БДС Компас

Издание на Българския институт за стандартизация

Брой 4
октомври – декември 2016

УПРАВЛЕНИЕ НА РИСКА

Новите акценти в директивата за електромагнитна съвместимост

ISSN 1314-3611

БДС БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ

Българският институт за стандартизация (БИС) е националният орган по стандартизация в Република България и е създаден по реда на Закона за националната стандартизация от 2005 г. (ДВ, бр. 88 от 4 ноември 2005). БИС е обществено-правна организация, в която членуват всички заинтересовани от дейността по стандартизация фирми, организации и институции.

Нашата дейност е насочена както към непрекъснато подобряване на националната стандартизационна система и привличане на повече участници в дейността по стандартизация, така и към подобряване на управлението и организацията на работа.

Основни дейности на БИС:

- **разработва, приема и одобрява български стандарти;**
- **участва в работата на европейските и международните организации за стандартизация;**
- **издава и разпространява български стандарти, проекти и стандартизационни документи;**
- **издава официален бюлетин и каталог на българските стандарти;**
- **продава международни стандарти и чуждестранни национални стандарти и проекти;**
- **създава и поддържа база данни за стандарти и стандартизационни документи;**
- **организира курсове, семинари, конференции и други форми за обучение;**
- **създава система за оценяване на съответствието с изискванията на българските стандарти;**
- **осъществява сътрудничество със сродни организации за стандартизация от други държави.**

БИС полага усилия за сближаване и отразяване интересите на всички заинтересовани както в частния, така и в обществения сектор, ръководейки се от принципите на стандартизацията - балансирано участие, равнопоставеност, прозрачност, общо съгласие.

София 1797, жк „Изгрев“ ул. „Лъчезар Станчев“ № 13, тел.: +359 2 8174-504, факс: +359 2 8174-535

e-mail: info@bds-bg.org, www.bds-bg.org

БДС Компас

Издание на Българския институт за стандартизация

Брой 4

октомври – декември 2016

Редакционен коментар

Рискът дебне отвсякъде... И нито една организация не е застрахована, без значение от големина, предмет на дейност, обхват или географско местоположение.

Този брой на списание „БДС Компас” е посветен на тази много важна за всяка фирма дейност – управлението на риска.

Представяме речника за управление на риска *Ръководство 73 на ISO*, чиято цел е да се подобри разбирането на идеята и термините, свързани с управлението на риска.

Всяка организация по света е изправена пред вътрешни и външни фактори и влияния, които създават неувереност дали и кога ще постигне целите си. Всички дейности съдържат риск, но той се управлява, като се идентифицира, анализира и след това се преценява как да се въздейства върху него. *БДС ISO 31000 Управление на риска. Принципи и указания* описва подробно този систематичен и логичен процес. Разказваме и как се прилага ISO 31000 в Ръководството *СД ISO/TR 31004*, което дава много практически насоки при прилагането на принципите за управление на риска. *БДС EN ISO 31010 Управление на риска. Методи за оценяване на риска* е универсален стандарт, който дава указания за избор на методи за оценяване на риска в много промишлени отрасли и видове системи. Представяме методите за оценяване на риска, които може да се класифицират по различни начини, за да се помогне за разбирането на силните и слаби страни.

Информацията е може би най-важният икономически актив в наши дни. Представяме *БДС ISO/IEC 27005 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията*, който съдържа указания за управление на риска, свързан със сигурността на информацията. Стандартът е приложим за различни организации – търговски, държавни или неправителствени. Рисковете не са статични. Заплахите, уязвимостите, вероятността или последствията могат да се променят ненадейно без особена индикация. Стандартът подчертава, че е необходим постоянен мониторинг, за да се открият тези промени. Всяка организация трябва да наблюдава своите активи, необходимите модификации на стойностите на активите, заплахите, уязвимостите и инцидентите. Понякога малките рискове могат ненадейно да се превърнат в големи, или пък акумулирането на много малки рискове да причини непоправими щети.

За това как стандартите дават модел за изграждане на устойчиви системи за управление, разказва експертът Петър Лозев. Преди четвърт век са публикувани първите стандарти ISO 9001 за системи по качество, което е началото на глобално явление, довело впоследствие до разширяване на стандартите за системи за управление в областта на околната среда, здравето и безопасността при работа, образованието, здравеопазването, общините, разказва той.

И накрая нещо много важно за икономическите оператори у нас – новите акценти в директивата за електромагнитна съвместимост, представени от инж. Розалина Гичева.

Списание „БДС Компас” ще продължава да информира за всичко ново и важно в необятния свят на стандартизацията. И нека рисковете за дейността на българските фирми да са по-малки и предвидими през следващата година...

Весели празници!

Съдържание:

Главен редактор

Ефтика Георгиева

Редакционен екип

Ирен Дабижева, Росица Георгиева, Евгения Жегова, Камелия Миланова

За контакти

тел. 02/8174-511, e-mail: compass@bds-bg.org

Предпечат

Нина Николова

Български институт за стандартизация

Речникът за управление на риска

Ръководство 73 на ISO Управление на риска. Речник цели да се подобри разбирането на идеята и термините, свързани с управлението на риска, които са общоприложими за различни организации и функции, независимо от техния вид и сфера на дейност.

