги на гражданите потвърждават относително голямата вероятност и честота на проявление на рискове от срив на системите за електронна обработка на информация, а именно:

- Нарушаване работата на организационната структура като цяло;
- Зависимост от дейността на други организации, свързани с основната дейност на центровете, свързани с нарушаване работата на ИТ оборудването;
- Нарушено обслужване на гражданите;
- Възможни искове за щети, което ще доведе до нови разходи;
- Намаляване на продуктивността, както и прекъсване на цели процеси;
- Създаване на негативен имидж на администрацията, предоставяща услуги на гражданите.

В такава среда всяко ведомство или обособена организационна единица на ЦДА е необходимо да предприема действия за намаляване на тези рискове. В зависимост от компетентността на екипите на съответното ведомство и управленските приоритети се предприемат действия за превенция в посока защита на центровете за съхранение на особено чувствителна информация в съответствие с вътрешноведомствените политики за мрежова и информационна сигурност. Но тъй като електронното управление и е-правителството предполагат интензивен информационен обмен между ведомствата и обособените организационни единици на ЦДА, въвеждането на специфични вътрешно ведомствени системи влияе върху възможностите за ефективен обмен на данни и развиването на общи за ЦДА политики за достъп и защита на информация във всяка

фаза от жизнения й цикъл: създаване, временно съхранение, оперативен достъп, предаване, дълготрайно съхраняване и архивиране.

От друга страна, за целевите групи участници в електронното държавно управление и потребителите на е-правителството, усещането за достъпност на услугите се формира от конкретните проявления на изброените рискове, ограничавани и управлявани по вътрешноведомствени политики и правила, които не са унифицирани, т.е. оперативна съвместимост и информационна сигурност по отношение на центровете за съхранение на особено чувствителна информация в ЦДА не е осигурена като интегриран и непрекъснат процес.

От трета страна, по силата на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност ИТ отделите и структурите на ЦДА са предприели определени мерки за физическа защита на информационните системи, защитата им от природни бедствия и пожари, за да се гарантира безотказно действие, съхранение и/или предаване на данни и услуги, свързани с тези мрежи и системи. Анализът на тези мерки, адаптирането на вече създадената инфраструктура към системата от унифицирани изисквания, са важен елемент за ефективността на включването на вече направените инвестиции в цялостния инвестиционен процес, съпътстващ постигането на изискваното ниво на оперативна съвместимост и информационна сигурност на центровете за съхранение на особено чувствителна информация, обслужващи ЦДА.

В резултат на пълноправното ни членство в ЕС, България има ангажименти да прилага регулациите и да изпълнява целите и изискванията, определени с 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. Съгласно тази Директива подмножество на Европейската критична инфраструктура е Европейската информационна критична инфраструктура, за защитата на която се доразвива чрез програмния документ - 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 широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“, рег.№ COM(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.

Защитата на информацията и осигуряване на оперативна съвместимост в центровете за съхранение на особено чувствителна информация на държавна администрация в Република България се развива като процес в съответствие с Общата стратегия за електронно управление 2011-2015 г. (Раздел 6.Технологичен модел). В тази стратегия са намерили отражение както разгледаните вече програмни документи, така и Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество за мрежова и информационна сигурност (рег.№ 2009 / C 321/01) и 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).

Представеният в Раздел 6 на Стратегията Технологичен модел на Електронното управление, обобщава натрупания положителен опит у нас в областта на експлоатационната сигурност и защитата на критичната информационна инфраструктура на държавната администрация и определя двата основни принципа, които са основата и дефинират необходимостта от разработването на Система от Единни държавни изисквания при разработването и въвеждането на системи и технологии за защита на информацията и осигуряване на оперативна съвместимост на центрове за съхранение на особено чувствителна информация на централна държавна администрация, а именно:

- **Технологичен неутралитет** (Раздел 6. т.6.5 от Стратегията)[1], с който се определя, че системите и решенията за електронно управление трябва да отговарят на утвърдени международни стандарти и да са максимално независими от конкретни операционни системи, платформи, технологии, софтуер и доставчици. Такива стандарти в областта на електронното управление, съгласно цитирания раздел от Стратегията се разработват от редица международни организации, сред които са:
  - International Organization for Standardization (ISO);
  - Internet Engineering Task Force (IETF)
  - United Nations Centre for Trade Facilitation and Electronic Business;
  - Organization for the Advancement of Structured Information Standards (OASIS);
  - World Wide Web Consortium и др.

- **Стандартизация** (Раздел 6. т.6.6. от Стратегията)[1] – този принцип, заложен в Стратегията, определя и ключовата за въвеждането на Системата от Единни държавни изисквания при разработването и въвеждането на системи и технологии за защита на информацията и осигуряване на оперативна съвместимост на центрове за съхранение на особено чувствителна информация позиция на държава, че е необходимо „…въвеждане на стандартизация по отношение на доставката, разработката и поддръжката на софтуерни решения. Трябва да се въведе системен подход, гарантиращ високото качество на информационните решения и регламентиращ минималните изисквания във всяка една фаза при извършване на доставка или разработка на софтуер”[1]. На практика с т.6.6 от стратегията се поставя задачата за разработването на настоящата Система от критерии.

В Общата стратегия[1] ясно е определена ролята на стандартизацията като „…основна предпоставка за многократното използване на наличните технологии, решения и знания (инфраструктура, приложения, решения, лицензи и технологични средства), както и се определя необходимостта от приложимост и целта на ново създаващите се национални изисквани и регулации, не само за предстоящите за изграждане обекти на Критичната информационна и комуникационна инфраструктура

(КИКИ), а и за увеличаване на „…стабилността и зрелостта на съществуващите решения", което да доведе до ефективно и дългосрочно усвояване на вече направените инвестиции, както до значително намаляване на експлоатационните разходи и разходите за поддръжка и обслужване.

Текущото състояние на системите и технологиите са прилагани с цел защита на информацията и осигуряване на оперативна съвместимост в центровете за съхранение на особено чувствителна информация на държавна администрация в Република България, отразява характерната тенденция да се търси унификация и приемственост на прилаганите решения, като се залага на утвърдени и световно признати производители и доставчици на оборудване и системни интегратори с опит при въвеждането в експлоатация на критични информационни активи. Всички разработени в последните 5 години програмни документи потвърждават волята за прилагане на вече разгледаните два принципа за технологичен неутралитет и стандартизация. Пример за това е и Националната програма за ускорено развитие на Информационното общество в Република България[2]. Чрез тази програма се дефинира устойчивата национална традиция и оперативната рамка на българския модел на ИО в технологичен, икономически и социален план. Чрез програмата ясно се определя необходимостта от анализ (в т.ч. риск анализ) на процеса на конвергенцията на информационните и комуникационни технологии (ИКТ) до постигане на единна, устойчива на рискове, непрекъсната среда за обмен на електронното съдържание и предоставяне на електронни услуги. В този контекст са и част от дефинираните в Програмата оперативни цели, насочени пряко към КИКИ, работеща за целите на държавната администрация:

- **Пълна съвместимост с политиката на Европейския съюз;**
- **Интегриране на националните ИКТ ресурси;**
- **Сигурност на мрежите и информацията**, като тук специален акцент е поставен на необходимостта да се прилагат „…система от норми, санкции и ресурси за осигуряване безопасност на данните и ИКТ системите. Всички усилия осъществявани в областта на ИО трябва да следват утвърдени принципи и стандарти за сигурност и да не създават предпоставки и условия за компрометиране и уязвимост на свои и чужди данни. Това включва: електронни подписи и електронни документи, защита на данните, защита от кибер престъпления, защита на интелектуалната собственост, регулиране на интернет съдържанието, защита на потребителите".

Въвеждането на Единни държавни изисквания за защита на критичните информационни активи и осигуряване на оперативна съвместимост на центрове за съхранение на особено чувствителна информация на централна администрация е ключов етап от изпълнението на Общата стратегия за електронно управление 2011-2015. Чрез този етап се осигурява постигането и поддържането на оперативно съвместима и устойчива на рискове информационна инфраструктура на електронното управление в Република България.

2. Обхват, област на приложение и приоритети при разработването на Единните държавни изисквания към центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация.

2.1. Дефиниции

Особено чувствителна информация (ОЧИ) - информация, която като съдържание и области на приложение попада в обхвата и регулаторната рамка на:

- ДИРЕКТИВА 95/46/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ОТ 24 ОКТОМВРИ 1995 ГОДИНА ЗА ЗАЩИТА НА ФИЗИЧЕСКИТЕ ЛИЦА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ И ЗА СВОБОДНОТО ДВИЖЕНИЕ НА ТЕЗИ ДАННИ[4];
- РАМКОВО РЕШЕНИЕ 2008/977/ПВР НА СЪВЕТА от 27 ноември 2008 година относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателно-правни въпроси[5];
- ДИРЕКТИВА 2006/24/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО[7];
- Чл.2.(г) от 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[9] – чувствителна информация във връзка с критичната европейска инфраструктура;
- ЗАКОН за защита на класифицираната информация[3];
- ЗАКОН за защита на личните данни[8];
- Наредба за задължителните общи условия за сигурността на автоматизираните системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация[12].