„БДС Компас" представя някои от основните термини:

риск влияние на неопределеността за постигането на цели	en fr	risk risque
управление на риска координирани дейности за ръководене и насочване на дадена организацията по отношение на риска	en fr	risk management management du risque
организационна рамка на управлението на риска съвкупност от елементи, създаващи основите и ръководните организационни разпоредби за разработването, внедряването, наблюдението, прегледа и непрекъснатото подобряване на управлението на риска в цялата организация	en fr	risk management framework cadre organisationnel de management du risque
политика за управление на риска декларация за общите намерения и насоченост на дадена организация по отношение на управлението на риска	en fr	risk management policy politique de management du risque
план за управление на риска програма, включена в организационната рамка на управлението на риска, определяща подхода, елементите на управлението и ресурсите, които трябва да бъдат осигурени за управлението на риска	en fr	risk management plan plan de management du risque
процес на управление на риска систематично прилагане на политика, процедури и практики за управление на дейностите за обмен на информация, за консултиране, за установяване на обстоятелствата, както и дейностите по идентифициране, анализ, преценяване, въздействие, наблюдение и преглед на риска	en fr	risk management process processus de management du risque
оценяване на риска съвкупност от процеси на идентификация, анализ и преценяване на риска	en fr	risk assessment appreciation du risque
идентификация на риска процес на откриване, разпознаване и описание на рискове	en fr	risk identification identification des risques
описание на риска структурирано представяне на риска, съдържащо обикновено четири елемента: източници, събития, причини и последствия	en fr	risk description description du risque
анализ на риска внедрен процес на разбиране за същността на даден риск и за определяне нивото на риск	en fr	risk analysis analyse du risque
матрица на риска инструмент за класиране и показване на рискове чрез определяне на категорията на последствията и тяхната възможност	en fr	risk matrix matrice de risque
ниво на риск значимост на риска или на комбинация от рискове, изразена чрез комбинация от последствия и тяхната възможност	en fr	level of risk niveau de risque
преценяване на риска процес на сравняване на резултатите от анализа на риска с критериите за риск, за да се определи дали рискът и/или неговата значимост са приемливи или допустими	en fr	risk evaluation évaluation de risque

БДС Компас

Как се управлява рискът: принципи и указания

Всяка организация по света, независимо от вид и големина, е изправена пред вътрешни и външни фактори и влияния, които създават неувереност дали и кога ще постигне целите си.

Всички дейности съдържат риск, но той се управлява, като се идентифицира, анализира и след това се преценява как да се въздейства. ***БДС ISO 31000 Управление на риска. Принципи и указания*** описва подробно този систематичен и логичен процес. Този стандарт може да бъде прилаган от различни организации с икономическа и обществена дейност.

Стандартът препоръчва процесът на управление на риска да се интегрира в процесите на управление на цялата организацията, в нейната стратегия и планиране, управление, създаване на отчети, както и в политиките, ценностите и културата на организацията.

Успехът на управлението на риска зависи от ефикасността на организационната рамка за управление. Изисква се засилен и постоянен ангажимент на ръководството, както и създаване на точен стратегически план, водещ до ангажимент на всички нива.

Преди разработването и внедряването е важно да се оценят и разберат вътрешните и външните за организацията обстоятелства. Външни са например социалната, културната, политическата, правната, финансовата, технологичната, икономическата, природната и конкурентната среда. Вътрешни са управлението, структурата, ресурсите, ролите и отговорностите на организацията.

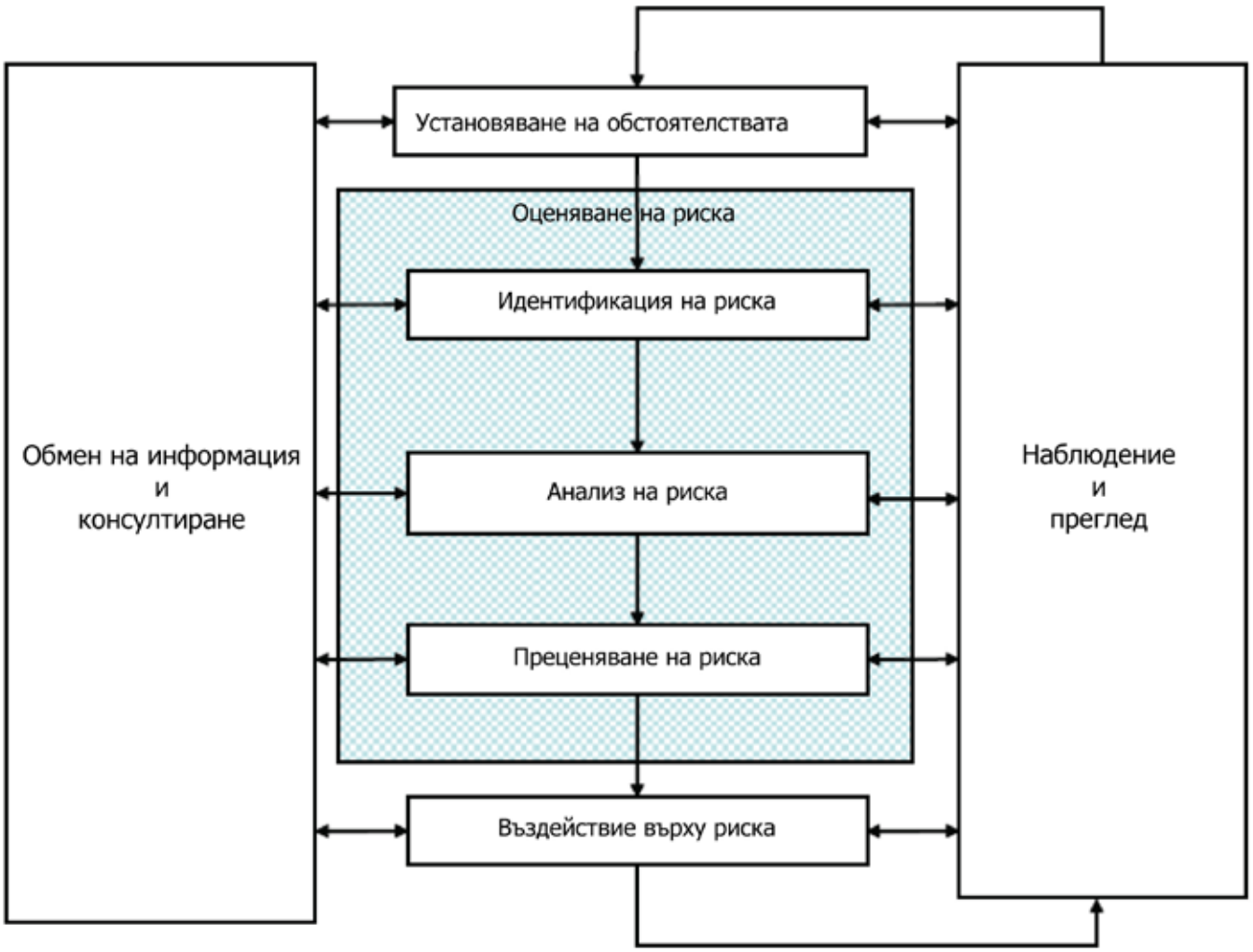
Необходимо е управлението на риска да се интегрира във всички практики и процеси по подходящ и ефективен начин. Затова организацията разработва план за управление на риска и отделя необходимите ресурси, както и създава механизми за вътрешен и външен обмен на информация.