Критична информационна и комуникационна инфраструктура (КИКИ)[10] – обособена част от ИКТ системи, услуги, мрежи и инфраструктури (накратко ИКИ), които формират или обслужват жизнено важна част от европейската икономика и общество, като или предоставят съществени продукти и услуги, или представляват основната платформа за други критични инфраструктури. Този тип КИК се определят за критични информационни и комуникационни инфраструктури (КИКИ), тъй като тяхното разстройване или разрушаване би могло да окаже сериозно въздействие върху жизнено важни обществени функции.

Защита на КИКИ[11] - защитата на критичната информационна инфраструктура (ЗКИИ) следва да се разбира, разглежда и реализира на практика като всеобхватен и систематичен подход по отношение на сигурността в кибернетичното пространство, като както активни действия за въвеждане на минимални стандарти, технически мерки за сигурност, организационни мерки и обучение на отделните

потребители, предприятията и обществените институции, така и мерки за реагиране като наказателно-правни, гражданско-правни и административни санкции.

Център за данни – архитектурно обособено и защитено от външни физически въздействия пространство за съсредоточаване и осигуряване на ефективна работна среда за функциониране на централизирани информационни и комуникационни ресурси за обработка и ресурси за дълготрайно съхранение на информация. Центърът за данни е интегриран функционален комплекс от:

- *Архитектурно обособено и защитено от външни природни и физически въздействия пространство* с характерни интериорни решения, осигуряващи ефективното функциониране на централизираните комуникационни и информационни ресурси;
- *Техническа инфраструктура*, осигуряваща непрекъсната работна среда за информационното и комуникационното оборудване – непрекъснато токозахранване, климатизация, филтриране, вентилиране и поддържане на качеството на въздуха, пожароустойчивост и пожарозащита, физическа защита от не санкциониран достъп;
- *Информационна инфраструктура*, осигуряваща непрекъснатата обработка, съхранение и достъп до информация;
- *Комуникационна инфраструктура* – осигуряваща защитения външен и резервирания вътрешен обмен на данни, както и обмен на информация за целите на управление на инфраструктурата на центъра;
- *Организационна инфраструктура* – чрез система от функционални процедури и роли, с подходяща квалификация и опит се гарантира мониторинга, поддържането и управлението на достъпа до базовите услуги на центъра за данни.

2.2. Обхват и области на приложение.

Единните унифицирани изисквания са приложими за Центрове за данни, в които се създава, съхранява, обработва и осигурява достъп до особено чувствителна информация, съгласно т.1.2.1.

Центровете за съхранение на особено чувствителната информация, обслужващи електронното правителство и дейностите на централната държавна администрация са част от информационната критична инфраструктура на Република България.

Обхвата на Единните унифицирани изисквания се състои в определянето на минималните задължителни технически и организационни характеристики и дейности, които да осигурят ефективна защита на центровете за съхранение на особено чувствителната информация.

Базовият критерий за принадлежност на конкретен център за данни на ЦДА към обхвата на приложение на Единните унифицирани изисквания, е оперирането в рамките на този център (съхранение, обработка и осигуряване на достъп) с особено чувствителна информация, определена съгласно т.1.2.1.

3. Система от Единни държавни изисквания при разработването и въвеждането на системи и технологии за защита на информацията и осигуряване на оперативна съвместимост на центрове за съхранение на особено чувствителна информация на централна държавна администрация – Методическа част на ЕУИЦСОЧИ.

3.1. Структура, класификация и критерии за приложимост

3.1.1. Приложими стандарти и добри практики.

При определяне на структурата и съдържанието на Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация са оценени и обобщени стандартизационните практики в технологичната област.

Таблица 1. Сравнителен анализ на изискванията към Центровете за данни – приложими стандарти

№	Изискване (критерий) към Център за данни	ISO/IEC 24764	EN 50173-5	TIA-942
1	Архитектура /Инженерна защита/ Интериор	✔	✔	✔
2	Технологии за окабеляване/ физическа комуникационна среда	✔	✔	✔
3	Резервиране на инфраструктурата	✔	✔	✔
4	Заземяване/ Управление на потенциалните разлики	IEC 60364-1	EN 50310	TIA-607
5	Класове на защита - общо класифициране	✖	✖	✔
6	Кабелна топология/Маршрутизиране на кабелните снопове	IEC 14763-2*	EN 50174-2 /A1	TIA-569
7	Двойни тавани и подове	IEC 14763-2*	EN 50174-2 /A1	✔
8	Натоварване на пода	✖	✖	✔
9	Разпределение на пространството (помещения, врати)	IEC 14763-2*	EN 50174-2 /A1*	✔
10	Захранване/ Непрекъсваемо захранване	✖	✖	✔
11	Противопожарна защита / безопасност	✖	EN 50174-2 /A1*	✔
12	Охлаждане	✖	✖	✔
13	Осветление	✖	✖	✔
14	Администриране/ Етикетиране	IEC 14763-2*	EN 50174-2 /A1*	✔
15	Температурни режими/ Влажност	✖	✖	✔

На Таблица 1 са представени 15 основни изисквания, които се предявяват към инфраструктурата и ИКТ системите в центровете за данни съгласно водещите приложими стандарти в разглежданата технологична област:

- БДС EN50173-5. Информационни технологии. Системи за структурно окабеляване. Част 5: Центрове за данни (01.06.2007) и Анекс БДС EN50173-5/A1:2010(21.01.2011);
- ISO/IEC 24764:2010. Информационни технологии. Общи кабелни системи за център за данни (01.04.2010);
- ANSI/TIA-942-2005. Стандарт за телекомуникационна инфраструктура на център за данни (12.05.2005).

При формирането на ЕУИСОЧИ са приложени приоритетите при прилагане на стандартизационните практики, съгласно Раздел 6. т.6.6. от ОБЩА СТРАТЕГИЯ ЗА ЕЛЕКТРОННО УПРАВЛЕНИЕ В РЕПУБЛИКА БЪЛГАРИЯ 2011-2015[1], като във връзка с тези приоритети ANSI/TIA-942-2005 се разглежда под формата на добра практика (ANSI/TIA не се определят като директно приложими стандарти в Раздел 6. т.6.6.).

На фиг.1 и Таблица 2 са представени резултатите от топологичното и терминологичното съответствие на приложимите стандарти по отношение на кабелните системи за Центрове за данни.

При разработването на ЕУИСОЧИ се прилага терминологията и топологичния модел, определени чрез БДС EN50173-5 и БДС EN50173-5/A1:2010. При инфраструктурен елемент извън обхвата на БДС EN50173-5 се прилагат стандартите при следния приоритет:

а/. ISO/IEC 24764:2010 – за общите структурни кабелни системи;

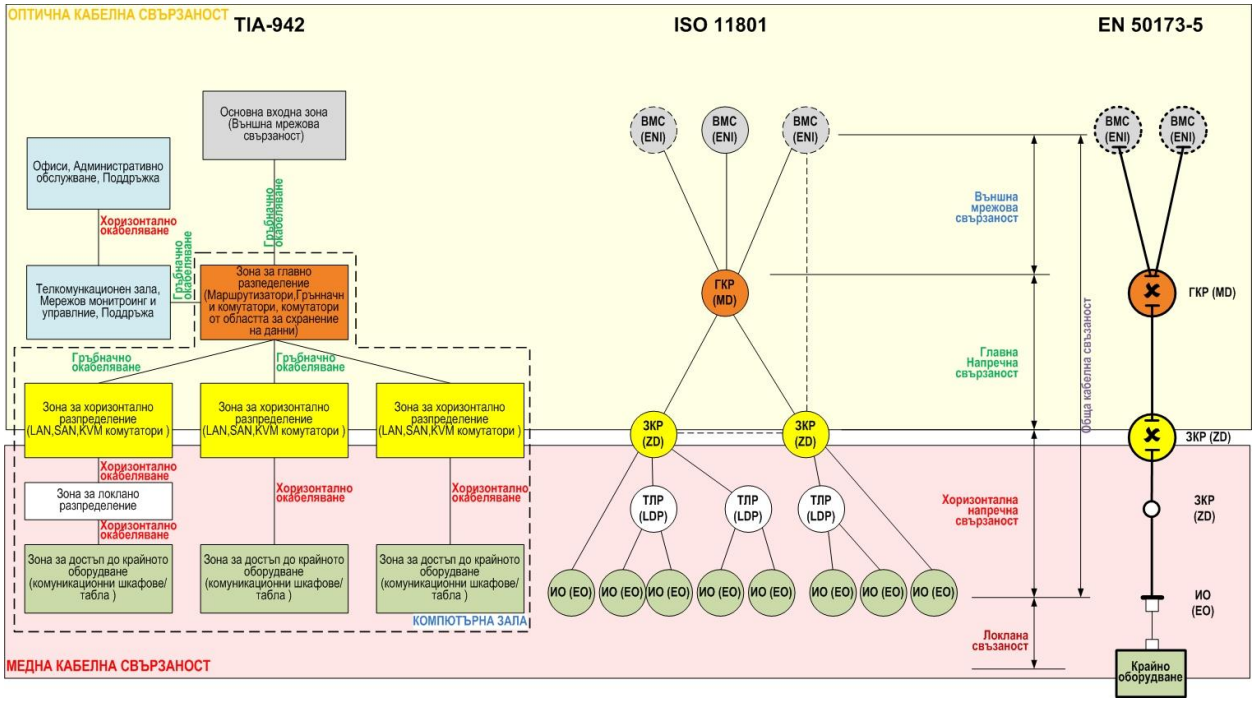
б/. ISO 11801:2002 – при резервирането на топологията на физическата свързаност и постигането на определен клас на надеждност и отказоустойчивост на комуникационната инфраструктура;

в/. BICSI 002-2011 - при проектирането на токоразпределението и топлоотвеждането;

г/. БДС EN стандартите за специфични системи и елементи на инфраструктурата;

д/ .Приложими национални нормативи и регулации;

е/. Приложими добри практики за случаите, когато не могат да бъдат отнесени пряко за съответствие към някой от предходните (а/.-г/.).

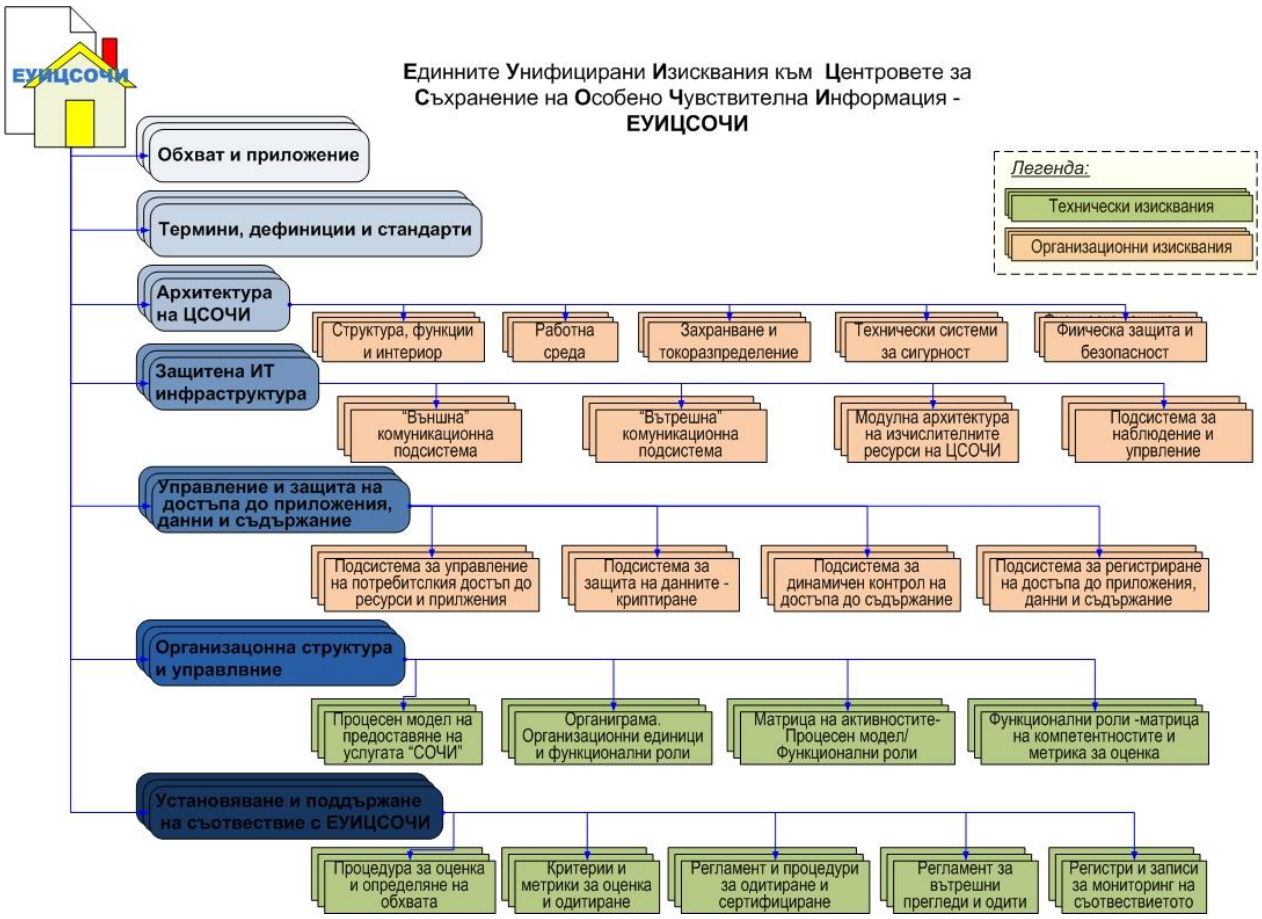


Фиг.1.Топологично съответствие, съгласно приложимите стандарти и добри практики на елементите на структурната кабелна система на Център за данни

Таблица 2. Терминологичното съответствие на приложимите стандарти по отношение на кабелните системи за Центрове за данни

№	ISO/IEC 24764	ISO 11801	TIA-942
1	*External Network Interface(ENI)*	*Campus Distributor (CD)*	*ENI (External Network Interface) ER (Entrance Room)*
	Външна мрежова свързаност (ВМС)	**Междусграден мрежов разпределител**	**Външна мрежова свързаност**
2	*Network Access Cable*	*Primary Cable*	*Backbone Cabling*
	Кабел за външна мрежова свързаност	**Първичен комуникационен кабел**	**Гръбначна кабелна свързаност**
3	*Main Distributor (MD)*	*Building Distributor (BD)*	*MC (Main Cross Connect) MDA (Main Distribution Area)*
	Главен кабелен разпределител (ГКР)	**Сграден разпределител**	**Главна напречна свързаност Зона за главно разпределение**
4	*Main Distributor Cable*	*Secondary Cable*	*Backbone Cabling*
	Главен разпределителен кабел	**Вторичен комуникационен кабел**	**Гръбначна кабелна свързаност**
5	*Zone Distributor (ZD)*	*Floor Distributor (FD)*	*HC (Horizontal Cross Connect) HDA (Horizontal Distribution Area)*
	Зонов разпределител	**Етажен разпределител**	**Хоризотална напречна свързаност Зона за хоризотално разпределение**
6	Zone Distribution Cable	Tertiary/Horizontal Cable	Horizontal Cabling
	Зонов разпределителен кабел (ЗКР)	**Хоризонтален кабел**	**Хоризонтално окабеляване**
7	*Local Distribution Point (LDP)*	*Consolidation Point (CP)*	*CP* (Consolidation Point) ZDA (Zone Distribution Area)*
	Точка за локално разпределение (ТЛР)	**Точка за кабелно консолидиране**	**Точка за локално разпределение**
8	*Local Distribution Point Cable*	*Consolidation Point Cable*	*Horizontal Cabling*
	Локален разпределителен кабел	**Кабел до точката на консолодиране**	**Хоризонтално окабеляване**
9	*Equipment Outlet (EO)*	*Telecommunications Outlet (TO)*	*EO (Equipment Outlet) EDA (Equipment Distribution Area)*
	Изход за оборудване (ИО)	**Телекомуникационен изход**	**Зона за достъп до оборудването**

3.2. Описание на множеството от изисквания.



Фиг.2. Структурата и съдържанието на Единните Унифицирани Изисквания към Центровете за Съхранение на Особено Чувствителна Информация – ЕУИЦСОЧИ

Структурата на системата от Единни унифицирани изисквания към Центровете за съхранение на особено чувствителна информация е представена на фиг.2. При формирането на структурата е приложен модел за интегрирана превенция и подтискане на рисковия потенциал при съхранение, обработка и достъп до чувствителна информация в КИКИ. Със структурата се въвеждат два типа изисквания – технически и организационен. От гледна точка на **техническите изисквания** и след анализ на приложимите стандарти и добрите практики са обособени три тематични групи:

- **Архитектурни и конструктивни изисквания (*Архитектура на ЦОЧИ*)** към спомагателните и поддържащите системи – обслужват процеса на съхранение, обработка и достъп до особено чувствителна информация (ОЧИ);
- **Изисквания към защитената КИКИ (*Защитена ИТ инфраструктура*)** - пряко участваща в процеса на съхранение, обработка и достъп до ОЧИ;
- **Изисквания към програмните системи и модули за осигуряване на приложната защита на ОЧИ** (***Управление и защита на достъпа до приложения, данни и съдържание***) – обслужват процеса на съхранение,

обработка и достъп до ОЧИ на ниво приложни програмни системи и инфраструктура за управление на достъпа до ресурсите на центъра за данни.