Принципи

Управлението на риска:

- *създава стойност и я запазва.*
- *е неразделна част от организационните процеси.*
- *е неразделна част от процеса на вземане на решения.*
- *разглежда ясно неопределеността.*
- *е систематично, структурирано и своевременно.*
- *се основава на най-добрата налична информация.*
- *е приспособимо.*
- *отчита човешките и културните фактори.*
- *е прозрачно и всеобхватно.*
- *е динамично, повтарящо се и реагиращо на измененията.*
- *улеснява непрекъснатото подобряване на организацията.*

Процесът на управление на риска е показан на следната фигура:



Организацията трябва да определи критерии, позволяващи да се оцени значимостта на риска. Те отразяват ценностите, целите и ресурсите, като те може да бъдат наложени или да произтичат от задълженията за спазване на нормативни актове или на други изисквания.

Оценяването на риска е цялостен процес на идентификация, анализ и преценяване на риска.

Организацията трябва да идентифицира източниците на риск, областите на въздействие, събитията (включително изменения в обстоятелствата), както и техните причини и потенциални последствия. Този етап има за цел да се състави изчерпателен списък на рискове, които могат да провокират, подбудят, ускорят или забавят постигането на целите.

Анализът осигурява входни данни за преценяването на риска и за вземането на решения за необходимостта от въздействие и позволява да се изберат най-подходящите методи. При анализа се вземат предвид причините и източниците на риск, техните положителни и отрицателни последствия и възможността той да се появи.

Преценяването включва сравняване на нивото на риска, определено по време на процеса на анализ, с критериите за риск, разработени по време на установяването на обстоятелствата.

Въздействието върху риска включва избор и внедряване на една или повече възможности за изменението му. Веднъж внедрено, въздействието върху риска поражда или изменя средствата за неговото управление. Въздействието върху риска е повтарящ се процес за:

- *оценяване на въздействието върху риска*
- *решаване дали нивата на остатъчния риск са допустими*
- *когато не са допустими – ново въздействие върху риска и*
- *оценяване на ефикасността на това въздействие върху риска.*

Информацията, предоставена в плановете за въздействие върху риска, трябва да включва:

- *причините, с които се обосновава избора на възможности за въздействие върху риска, включително и очакваните ползи*
- *персонала, отговорен за одобряването на плана, и тези, които са отговорни за неговото прилагане*
- *предлаганите действия*
- *потребностите от ресурси, включително и тези за непредвидени разходи*
- *критериите за успех и ограниченията*
- *изискванията за контрол и наблюдение.*

Прегледът трябва да бъде част от процеса за управление на риска и да включва контрол или редовно наблюдение, които могат да са периодични или според конкретния случай. Резултатите задължително се записват с цел дейностите по управление на риска да бъдат проследими. Записите осигуряват базата за подобряване на методите и инструментите, както и на процеса като цяло.

Приложение А предоставя допълнителни препоръки за организациите, които желаят да управляват риска по-ефикасно, като непрекъснато подобряване, цялостна отговорност, прилагане на управлението на риска при всяко вземане на решения, непрекъснат обмен на информация и цялостно интегриране в структурата на управление на организацията. (БДС Компас)

Как се прилага ISO 31000

ISO 31000 обяснява как да се управлява ефикасно рискът, но не и как да се интегрира в процесите за управление на организацията. Макар че организациите са различни и техните изходни точки могат да се различават, във всички случаи е приложим общ и системен подход. Това е разяснено в ръководството ***СД ISO/TR 31004 Управление на риска. Указания за прилагането на ISO 31000***.

Ръководството дава много практически насоки за прилагането на принципите за управление на риска. Така например, за да се приведе в действие принципът ***„Управлението на риска е неразделна част от процеса на вземане на решение"***, от самото начало трябва да бъдат разгледани внимателно въпроси като:

- *Как и къде в организацията се вземат решения?*
- *Кой е включен в процеса на вземане на решения?*
- *Какви знания и умения са необходими на тези, които вземат решения?*
- *Какви указания и помощ са необходими за съществуващия персонал?*
- *Как ще бъдат засегнати външните заинтересовани страни?*
- *Какви процеси за вземане на решения в организацията трябва да се променят?*

В стандартизационния документ са дадени примерни въпроси, свързани с организацията и човешките ресурси, на които би било полезно да се даде отговор:

- *Съответства ли организационната структура на потребностите на организацията?*
- *Ясно ли са определени лицата с официални отговорности?*
- *Съдържат ли всички длъжностни характеристики ясни описания на правомощията и отговорностите на отделните лица?*
- *Дали всички канали за обмен на информация са ясни и ефикасни?*
- *Извършват ли се периодични проверки дали съобщената информация е разбрана и разтълкувана правилно на всички нива в организацията?*
- *Наблюдава ли се моралната атмосфера в организацията?*
- *Извършва ли се преглед на взаимодействието между отделните екипи?*
- *Съществуват ли механизми, които да разпознават и реагират на слухове в рамките на организацията, преди те да повлияят по негативен начин?*
- *Има ли ясни политики за начина на назначаване, заплащане и повишение?*
- *Ако политиките създават проблеми, има ли процес за тяхното преразглеждане?*
- *Спазват ли се политиките и процедурите? Ако не се спазват, има ли разследване. Приведени ли са в действие?*
- *Проверяват ли вътрешните и външните одитори за случаи на небезопасно или неетично поведение в организацията?*

Дори и малките организации трябва да отчитат глобалните изменения, например финансовата криза от 2008 г. оказа сериозно въздействие върху някои по-дребни доставчици, чиито основни клиенти бяха засегнати пряко или косвено

от банкови фалити. Такива външни събития или нововъзникващи обстоятелства могат да изискват активни промени в организационната рамка за управление на риска.

Вътрешните характеристики, които може да бъдат изменени, включват:

- *структура*
- *управленски практики и изисквания*
- *политики, вътрешни норми и модели*
- *договорни изисквания*
- *стратегически и оперативни системи, повлияни от вътрешни или външни фактори (например, промени в нормативни актове)*
- *възможности и ресурси (например, финансов капитал, репутация, време, хора, процеси, системи и технологии)*
- *знания, умения и интелектуална собственост*
- *информационни системи и потоци*
- *социално, екологично и културно поведение*
- *други приоритети на организацията и неотложни изисквания, които могат да бъдат възприети като конкуриращи се с намеренията на организацията за управление на риска.*

Водещи показатели, които биха могли да насочат вниманието към изменения във външната среда, са:

- *определяне на цените на търговски артикули, лихвени проценти на банките, доходност на облигации, валутни курсове, индекси на фондовия пазар, индекс на потребителските цени (тенденции)*
- *индекс (тенденции)*
- *ниво или случаи на измами в подобни организации*
- *данни за големина на пазара и растеж и внезапни промени в обема на поръчките*
- *политическа и социална стабилност, социално недоволство и демонстрации.*

Ако средата, в която работи организацията, се е променила след разработването на организационната рамка за управление на риска, тя трябва да бъде оценена повторно и приведена в съответствие с тези промени.

Освен интегриране на управлението на риска с основните процеси на дейността е необходимо да се създаде взаимодействие между всички разновидности на системата за управление, например управление на качеството, управление по отношение на околната среда, управление на безопасността, управление на сигурността, спазване на изискванията, финансова и управленска отчетност и дори с управление на застраховането, насочено към събития, които могат да бъдат финансово прехвърлени към други организации. Тези отделни системи за управление трябва да формират интегрирана система за управление, основана на политиката и стратегията на организацията. Дори когато има отделни системи за управление, за да се управляват определени рискове, организационната рамка за управление на риска трябва да се разшири и да ги включи.

Такъв подход за управление на риска може да включва следното:

- *прилагане в системата за управление на качеството на методи за управление на риска, които се отнасят основно за управление на риска за продукти и проекти*
- *въздействие върху неопределеността в управлението по отношение на околната среда, например инциденти и потенциални злополуки в опасни помещения, обезвреждане на опасни материали и вещества*
- *въздействие върху рисковете, комбинирано с дейности като безопасност при работа*
- *въздействие върху рисковете за сигурността, например действия на насилие срещу организацията или нейни служители или клиенти*
- *въздействие върху рисковете за сигурността на информационните технологии (ИТ), например прекъсване на функционирането на ИТ, загуба на данни, нарушаване на поверителността и осигуряване на непрекъснатост на дейността*
- *управление на рисковете за непрекъснатост на дейността, с което да се осигури подготовка и бърза реакция*
- *установяване на мерки за контрол за защита на активите на организацията с цел осигуряване на правилно докладване, за гарантиране на съответствие с изискванията на нормативните актове или за управление на рискове, подлежащи на застраховане, по начин, който свежда до минимум застрахователните премии. (БДС Компас)*

Методите за управление на риска

БДС EN ISO 31010 Управление на риска. Методи за оценяване на риска е универсален стандарт, който дава указания за избор на методи за оценяване на риска в много промишлени отрасли и видове системи.

Методите за идентификация на риска може да включват:

- *методи, основани на доказателства, примери за които са списъци за проверка и прегледи на данни за минали периоди*
- *системни екипни подходи, когато екип от специалисти следва системен процес, за да идентифицира рискове чрез структуриран набор от напомняния или въпроси*
- *методи за индуктивно разсъждение, например HAZOP (Изследване на опасностите и работоспособността).*

Може да се използват различни помощни средства за подобряване на точността и пълнотата при идентифициране на рисковете, включително провеждане на „мозъчна атака" и методологията „Делфи".

Методите, използвани при анализа на рискове, може да са качествени, полуколичествени или количествени. Необходимата степен на подробност зависи от конкретното приложение, наличието на надеждни данни и потребностите на организацията.

Качественото оценяване определя последствията, вероятността и нивото на риска чрез термини като „високо", „средно" и „ниско". Полуколичествените методи използват цифрови скали за оценяване на последствията и на вероятността и ги комбинират, за да получат нивото на риска, като използват формула. Количественият анализ пък дава оценки на фактически стойности за последствията и техните вероятности, както и стойности за нивото на риска в конкретни единици.