От гледна точка на **организационните изисквания** - те преди всичко се свързват с въвеждането на т.нар. Система за управление на сигурността на информацията (СУСИ) и свързаните с тази система (ISO 27001:2006) оценки на риска, политики и процедури за сигурност и защита, организационна структура, контрол на съответствието, коригиращи действия и др. Чрез организационните изисквания се въвежда и унифициране на организационния модел за функциониране на ЦСОЧИ, както и трансформирането на модела за осигуряване на защитата на ОЧИ от йерархично-функционален към процесно-ролеви, което е добра световна практика при осигуряване на дейности за предоставяне на критични обществени услуги (продукти).

В *Приложение 1. Описание на Единни унифицирани изисквания* са дефинирани на базата на структурния модел от фиг.2 и приложимите стандарти и добри практики (т.2.1) конкретни критерии, условия и ограничения към Центровете за съхранение на особено чувствителна информация.

Системата от изисквания съгласно *Приложение 1. Описание на Единни унифицирани изисквания* е адаптирана за съществуващи и за новоизграждащите се ЦСОЧИ, като за всяко дефинирано изискване е определена:

- Метрика за установяване на съответствие, като дадените стойности са прагови и могат да бъдат надвишавани в зависимост от спецификата и сферата на приложение на конкретен ЦСОЧИ;
- Стандарт, нормативна регулация и/или добра практика, във връзка с която се въвежда това изискване и се формира конкретната стойност или доверителен интервал за съответствие.

3.3. Приложна функционалност и критерии за установяване на съвместимост

3.3.1. Специфика на интегрираното прилагане на унифицираните изисквания в система - възможни конфликтни точки и процедури за управление на промените и разрешаване на конфликти.

При прилагане на системата от Единни унифицирани изисквания съгласно *Приложение 1. Описание на Единни унифицирани изисквания* е възможно да възникнат конфликтни точки, за които се прилагат следните правила за разрешаване:

- При конфликт между ЕУИЦСОЧИ и приложим във връзка с определено изискване ISO, EN или БДС стандарт, се прилага съответствие съгласно нормата, заложена в стандарта. Приоритета на специфичните стандарти в технологичната област е определен в т.2.1.
- При конфликт или невъзможност за прилагане на определено изискване за ЦОСЧИ, изградени при въвеждането на ЕУИЦСОЧИ, изискването се прилага до постигане на практически реализуемата степен на съответствие при текущите ограничения на архитектурата и инфраструктура на конкретния център, като в одиторския доклад за установяване на първоначално съответствие с

ЕУИЦСОЧИ се записват като забележка причините за установеното частично несъответствие.

- При конфликт между ЕУИЦСОЧИ и нововъведен ISO, EN или БДС стандарт, се инициира процедура за коригиращи действия и актуализация на *Приложение 1. Описание на Единни унифицирани изисквания*.
- При конфликт между ведомствена политика или процедура във връзка със съхранение и/или обработка на ОЧИ и ЕУИЦСОЧИ се прилагат ЕУИЦСОЧИ.
- При конфликт между ведомствена политика или процедура във връзка със защита на КИКИ и ЕУИЦСОЧИ (доколкото голяма част от съществуващите центрове за данни на държавната администрация се класифицират като КИКИ, съгласно настоящите изисквания и регулацията за CIIP[10]) се прилагат ЕУИЦСОЧИ.

За управлението и поддържането на промените в ЕУИЦСОЧИ се приемат и публикуват приложения, в които ясно се указват характера на промените и отражението им в структурата и съдържанието на основния документ и вече публикуваните приложения.

3.3.2. Специфични особености при прилагане на Система от Единни държавни изисквания – Технологична част.

3.3.2.1. Технологични особености при дефинирането на Системата от единни унифицирани изисквания и определянето на минималните стойности и доверителните интервали за едно или група изисквания.

От приложна гледна точка с прилагане на ЕУИСОЧИ се очаква да бъдат решени 4-те групи характерни задачи, които възникват при проектирането на центрове за данни:

- Разположение на ресурсите – местата за разполагане на компютрите, масивите за данни и мрежовите комуникационни устройства.
- Захранване и разпределение на захранването – до всяко устройство да постъпва непрекъснато във времето необходимото му като параметри захранване за нормално функциониране и изпълнение на базовото предназначение в архитектурата на центъра.
- Отопление, вентилация и климатизация – осигуряване на микроклимата в зоните за разполагане на устройствата, такъв, че да отговаря на експлоатационните режими на работа на устройства за монтаж в закрити помещения.
- Структурна кабелна система – осигуряване на физическата комуникационна среда вътре между устройствата в центъра и външната свързаност на центъра с комуникационната система.

Общият технологичен измерител при прилагането на ЕУИЦСОЧИ **е надеждност и достъпност на услугата съхранение и обработка на ОЧИ, измерена в % от общото време за недостъпност до тази услуга за 1 година.**

Дефинираните минимални стойности и доверителни интервали на изискванията в *Приложение 1. Описание на Единни унифицирани изисквания,* формирани на базата на приложими стандарти и добри практики и с цел да се постигне:

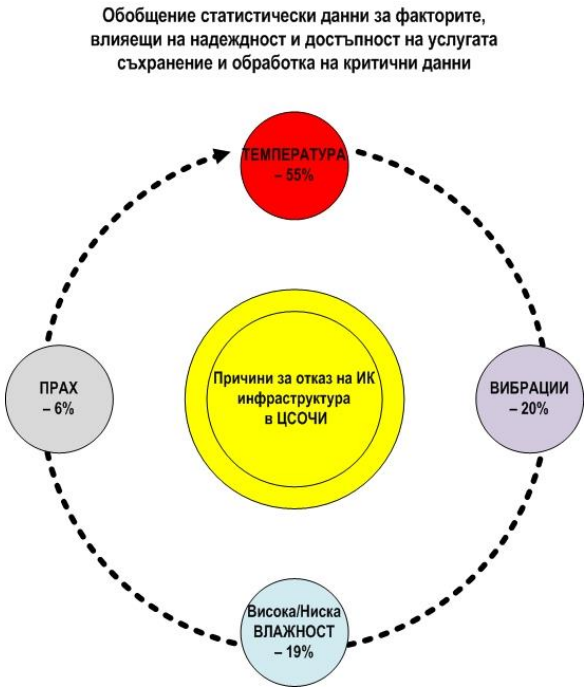
Общо годишно време за недостъпност на услугата „съхранение и/или обработка на особено чувствителна информация" ≤ 60 минути за Център за данни, част от Критична информационна и комуникационна инфраструктура на Р България при максимална продължителност на един непрекъснат период от време за недостъпност на услугата ≤ 10 минути*.

**В зависимост от степента на критичност на информацията и информационната услуга се дава възможност Възложителите да определят по-малки от дефинираните чрез ЕУИЦСОЧИ стойности на параметрите за оценка на надеждността на услугата съхранение и обработка на ОЧИ: общо годишно време на недостъпност и максимална продължителност на един непрекъснат период от време за недостъпност.*

При формиране и дефиниране на технологичните изисквания, както и при формирането на минималните стойности и доверителните интервали в *Приложение 1. Описание на Единни унифицирани изисквания* е взета под внимание статистическата оценка за влиянето на инфраструктурата върху надеждността на представяните услуги в центровете за данни[13,14,15,16,17] – фиг.3.

Приетото ограничение за не повече от 10 минути недостъпност на услугите, предоставяни чрез ЦОЧИ се отразява върху изискванията от *Приложение 1*, които имат пряко отношение към резервирането на ресурсите в ЦОЧИ:

- Захранващи кабелни сегменти и токоразпределително оборудване – пълна резервираност (2N), еквивалентна на TIA942/ Tier4;
- Комуникационни кабелни сегменти и комуникационно оборудване - външна, главна (гръбначна), хоризонтална и локална свързаност - пълна резервираност (2N за оборудването), еквивалентна на TIA942/ Tier4;
- Непрекъсваеми източници на захранване – пълно резервиране (2N) във връзка с добрите практики на TIA942/ Tier4;
- Системата за топлоотвеждане и охлаждане - 2N във връзка с добрите практики на TIA942/ Tier4 резервиране се осигурява чрез прилагане на технология с охладена вода, достигаща от резервираните външни тела до резервираните локални топлообменни модули по двоен тръбен път;
- Изчислителните ресурси чрез прилагане на виртуализация и модулна структура на физическите сървъри;
- Дискови масиви за съхранение на данни - прилагане на 2N резервиране за архитектурните елементи на масива и физическите носители за данни.



*Фиг.3. Средна статистическа оценка на влиянието на инфраструктурните фактори върху надеждността на предоставяне на услугата съхранение на особено чувствителна информация (критични данни) *Източник Learning Network Cisco[14]*

По отношение на частта от *Приложение 1. Описание на Единни унифицирани изисквания* във връзка с оценката за запълването на пространството в комуникационните шкафове при избора на критерии и метричната им оценка, е приложен технологичния принцип, известен от добрите практики като **правило 3+2** [14,18].

Във връзка с прилагането на **правилото 3+2** се приема, че за всеки сървър в шкафа са нужни 5 инфраструктурни системи: **3** (**1-к**омуникации, **2-**захранване, **3-м**ониторинг/управление) **+ 2** (**1-о**хлаждане/климатизация + **2-ф**изически монтаж /закрепване/ фиксиране в шкафа). За тези системи **(3+2)** според цитираните източници[14,18] и анализа на добрите практики, както и от гледна точка на постигане на ефективност на площта в центъра, не трябва да заемат **повече от 18% от общото пространство във всеки шкаф** с изключение на функционално специализираните за спомагателна инфраструктура шкафове.

Друго ключово ограничение, което се приема е от гледна точка на факта, че центъра ще осигурява надеждното функциониране на КИКИ за съхранение и обработка на ОЧИ, то е недопустимо препълване на комуникационните шкафове от една страна и от друга остава валиден и принципа за ефективно използване на площта. При отчитане на тези две ограничителни условия и от гледна точка на практиката за все по-често използване на модулни (blade) сървърни решения и масиви от данни с висока плътност в *Приложение 1. Описание на Единни унифицирани изисквания* е прието ограничението за максимална инсталирана мощност за един шкаф с КИКИ – **не по-голяма от 15kW**. Добрите практики[14,17,18] показват, че това ограничение осигурява възможност за

прилагане на съвременни модулни технологии за осигуряване на изчислителен ресурс от една страна и от друга - фактически се ограничава броя инсталирани сървъри в един комуникационен шкаф до 40, при което се постига среден клас плътност[17,18].

При пространственото разполагане на комуникационните шкафове в *Приложение 1* са определени минималните разстояния от предната и задната страна на всеки комуникационен шкаф (не по-малко от 1000мм от предната страна и не по-малко от 600 мм от задната страна) до интериорен елемент от центъра (шкаф от съседна редица, стена или друг елемент). Тези разстояния се определят от съображения за свободно монтиране, демонтиране, профилактика и добавяне на ново оборудване.

При определяне на изискванията към структурната кабелна система *Приложение 1. Описание на Единни унифицирани изисквания,* са приложени актуалните действащи стандарти БДС EN50173-5. Информационни технологии. Системи за структурно окабеляване. Част 5: Центрове за данни (01.06.2007) и Анекс БДС EN50173-5/A1:2010(21.01.2011), които определят типа на приложните кабелни секции, физически стандарти за комуникация, максимални дължини по типове зони за разпределение – главно разпределение, зонално хоризонтално разпределение, локално крайно разпределение.

3.3.2.2. Функционален обхват и специфични особености при реализацията и взаимодействието на подсистемите от Защитената ИТ инфраструктура.

ЕУИСОЧИ се разработват с цел да осигуряват предоставянето на услугата СОЧИ в контекста на защитата на КИКИ. В този смисъл, тези изисквания имат специфичен обхват – приложими са за всеки център за данни, в който се съхранява чувствителна информация. Тези изисквания имат по-широк обхват от конкретен стандарт или регулация, защото в тях е заложен интегриран подход за осигуряване на услугата защитен достъп до чувствителна информация. От една страна чрез ЕУИСОЧИ се разширява разбирането за критичен информационен актив, като към обичайния за ISO27001 информационен актив – данни се добавят всички технически и инфраструктурни активи, които осигуряват процеса на предоставяне на защитената приложна услуга обработка на критични данни.

В този смисъл системата за осигуряване на устойчиво съответствие с ЕУИСОЧИ по аналогия може да бъде наречена Система за управление на сигурността на критичните информационни активи (СУСКИА). Една надеждно защитена информация (структуриран или не обем данни) запазва свойството си защитена, до момента на заявката за достъп до защитеното съдържание. От този момент в процеса за осигуряване на достъп се включва разширената система от критични информационни активи – частен случай на която са ЦСОЧИ. На практика, чрез обхвата си ЕУИСОЧИ специфицират взаимодействията между критичните данни и КИКИ с цел предоставяне на защитен достъп, както и превенция на самата КИКИ и обработваните критични данни от естествените и специфични рискове.

Чрез ЕУИСОЧИ се установява интегриран технологичен и организационен модел на център за данни от КИКИ, в рамките, на който са осигурени измерими с

рисковия си потенциал условия за съхранение, обработка и предоставяне на защитен достъп до особено чувствителна информация.

3.3.2.2.1. Раздел I. Минимални архитектурни изисквания.

Разделът за минимални архитектурни изисквания (*Приложение 1* дава насоки по отношение на географското разположение, екстериорното позициониране и интериорната конфигурация на центъра и тази част от инфраструктурата, която не е свързана като функции с електрозахранването. Представени са ключовите изисквания и ограничения при избора на устойчиви на риск регион и сграда за разполагане на ЦСОЧИ, като ЦСОЧИ е класифициран като обект Категория I, съгласно Приложение 1 на Наредба 7/08.06.1998 за системите за физическа защита … [22].

При определяне на изискванията към структурата и предназначението на помещенията на територията на ЦСОЧИ са приложени серия от добри практики във връзка с приоритетното прилагане на стандартите, съгласно т.2.1[19,20,21,23,24,25,26]. В резултат на обобщаване на изискванията на групата изброени стандарти към структурата и предназначението на помещенията на ЦСОЧИ се определя следната минимална конфигурация на зоните и залите – фиг.4.

Фиг.4.Структура и предназначение на помещенията в ЦСОЧИ.

Във връзка с поставените изисквания съгласно фиг.4 на територията на ЦСОЧИ се формират две зони с повишена защита от тип „защитена стая”:

- Компютърна зала – пожароустойчивост на защитената стая съгласно БДС EN 1047-2:2010 и добрите практики на ANSI/TIA 942 минимум 60 минути за залата (стени, под, таван, врати) и монтиране, изпитване и сертифициране на система за подтискане на паразитните електромагнитни излъчвания, съгласно Наредбата за задължителните условия за сигурност на АИС или мрежи ...[12] – клас SIDP-27 (TEMPEST) Ниво „С” (чл.60.ал.1 и във връзка с чл.70.ал.2).
- Зала за мониторинг и управление на защитената инфраструктура на ЦСОЧИ - монтиране, изпитване и сертифициране на система за подтискане на паразитните електромагнитни излъчвания, съгласно Наредбата за задължителните условия за сигурност на АИС или мрежи ...[12] – клас SIDP-27 (TEMPEST) Ниво „В”.

За всички останали помещения се изисква да нямат външни прозорци и вратите да са с контролиран достъп и ниво на огнеустойчивост „EI 60” [24,27], както и работна среда във връзка с нормите, определени с НАРЕДБА № 3 от 18.09.2002 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи[29].

3.3.2.2.2. Раздел II. Минимални изисквания към работната среда, вентилация и климатизация на ЦСОЧИ.

В този раздел са приложени разпоредбите на НАРЕДБА № 3 от 18.09.2002 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи[29], както и добри практики при проектирането на центрове за данни в BICSI 002-2011.Art.5.3 [25] и ANSI/TIA 942.G.61/G.6.2[23].

На базата на общото топлоотделяне в Компютърната зала ЦСОЧИ са разделени на два класа:

При общо топлоотделяне ≤ 25kW се дава възможност топлоотвеждането и охлаждането да се реализира по технология с резервирано директно изпарение.

При общо топлоотделяне над 25kW се определя технология за топлоотвеждане на базата на охладен агент.

Също при изпълнението на решението за топлоотвеждане се поставя изискване за 2N резервираност на всички елементи от системата: агрегати, помпи, тръбни пътища, ел. захранващи модули.

По отношение на климатизирането и работната среда във всички останали помещения на ЦСОЧИ се прилагат изискванията съгласно Раздел I.

3.3.2.2.3. Раздел III. Минимални изисквания към осигуряването на ефективно токоразпределение и непрекъснато електрическо захранване.

В този раздел са приложени разпоредбите на Наредбата №3/09.06.2004 за устройството на електрическите уредби и електропроводните линии[28], както и детайлно представените добри практики при проектирането на центрове за данни в BICSI 002-2011.Art.5.4.2.Table-1[25]. Акцент в изискванията е поставен върху

класифицирането на ЦСОЧИ като обект „Нулева категория” по отношение на присъединяването на центъра към електропреносната система[28]. От гледна точка на вътрешното токоразпределение са предявени изисквания за 2N резервираност на основното захранване на всяко от нивата на разпределение: главно разпределително табло, хоризонтални разпределителни табла, захранващи възли в комуникационните шкафове. За всяка захранваща линия са поставени изисквания за оразмеряване (преоразмеряване) на базата на увеличение със съответен коефициент на номиналната консумация на захранваната зона. Както вече беше подчертано в т.3.1., за да се избегне пренасищане на шкафове с оборудване, което се разглежда като рисков фактор, като за всеки шкаф за оборудване на ЦСОЧИ е поставено ограничение за сумарната максимална инсталирана мощност на основното и спомагателното оборудване – да не надвишава 15kW.