Стандартът посочва, че разпространен е подходът, който разделя рисковете на три зони:

- *горна зона, където нивото на риска се счита за недопустимо, каквито и да са ползите, които може да донесе дейността, и въздействието върху риска е от съществено значение, каквато и да е неговата цена*
- *средна зона (или „сива" област), когато разходите и ползите се вземат предвид и благоприятните възможности се съпоставят с потенциалните последствия*
- *долна зона, където нивото на риска се счита за пренебрежимо или толкова малко, че не са необходими мерки за въздействие върху риска.*

Оценяването на риска може да се извършва с различна задълбоченост и подробност и с използване на един или повече методи – от прости до сложни. Подходящият метод трябва да:

- *бъде обоснован и подходящ за ситуацията или организацията*
- *дава резултати във вид, който разширява разбирането на естеството на риска и как да се въздейства върху него*
- *бъде годен за ползване по начин, който е проследим, повторим и проверим.*

Основанията за избора на метод трябва да са посочени, като се държи сметка за съответствието и пригодността му. Когато се обединят резултатите от различни изследвания, използваните методи и резултати трябва да са сравними.

Методът се избира на основата на приложими фактори като:

- *Целите на изследването; например, ако се предприема сравнително изследване между различни възможности, може да се окаже приемливо да се използват не много подробни модели на последствията.*
- *Потребностите на хората, вземащи решения. В някои случаи високата степен на подробност е необходима за вземането на правилно решение, в други по-общото разбиране е достатъчно.*

- *Видът и обхватът на анализираните рискове.*
- *Потенциалната величина на последствията.*
- *Степента на експертен опит и знания, човешки и други необходими ресурси. Опростеният метод, когато е използван правилно, може да осигури по-добри резултати, отколкото по-сложна, но лошо приложена процедура.*
- *Наличието на информация и данни. Някои методи изискват повече информация и данни, отколкото други.*
- *Необходимостта от актуализиране на оценяването на риска. Оценяването може да е необходимо да се актуализира в бъдеще и някои методи в това отношение са по-пригодни за изменения от други.*
- *Всички нормативни и договорни изисквания.*

Методите за оценяване на риска може да се класифицират по различни начини, за да се помогне за разбирането на техните относително силни и слаби страни. Следната таблица показва приложимостта на методите, използвани за оценяване на риска.

Инструменти и методи	Процес на оценяване на риска				
	Идентификация на риска	Анализ на риска			Преценяване на риска
		Последствие	Вероятност	Ниво на риска	
Мозъчна атака	ПР	НП	НП	НП	НП
Структурирани или полуструктурирани интервюта	ПР	НП	НП	НП	НП
Метод „Делфи”	ПР	НП	НП	НП	НП
Списъци за проверка	ПР	НП	НП	НП	НП
Предварителен анализ на опасностите (PHA)	ПР	НП	НП	НП	НП
Изследване на опасностите и работоспособността (HAZOP)	ПР	ПР	П	П	П
Анализ на опасностите и контрол на критичните точки (HACCP)	ПР	ПР	НП	НП	ПР
Оценяване на рисковете за околната среда	ПР	ПР	ПР	ПР	ПР
Структуриран анализ “Какво ще стане, ако?” (SWIFT)	ПР	ПР	ПР	ПР	ПР
Анализ на сценариите	ПР	ПР	П	П	П
Анализ на влиянието върху дейността	П	ПР	П	П	П
Анализ на основните причини	НП	ПР	ПР	ПР	ПР
Анализ на появяването на дефекти и на последствията от тях (FMEA)	ПР	ПР	ПР	ПР	ПР
Анализ чрез дърво на отказите	П	НП	ПР	П	П
Анализ чрез дърво на събитията	П	ПР	П	П	НП
Причинно-следствен анализ (CCA)	П	ПР	ПР	П	П
Анализ на причинно-следствените връзки	ПР	ПР	НП	НП	НП
Анализ на нивата на защита (LOPA)	П	ПР	П	П	НП
Дърво на решенията	НП	ПР	ПР	П	П
Анализ на надеждността на човешкия фактор	ПР	ПР	ПР	ПР	П
Анализ “Възелът на папийонката”	НП	П	ПР	ПР	П
Техническо обслужване на база на безотказност	ПР	ПР	ПР	ПР	ПР
Преходен анализ и анализ на скритите състояния	П	НП	НП	НП	НП
Анализ на Марков	П	ПР	НП	НП	НП
Имитационно моделиране по метода „Монте Карло”	НП	НП	НП	НП	ПР
Бейсова статистика и Бейсови мрежи	НП	ПР	НП	НП	ПР
FN криви	П	ПР	ПР	П	ПР
Показатели на риска	П	ПР	ПР	П	ПР
Матрица на последствията/вероятностите	ПР	ПР	ПР	ПР	П
Анализ на разходите и ползите	П	ПР	П	П	П
Многокритериен анализ на решенията (MCDA)	П	ПР	П	ПР	П
Забележка: Съкращенията означават: Препоръчителен (ПР), Неприложим (Н), Приложим (П)					

Всеки един от методите е разяснен допълнително в отделно приложение, отнасящо се за естеството на оценяването, което те предлагат, и указанията за тяхната приложимост в някои ситуации. Описани са подробно всичките 36 метода заедно с преимуществата и недостатъците в използването им. (БДС Компас)

Как се управлява рискът за сигурността на информацията

БДС ISO/IEC 27005 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията предоставя указания за управление на риска за сигурността на информацията и е в подкрепа на изискванията на системата за управление на сигурността на информацията (СУСИ). Стандартът обаче не определя специфичен метод за това, а от самата организация зависи как ще определи своя подход към управлението на риска в зависимост например от обхвата й или сектора от индустрията. Стандартът е приложим за всякакъв вид организации – търговски, държавни или неправителствени.

Управлението на риска за сигурността на информацията трябва да бъде непрекъснат процес, който може да бъде приложен към организацията като цяло, към всяка отделна нейна част (например отдел, физическо местоположение, услуга), към всяка информационна система или към специфични аспекти на контрола на дейността й.

В една система за управление на сигурността на информацията установяването на контекста, оценяването на риска, разработването на план за третирането и приемането му са част от модела „Планиране–Изпълнение–Проверка–Действие" (PDCA – Plan–Do–Check–Act). Таблицата обобщава дейностите по управление на риска за сигурността на информацията, приложими към четирите фази на процеса на СУСИ:

Процес на СУСИ	Процес на управление на риска за сигурността на информацията
Планиране	Установяване на контекста Оценяване на риска Разработване на план за третиране на риска Приемане на риска
Изпълнение	Изпълнение на плана за третиране на риска
Проверка	Непрекъснат мониторинг и преглед на рисковете
Действие	Поддържане и подобряване на процеса за управление на риска за сигурността на информацията

Критериите за риска трябва да бъдат разработени, като се взема предвид:

- *стратегическата стойност на информационния процес за дейността на организацията*
- *критичността на включените информационни активи*
- *законовите и регулаторни изисквания, както и договорните задължения*
- *оперативната и бизнес значимост на наличността, конфиденциалността и целостта*
- *очакванията и разбиранията на заинтересованите страни, отрицателни последствия за доброто име и репутацията.*

Критериите за въздействие са разработват, като се взема предвид:

- *нивото на категоризация на информационния актив, върху който е оказано въздействие*
- *пробивите в сигурността на информацията (например загуба на конфиденциалност, интегритет и наличност)*
- *намалената работоспособност (вътрешна или на трети страни)*
- *загуба на дейност или обезценяване*
- *нарушаване на планове и срокове*
- *вреда за репутацията*
- *неспазване на законови, регулаторни или договорни изисквания.*

Критерии за приемане на риска се разработват, като се вземат предвид:

- *различни прагове с желаното крайно ниво на риска, но с осигурено одобрение от страна на висшето ръководство за приемане на рискове над тези нива при определени обстоятелства,*
- *че могат да бъдат представени като съотношение на очакваната печалба (или друга бизнес полза) към преценения риск,*
- *че различни критерии могат да бъдат прилагани към различни класове риск. Например тези, които могат да доведат до несъответствие с нормативните актове, не могат да бъдат приети, но може да бъде допуснато приемане на сериозни рискове, ако това е определено като договорно изискване,*
- *че могат да включват изисквания за бъдещо допълнително третиране. Например рискът може да бъде приет, ако има одобрение и задължение за действие за намаляването му до приемливо ниво за определен срок,*
- *че могат да се различават в зависимост от това колко продължително се очаква да съществува този риск,*
- *бизнес критерии, законови и регулаторни аспекти, дейности, технология, финанси, социални и хуманитарни фактори.*

Рисковете не са статични. Заплахите, уязвимостите, вероятността или последствията могат да се променят ненадейно без някаква индикация. Стандартът подчертава, че е необходим постоянен мониторинг, за да се открият тези промени. Всяка организация трябва да наблюдава своите активи, необходимите модификации на стойностите на активите, заплахите, уязвимостите и инцидентите. Понякога малките рискове могат ненадейно да се превърнат в големи, или пък акумулирането на много малки рискове да причини непоправими щети.

Организацията трябва да идентифицира и опише активите си на приемливо ниво на подробност. ***Стандартът посочва два вида активи:***

- *основни – бизнес процеси и дейности и информация (например процеси, чиято загуба прави невъзможно изпълнението на ключови дейности, секретни или съдържащи частни технологии, договорни, законови или регулаторни изисквания).*
- *съпровождащи – хардуер, софтуер, мрежа, персонал, местоположение, организационна структура.*

Заплахите могат да бъдат преднамерени, случайни или вследствие от обкръжаващата среда (природни) и могат да водят до щети или прекратяване на услуги от първа необходимост. Таблицата дава примери за типични заплахи:

Вид	Заплаха
Физически щети	Пожар
	Щети от вода
	Замърсяване
	Голяма катастрофа/злополука
	Разрушаване на устройства или носител
	Прах, корозия, замръзване
Природни събития	Климатично явление
	Сеизмично явление
	Вулканично явление
	Метеорологично явление
	Наводнение
Прекратяване на услуги от първа необходимост	Повреда на климатична или водоснабдителна система
	Прекратяване на електроснабдяване
	Повреда на телекомуникационни устройства
Смущения от излъчване	Електромагнитно излъчване
	Термично излъчване
	Електромагнитни импулси
Компрометиране на информация	Подслушване на компрометирани смущаващи сигнали
	Отдалечено шпиониране
	Подслушване
	Кражба на носител или документи
	Кражба на устройства
	Възстановяване на рециклирани или изхвърлени носители
	Разкриване
	Данни от недостоверни източници
	Фалшифициране с хардуер
	Фалшифициране със софтуер
	Разкриване на позиция
Технически повреди	Повреда на устройства
	Неизправност на устройства
	Насищане на информационната система
	Неизправност на софтуер
	Пробив в експлоатируемостта на информационна система
Неоправомощени действия	Неразрешено използване на съоръжения
	Измамно копиране на софтуер
	Използване на подправен или копиран софтуер
	Разрушаване на данни
	Противозаконно обработване на данни
Компрометиране на функции	Грешка при използване
	Злоупотреба с права
	Фалшифициране на права
	Отказ на действия
	Пробив в наличността на персонала