3.3.2.2.4. Раздел IV. Минимални изисквания към техническите системи за физическа защита ,безопасност и сигурност на ЦСОЧИ.

За определяне на минималните изисквания по Раздел IV са приложени разпоредбите на серия специализирани стандарти в областта на техническите системи за сигурност и безопасност[30,31,32,33,34,35,36,37], като общата регулация за обхвата на прилагане на тези системи за обекти от класа на ЦСОЧИ е определена с Наредбата за задължителните условия за сигурност на АИС или мрежи ...[12].

Във връзка с конфигурацията на помещенията на ЦСОЧИ (фиг.4) в Раздел IV са определени приложимите технологии и методи за идентификация на лица и контрол на достъпа за различните по степен на сигурност зони и във връзка с приложимите стандарти[30,31,32].

Към подсистемата за видеонаблюдение са определени минимални изисквания, като са приложени разпоредбите от НАРЕДБА за задължителните условия за сигурността на АИС или мрежи, в които се съхранява, обработва и пренася класифицирана информация - чл.44. ал2.т.2 и във връзка с ЗЗКИ Глава VI. В допълнение, от гледна точка на минималните технологични изисквания и тестване на работоспособност, са приложени стандартите от групата БДС EN 50132[33,34,35]. Времето за съхранение на видеозаписите е определено във връзка с изискванията на чл.30.ал.5 и във връзка с ал.6 на същия член от Закона за частната охранителна дейност.

Предвид спецификата на приложението и необходимостта от ранна детекция за технологията за откриване на пожар, са наложени минимални технологични изисквания съгласно БДС 54-20:2006[36] за прилагане на т.нар. метод с „аспирираща димно-оптична детекция”, който се вписва в концепцията за принудително вентилиране на основните критични зони на ЦСОЧИ (Компютърна зала и Зала за мониторинг и управление).

Към пожарогасителната система са:

Компютърната зала и техническите помещения, в които не присъстват постоянно хора (при решение с централен UPS, агрегатно помещение и др.) са приложени регулациите на стандарт БДС EN 12094-1:2003[38] – гасене с инертен газ или газ, съдържащ халогенирани въглеводороди;

Административната зона, Залата за мониторинг и управление - регулациите на стандарти БДС EN 12845:2004+A2:2009 [39] и БДС EN 12259-1:1999+A1:2001/A2:2005[37] – гасене с вода чрез автоматична сприклерна инсталация.

3.3.2.2.5. Раздел V. Минимални изисквания към защитената инфраструктура на ЦСОЧИ.

При разработването на изискванията на този раздел са приложени групата стандарти БДС EN 50173, като за определяне на ограниченията към външната резервирана свързаност на ЦСОЧИ е използвана уводната част на стандарта[19], а при специфициране на вътрешната защитена топология и конфигурация на активно комуникационно оборудване – специализирана редакция на стандарта, посветена на структурните кабелни системи за центрове за данни [20].

С минималните ограничения се определя, че оптична кабелна свързаност се прилага на всички нива на разпределение, като само на ниво комуникационен шкаф е допустимо използване на медни кабели, най-малко Category 6A, съгласно допълненията и измененията, въведени с анекса към основния стандарт[21].

С ЕУИЦСОЧИ за топологията на структурното окабеляване на всички нива на разпределение е въведено минимално 2N резервиране от край до край, което се отразява и на броя и конфигурацията на инсталираните комуникационни портове за активното оборудване в Главния Кабелен Разпределител (ГКП)[20], Зоналните Кабелни Разпределители (ЗКП), Локалните Кабелни Разпределители (ЛКП) и терминиращите комуникация портове на крайното оборудване (ИО,ЕО[21]).

От гледна точка на специфициране, извикванията в Раздел V до голяма степен потвърждават и селектират по приложимост нормите на стандартите от технологичната област[19,20,21].

С раздел V се въвежда ограничение за организацията на изчислителните ресурси под формата на Модулната архитектура на изчислителните ресурси на ЦСОЧИ, която да осигури възможност за гарантиране на еквивалентно до ниво 2(N+1) резервиране на виртуалните ресурси, обслужващи критичните приложени процеси. В този смисъл се поставят конкретни функционални искания към организацията на изчислителните ресурси на ЦСОЧИ като интегриран комплекс от:

- Многоядрени процесорни архитектури;
- Споделени ресурси оперативна памет с възможност за модулно разширяване с добавяне на външни модули памет;
- Обща интелигентна комуникационна среда за обмен на данни между всички елементи от интегрирания комплекс с висока пропускателна способност;
- Модулна защитена подсистема за съхранение на данни с директна връзка към обединената комуникационна среда;
- Единен интерфейс за управление на модулната архитектура (многоядрени сървъри, споделен ресурс оперативна памет, обща среда за обмен на данни, модулна защитената подсистема);

- Поддържане на виртуализация и осигуряване на скалируема и адаптираща се изчислителна архитектура за съхранение, обработка и предоставяне на достъп до критични данни в ЦСОЧИ.

Тези изисквания са определени на базата на текущото технологично ниво на развитие на резервиране на ресурсите в средата на т.нар. виртуализирани изчислителни комплекси и във връзка с дадената възможност, съгласно ЗЗКИ. Раздел V. Чл.89. и да се дефинират специфични изисквания, съгласно чл.90.ал.2. и от гледна точка на добри практики, определени от ANSI/TIA 942- G.2./G.4 (Tier 4 requirements).

Ключовата роля на Раздел V от ЕУИСОЧИ се потвърждава и с дефинирането и детайлното специфициране в рамите на този раздел на минималните изисквания към Система за мониторинг и управление на основната инфраструктура и спомагателната инфраструктура на ЦСОЧИ.

По отношение на минималните изисквания към Система за мониторинг и управление на ЦОСОЧИ е приложен диференциран подход, като множествата наблюдавани и управлявани параметри са разделени:

По степен на критичност и приложение на помещението за Компютърната зала и за всички останали зали;

По принадлежност на наблюдаваните и управлявани параметри към основната инфраструктура (виртуализирания изчислителен комплекс) или към спомагателната инфраструктура (захранване, климатизация, осветление, системи за сигурност и безопасност).

Като допълнение към минималните изисквания към Система за мониторинг и управление на основната инфраструктура и спомагателната инфраструктура на ЦСОЧИ е развит и проблема за необходимостта от регистриране на събитията от мониторинга и действията (автоматични или по инициатива на оператор) за управление на ресурсите, като е приложена регулацията на чл.52 и чл.53 от Наредбата за задължителните условия за сигурността на АИС или мрежи, в които се съхранява, обработва и пренася чувствителна информация[12]:

- Регистрират се всички събития от мониторинг за основната инфраструктура;
- Регистрират се всички алармени събития от мониторинг на спомагателната инфраструктура;
- Регистрира се състояние на минималното множество параметри на работната среда, съгласно Приложение 1.V.5.1.2 и V.5.1.3. – една регистрация за период не по-голям от 5 минути;
- Регистрират се по време за достъп всички стартирани приложни процеси и ресурсите, които те използват;
- Регистрират се действията на всички потребители;
- Всички регистрации се архивират на защитено дисково пространство за период от 30 дни назад, като на всеки 24 часа регистрационния файл се архивира на два комплекта външни оптични дискови носители - единият комплект се съхранява на територията на ЦСОЧИ, вторият се съхранява извън територията на ЦСОЧИ по ред, определен с работна инструкция от внедрена СУСИ.

3.3.2.2.6. Раздел VI. Минимални изисквания за управление и защита на достъпа до ресурсите на ЦСОЧИ.

В Раздел VI се определят общите изисквания към сигурността на критичните информационни активи на ЦСОЧИ като се поставя **основно изискване за наличие на валиден и действащ сертификат за съответствие с изискванията на стандарта ISO/IEC 27001:2005**, издаден от сертификационен орган, имащ европейска акредитация, доказателство за съответствие спрямо изискванията на стандарта BDS ISO/IEC 27001:2006 и внедрена СУСИ.

Чрез ЕУИЦСОЧИ се определя, че управление и защита на достъпа до ресурсите на ЦСОЧИ се регулира и контролира чрез механизмите специфично разработената и внедрена СУСИ и в съответствие с БДС ISO/IEC 27001:2006. Това позволява организационното адаптиране на ЕУИЦСОЧИ към спецификата на конкретния център.