Стандартът подчертава, че специално внимание трябва да се обърне на източниците на заплахи, свързани с човешка дейност. Те са посочени също в таблица:

Произход на заплахата	Мотивация	Възможни последствия
Хакер, кракер	Предизвикателство Его Недоволство Състояние Пари	• Хакерство • Социален инженеринг • Проникване в система, пробиви • Неразрешен достъп до системата
Компютърен престъпник	Разрушаване на информацията Противозаконно разкриване на информация Спечелване на пари Неоторизирана промяна на данни	• Компютърно престъпление (например престъпно дебнене) • Акт на измама (например повторение, деперсонификация, подслушване) • Продажба на информация • Измама • Проникване в система
Терорист	Изнудване Разрушаване Експлоатация Отмъщение Политически ползи Медийно покритие	• Бомба/тероризъм • Информационна война • Системна атака (например разпределен отказ на услуга) • Проникване в системата • Фалшифициране на системата
Промишлен шпионаж (разузнаване, организации, чуждестранни правителства, други правителствени интереси)	Конкурентно предимство Икономически шпионаж	• Отбранително предимство • Политическо предимство • Икономическа експлоатация • Кражба на информация • Нарушаване на личното пространство • Социален инженеринг • Проникване в системата • Неразрешен достъп до системата (достъп до класифицирана, лична и/или свързана с технологиите информация)
Вътрешни за организацията лица (лошо обучени, недоволни, злонамерени, небрежни, нечестни или уволнени служители)	Любопитство Его Разузнаване Печелене на пари Отмъщение Неумишлени грешки и пропуски (например грешка при въвеждане на данни, грешка при програмиране)	• Нападение на служител • Изнудване • Разглеждане на лична информация • Злоупотреба с компютър • Измама и кражба • Продажба на информация • Въвеждане на фалшиви, опорочени данни • Подслушване • Злонамерен код (например вирус, логическа бомба, троянски кон) • Продажба на лична информация • Дефекти в системата • Проникване в системата • Саботаж на системата • Неразрешен достъп до системата

Петър Лозев: Стандартите дават модел за изграждане на устойчиви системи за управление

Визитка

Петър Лозев е секретар на БИС/ТК 34 „Управление на качеството и оценяване на съответствието”. Завършил е специалност „Международни икономически отношения” в УНСС-София. Има специализация по „Европейска интеграция” към Софийския университет „Св. Климент Охридски”. Водещ одитор на системи за управление на качеството по ISO 9001, системи за управление на околната среда по ISO 14001 с IRCA сертификати от LRQA, BVQI и TÜV Rheinland.

– Откога се занимавате със стандартизация?

– Началото на моя опит в областта на стандартите е от 2003 г. като експерт международна дейност в ИА „Сертификация и изпитване”. Поводът бе участие в дейностите по акредитация от Холандския орган за акредитация RVA. Изискванията за акредитиране на орган за сертификация на продукти изискваха познаването на редица европейски и международни стандарти и директиви, свързани с изискванията за документацията, структурата и управлението на органа, вземането на решения за сертификация, системата за управление на качеството. От 2007 притежавам сертификат на LRQA за одитор по системи за управление на качеството ISO 9001 и сертификат на BVQA за HACCP системи. От 2009 г. съм определен за секретар на БИС/ТК 34 „Управление на качеството и оценяване на съответствието”.

– Доколко са важни стандартите във Вашата област?

– Преди четвърт век, през декември 1987 г., са публикувани първите стандарти ISO 9001 за системи по качество: модел за осигуряване на качеството в проектирането/разработването, производството, монтажа и сервиза. Това бе началото на глобално явление, което впоследствие доведе до разширяване на стандартите за системи за управление в областта на околната среда, здравето и безопасността при работа, системи за управление в областта на образованието, здравеопазването, общините и наличие на акредитирани сертификати, приближаващи цифрата 1,5 милиона.

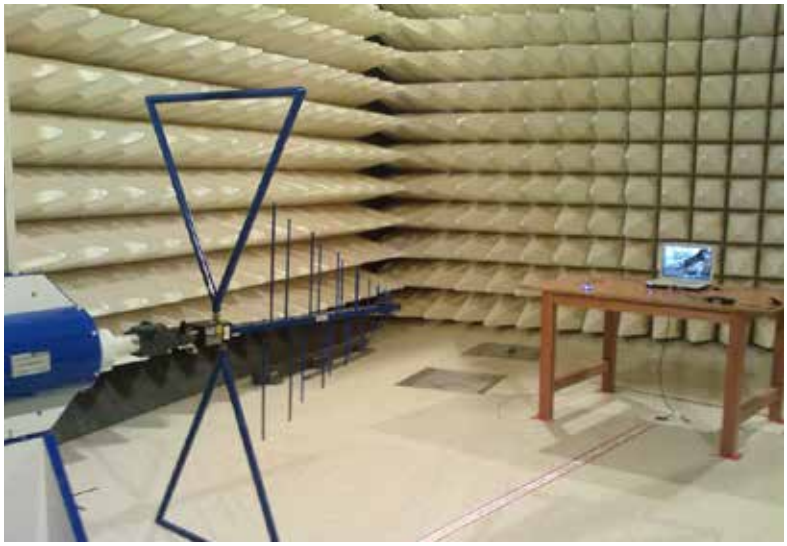
От началото на 2015 г. имаме ново такова значително събитие в областта на стандартите за системи за управление, което вече оказва влияние на цялата верига организации, обучители, консултанти, органи за сертификация, органи за акредитация, одитори и стандартизатори. Това е публикуването на приложение SL (преди това Ръководство ISO 83) към част 2 на Директивите на ISO, което определя общата рамка, терминология и основния текст за стандартите за системи за управление. Всички нови стандарти на ISO за системи за управление ще се придържат към тази рамка и всички настоящи стандарти за системи за управление ще се преработят по тази рамката при следващата им редакция. Така бъдещите стандарти за системи за управление на ISO ще изглеждат по един и същ на-

чин и ще носят усещането за познатост и разбираемост. Очаква се това да е началото на края на конфликтите, дублирането, объркването и недоразуменията, произтичащи досега от различните структури и терминологии на тези стандарти. Освен това, дава се възможност на организациите и всички заинтересовани страни да насочат вниманието си най-вече върху основните дейности и спецификата на организацията, а също и управлението на рисковете при интегриране и прилагане на различните системите за управление, касаещи качеството, околната среда, сигурността на информацията, здравето и безопасността при работа и други. Намеренията са тази нова структура да устои на предизвикателствата на следващите 20 години.