3.3.2.2.7. Раздел VII. Минимални изисквания към организационната структура на ЦСОЧИ.

При разработването на Минимални изисквания към организационната структура на ЦСОЧИ е отразена възникващата необходимост от осигуряване на работните процеси на територията на центъра и действащия към момента национален класификатор на професиите и длъжностите, въведен с Приложение 4 към Заповед №РД01-931/27.12.2010 и промените в НКПД-2011 от 01.01.2012.

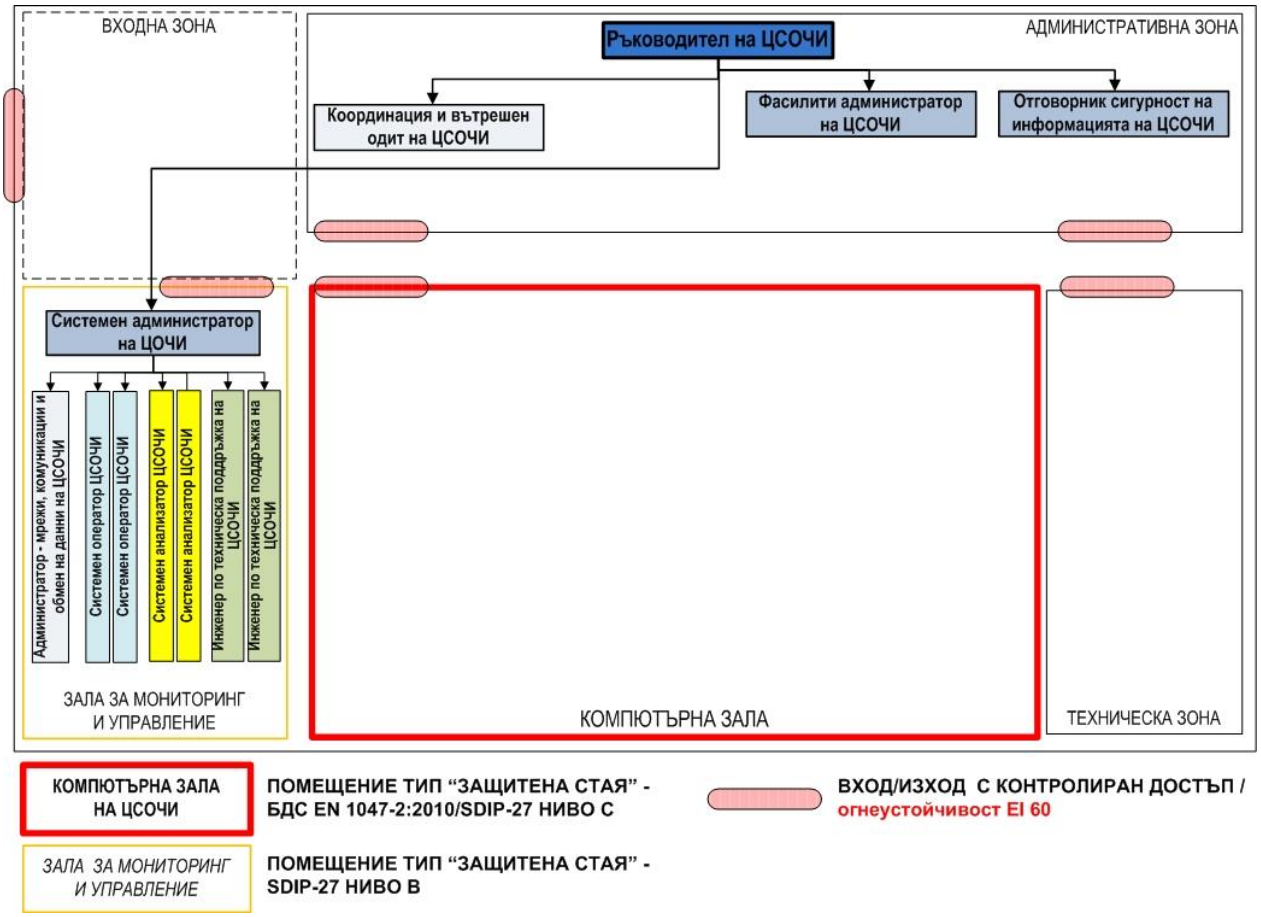
При определяне на организационната структура е възприет ролевия подход – дефинирани са функционални роли, за които в зависимост от мащаба на центъра може да се приложи синергия, т.е. един служител да изпълнява повече от една функционални роли. На фиг.5 е представена върху „картата" на ЦСОЧИ минималната организационна структура, осигуряваща нормалното функциониране на работните процеси на територията на центъра.

Минималните задължения и отговорности, присъщи на функционалните роли, са определени в *Приложение 1*. Акцентът в организационната структура е поставен върху три базови роли:

- Системен администратор – който е отговорен за непрекъснатата достъпност на защитената критична информационна инфраструктура на ЦСЧОИ;
- Фасилити администратора – който е отговорен за устойчивата и ефективна работа на спомагателната инфраструктура на ЦСОЧИ;
- Отговорника по сигурността на информацията – който е отговорен за прилагането на СУСИ и поддържането на нивото на защита на критичните информационни активи в съответствие с изискванията на БДС ISO/IEC 27001:2006 и ЕУИСОЧИ.

Цялостната дейност се наблюдава и контролира от Ръководителя на ЦСОЧИ във взаимодействие със служителя за Координация и вътрешен одит на ЦСОЧИ, който има отговорността да следи за прилагането на внедрената СУСИ и за поддържане на

съответствието с ЕУИЦСОЧИ на базата на определените в *Приложение 1* – критерии и метрики за установяване на съответствието.



Фиг.5. Минимална организационна структура, осигуряваща нормалното функциониране на работните процеси на територията на ЦСОЧИ

Функционалните характеристики на всяка роля се допълват от специфичните задължения и отговорности, които се присвояват на съответната роля във връзка с внедрената СУСИ.

3.3.2.2.8. Раздел VIII. Минимални изисквания при установяване и поддържане на съответствие с ЕУИЦСОЧИ.

В Раздел VIII е развито взаимодействието между ЕУИСОЧИ и определената като задължителна за разработване и внедряване СУСИ, съгласно извикванията на БДС ISO/IEC 27001:2006. За всеки един от разделите на ЕУИСОЧИ от Раздел I до Раздел VII е определен съответстващия механизъм за контрол и установяване на съответствие:

- **За минималните архитектурни изисквания към ЦСОЧИ** (*Приложение 1. Раздел I*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.9.1, A.9.2;
- **За минималните изисквания към работната среда** (*Приложение 1. Раздел II*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.9.2;

- **За минималните изисквания към токоразпределението и непрекъсваемото електрическо захранване** (*Приложение 1. Раздел III*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.9.2;
- **За минималните изисквания към техническите системи за физическа защита и безопасност** (*Приложение 1. Раздел IV*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.9.1;
- **За минималните изисквания към защитената ИТ инфраструктур**а (*Приложение 1. Раздел V*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.9.2, A.10
- **За минималните изисквания към управление и защита на достъпа до ресурсите** (*Приложение 1. Раздел VI*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.11;
- **За минималните изисквания към организационната структура** (*Приложение 1. Раздел VII*) – механизъм за контрол съгласно разработената СУСИ за ЦСОЧИ и във връзка с БДС ISO/IEC 27001:2006.A.8.

Първичният механизъм за установяване на съответствие с ЕУСОЧИ е чрез внедрените процедури за наблюдение и контрол от СУСИ, тъй като организационната система на стандарта гарантира ефективното установяване на съответствието и управление на несъответствията чрез конкретни коригиращи действия.

Вторичният механизъм за установяване на съответствие с ЕУСОЧИ е определен индиректно в Раздел VI. т.4. При конфигурирането на системата за мониторинг за наблюдаваните параметри, които имат пряка функционална връзка с критерии от *Приложение 1*, **задължително** се въвеждат прагови стойности, съгласно метричната оценка на съответния критерий. По този начин, чрез наблюдение и генериране на събитие при достигане на зададената критична стойност се осигурява в реално време ефективен механизъм за контрол на съответствието с по-голяма част от техническите критерии от *Приложение 1* – т.е. генерира се събитие с или без инкубационен период, което е обект за анализ и планиране на превантивни действия от Системния анализатор на ЦСОЧИ.

За всеки конкретен ЦСОЧИ системата от минимални изисквания, съгласно *Приложение 1*, може да бъде разширявана и допълвана,, като се спазват следните принципи:

- Метричните оценки в *Приложение 1* се определят като „минимални изисквания”;
- Не се допуска въвеждане на изискване, което противоречи или отменя базово изискване от дефинираните в *Приложение 1;*

- Не се допуска въвеждането на нови раздели и подраздели в структура на ЕУИЦОЧИ;
- При установяване на несъответствие с нововъведена нормативна регулация се отправя писмена заявка за корекция на базовата версия на ЕУИЦСОЧИ към упълномощения орган, който извършва корекцията и публикува нова базова версия.

БИБЛИОГРАФСКА СПРАВКА:

1. ОБЩА СТРАТЕГИЯ ЗА ЕЛЕКТРОННО УПРАВЛЕНИЕ В РЕПУБЛИКА БЪЛГАРИЯ 2011-2015 http://www.strategy.bg/FileHandler.ashx?fileId=1351;
2. Национална програма за ускорено развитие на информационното общество в Република България (2008-2010г.) http://www.mtitc.government.bg/page.php?category=492&id=3585;
3. Закон за защита на класифицираната информация http://www.dksi.bg/NR/rdonlyres/6DD6D686-B495-47F3-827F-69BFAF06F5D3/0/ZZKI_1_07_2012.pdf;
4. ДИРЕКТИВА 95/46/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ОТ 24 ОКТОМВРИ 1995 ГОДИНА ЗА ЗАЩИТА НА ФИЗИЧЕСКИТЕ ЛИЦА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ И ЗА СВОБОДНОТО ДВИЖЕНИЕ НА ТЕЗИ ДАННИ - http://www.cpdp.bg/?p=element&aid=30;
5. РАМКОВО РЕШЕНИЕ 2008/977/ПВР НА СЪВЕТА от 27 ноември 2008 година относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси http://www.cpdp.bg/?p=element&aid=428;
6. ДОКЛАД относно защитата на критичната информационна инфраструктура – постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство (2011/2284(INI) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0167+0+DOC+PDF+V0//BG;
7. ДИРЕКТИВА 2006/24/ЕО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО http://www.cpdp.bg/?p=element&aid=427;
8. Закон за защита на личните данни http://www.cpdp.bg/?p=element&aid=373;
9. 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;
10. 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 широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“ {SEC(2009) 399} {SEC(2009) 400} COM(2009) 149 окончателен, Брюксел, 30.3.2009 http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,bg&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=493232:cs&page=
11. СТАНОВИЩЕ на комисията по граждански свободи, правосъдие и вътрешни работи на вниманието на комисията по промишленост, изследвания и енергетика

относно защитата на критичната информационна инфраструктура — постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство (2011-2014/2284(INI)), Брюксел, 22.03.2012 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/ad/896/896970/896970bg.pdf;
12. НАРЕДБА ЗА ЗАДЪЛЖИТЕЛНИТЕ ОБЩИ УСЛОВИЯ ЗА СИГУРНОСТ НА АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ ИЛИ МРЕЖИ, В КОИТО СЕ СЪЗДАВА, ОБРАБОТВА, СЪХРАНЯВА И ПРЕНАСЯ КЛАСИФИЦИРАНА ИНФОРМАЦИЯ Приета с ПМС № 99 от 10.05.2003 г. Обн. ДВ. бр.46 от 20 Май 2003г., изм. ДВ. бр.44 от 9 Май 2008г., изм. ДВ. бр.57 от 24 Юли 2009г., изм. ДВ. бр.101 от 18 Декември 2009;
13. http://www.anixter.com/AXECOM/AXEDocLib.nsf/(UnID)/F9F7765DAF87FF1B86257383004E9C5F/$file/Data_Center_Guide.pdf;
14. https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/3795-102-1-10517/Introduction%20to%20Data%20Centres.pdf;
15. http://dcseurope.info/pdf/An-Introduction-to-Data-Center-Infrastructure-Management-English.pdf;
16. http://ece.aed.org/publications/mshs/dataanalysis/WebDataAnalysis.pdf;
17. http://www.emc.com/collateral/emc-perspective/h5843-green-data-ctr-ep.pdf;
18. http://www.apcmedia.com/salestools/NRAN-69ANM9_R1_EN.pdf;
19. БДС EN 50173-1:2011. Информационни технологии. Системи за структурно окабеляване. Част 1: Общи изисквания. http://www.bds-bg.org/standard/info.php?standard_id=56422;
20. БДС EN 50173-5:2007. Информационни технологии. Системи за структурно окабеляване. Част 5: Центрове за данни. http://www.bds-bg.org/standard/info.php?standard_id=45878;
21. БДС EN 50173-5:2007/A1:2010. Информационни технологии. Системи за структурно окабеляване. Част 5: Центрове за данни. http://www.bds-bg.org/standard/info.php?standard_id=55309;
22. НАРЕДБА № 7 от 8.06.1998 г. за системите за физическа защита на строежите http://www.gli.government.bg/upload/docs/2012-08/2_NAREDBA_7_ot_8061998_g_za_sistemite_za_fiziceska_zasita_na_stroejite.pdf;
23. **ANSI/TIA-942-2005**. Telecommunications Infrastructure Standard for Data Centers. TELECOMMUNICATIONS INDUSTRY ASSOCIATION. **Approved: April 12, 2005.** http://informatica.iessanclemente.net/manuais/images/9/9f/Tia942.pdf;
24. БДС EN 1634-3:2005/AC:2006. Изпитване на устойчивост на огън на врати и затварящи устройства. Част 3: Димозащитни врати и затварящи устройства. http://www.bds-bg.org/standard/info.php?standard_id=34396;
25. ANSI/BICSI 002-2011.Data Center Design and Implementation Best Practices Committee Approval: January 2011. First Published: March 2011. http://www.bicsi.org/uploadedfiles/BICSI_002_Sample.pdf;
26. БДС EN 1047-2:2010. Хранилища за ценности. Класификация и методи за изпитване за устойчивост на огън. Част 2: Помещения за данни и контейнери за данни. http://www.bds-bg.org/standard/info.php?standard_id=52930;

27. Наредба Із -1971 от 2009 за строително-техническите правила и норми за осигуряване на безопасност при пожар http://www.nspbzn.mvr.bg/NR/rdonlyres/528EE903-5B7F-4FE9-86A9-F39C59930F48/0/NSTPNOBP.pdf;
28. Наредба №3/09.06.2004 за устройството на електрическите уредби и електропроводните линии http://www.nspbzn.mvr.bg/NR/rdonlyres/0ADA80A3-58FA-4657-9971-8B1D7691F2F4/0/NUEL.pdf;
29. НАРЕДБА № 3 от 18.09.2002 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи. http://www.build.bg/bg/law/law_doc/296.pdf;
30. БДС EN 50133-1:2004/A1:2004. Алармени системи. Системи за контрол на достъп, използвани в приложения за сигурност. Част 1: Изисквания към системата. http://www.bds-bg.org/standard/info.php?standard_id=30555;
31. БДС EN 50133-2-1:2003. Алармени системи. Системи за контрол на достъп, използвани в приложения за сигурност. Част 2-1: Общи изисквания към съставните части. http://www.bds-bg.org/standard/info.php?standard_id=24669;
32. БДС EN 50133-7:2003. Алармени системи. Системи за контрол на достъп, използвани в приложения за сигурност. Част 7: Указания за прилагане. http://www.bds-bg.org/standard/info.php?standard_id=22197;
33. БДС EN 50132-1:2010. Алармени системи. Затворени телевизионни системи за наблюдение (CCTV), използвани в приложения за сигурност. Част 1: Изисквания към системите. http://www.bds-bg.org/standard/info.php?standard_id=53825;
34. БДС EN 50132-7:2002. Алармени системи. Затворени телевизионни системи за наблюдение, използвани в приложения за сигурност. Част 7: Правилник за приложение. http://www.bds-bg.org/standard/info.php?standard_id=19762;
35. БДС EN 50132-5-2:2011. Алармени системи. Затворени телевизионни системи за наблюдение, използвани в приложения за сигурност. Част 5-2: IP протоколи за предаване на видеосигнали. http://www.bds-bg.org/standard/info.php?standard_id=57509;
36. БДС EN 54-20:2006. Пожароизвестителни системи. Част 20: Засмукващи димни пожароизвестители. http://www.bds-bg.org/standard/info.php?standard_id=48448;
37. БДС EN 12259-1:1999 + A1:2001/A2:2005. Стационарни пожарогасителни инсталации. Съставни части на спринклери и инсталации за разпръскване на вода. Част 1: Спринклери. http://www.bds-bg.org/standard/info.php?standard_id=33498;
38. БДС EN 12094-1:2003.Стационарни пожарогасителни инсталации. Съставни части на инсталациите за гасене с газообразни вещества. Част 1: Изисквания и методи за изпитване на електрически автоматични устройства за управление и задържане. http://www.bds-bg.org/standard/info.php?standard_id=23980;
39. БДС EN 12845:2004+A2:2009 Стационарни пожарогасителни инсталации. Автоматични спринклерни инсталации. Проектиране, монтиране и поддържане. http://www.bds-bg.org/standard/info.php?natstd_id=79281.

ПРИЛОЖЕНИЯ:

ПРИЛОЖЕНИЕ 1. ЕУИЦСОЧИ - Минимални изисквания за съответствие в дефинираното множество критерии