– Това, че по дефиниция са доброволни, означава ли, че може и без тях?

– Тук ще отговоря с любимата фраза на д-р Деминг (считан за основател на тоталното управление на качеството): Да оцеляваш, е въпрос на избор (Survival is optional). Никой не може да те накара насила да бъдеш в крак с времето и развитието. Отдавна е известно в международен мащаб, че едва 50% от стартиращите фирми оцеляват до петата година (за България този показател е едва 7% оцеляващи фирми). Тук е силата на стандартите да дадат модела и най-добрата практика за изграждане на устойчиви системи за управление на фирмите, основани на тяхната стратегия и дългосрочната визия. Разработването на стандарти в областта на управление на качеството целят, от друга страна, непрекъснато подобряване на взаимодействието във веригата на доставки. Това налага всеки в зависимост от мястото си да прилага максимално изискванията на стандарта и да допринася за подобряването по цялата верига. От тази гледна точка да считаш прилагането на стандартите за доброволно, е равносилно на това сам да предрешиш съдбата си.

Новите акценти в директивата за електромагнитна съвместимост



Визитка

Инж. Розалина Гичева е завършила ВМЕИ, София (сега Технически университет). Има специализация „Манипулатори и роботи“ отново във ВМЕИ. От 2002 г. заема длъжността ръководител-отдел „Оценяване съответствието на Машини”, към „Център за изпитване и европейска сертификация“ ЕООД Стара Загора. Участва като експерт в БИС/ТК 52 „Безопасност на машините”.

Нова Директива за електромагнитна съвместимост (2014/30/ЕС) – нови акценти за икономическите оператори при нейното прилагане

Директива 2014/30/ЕС за електромагнитна съвместимост (ЕМС) влезе в сила на 18 април 2014 г. и се прилага от 20 април 2016 г. За разлика от повечето други директиви от Нов подход, основен акцент на директивата за ЕМС е не безопасността, а по-скоро функционирането на съоръженията, които могат да бъдат източник на смущаващи електромагнитни въздействия, или работата им може да се влияе от такива въздействия.

Необходимостта от промяната на Директива 2004/108/ЕО беше продиктувана от създаването на Новата законодателна рамка:

- *1. Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г., който определя изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти, правилата за акредитацията на органите за оценяване на съответствието, предвиди рамка за надзора на пазара на продукти и за осъществяване на контрол върху продуктите от трети държави, установи основните принципи относно маркировката „CE”.*
- *2. Решение № 768/2008/ЕО на Европейския парламент и на Съвета от 9 юли 2008 г. относно обща рамка за предлагането на пазара на продукти установи общи принципи и референтни разпоредби, предназначени за прилагане в секторното законодателство, с цел да се създаде последователна основа за преразглеждането или преработването на това законодателство, ясно и пропорционално разпределение на задълженията, което отговаря на ролята на всеки икономически оператор във веригата на доставка и дистрибуция.*
- *3. Завишаване на изискванията в критериите, установени в Директива 2004/108/ЕО, които трябва да бъдат изпълнени от органите за оценяване на съответствието, за да бъдат нотифицирани.*

Приложно поле (обхват) на Директива 2014/30/ЕС

Обхватът като цяло остава същият, а промените на задълженията на производителите са малко, като основно се гарантира, че директивата следва общите принципи на член 30 от Регламент (ЕО) № 765/2008.

Директива 2014/30/ЕС се прилага за голяма част от електрическите съоръжения, независимо какво е тяхното захранване (дали работят с батерия или са включени в захранващата мрежа).

Изключват се:

- *радионавигационно оборудване и далекосъобщително крайно оборудване*
- *въздухоплавателни средства*
- *радиосъоръжения, използвани от радиолюбители по смисъла на регламентите за радиосъобщенията*
- *съоръжения, които не могат да генерират или не допринасят за генерирането на електромагнитни излъчвания*
- *съоръжения, които работят без неприемливо влошаване при наличието на смущаващи електромагнитни въздействия, които обикновено се появяват вследствие използването на съоръженията по предназначение*
- *съоръжения, които превишават нивата, позволяващи нормалната работа на радио-, далекосъобщителни и други съоръжения, комплекти за изпитване, изработени по поръчка и предназначени за професионалисти, които се използват единствено в местата за извършване на научноизследователска и развойна дейност и за такива цели.*

Определения

- ***„съоръжение“*** *означава всяко устройство или неподвижно монтирана инсталация*
- ***„устройство“*** *означава всеки завършен уред или комбинация от уреди, предоставени на пазара като самостоятелна функционална единица, предназначени за крайния ползвател, и които могат да бъдат източник на смущаващи електромагнитни въздействия, или работата на които може да се влияе от такива въздействия*
- ***„неподвижно монтирана инсталация“*** *е конкретна комбинация от няколко вида устройства и, когато е приложимо, други уреди, които се сглобяват, монтират и са предназначени за постоянна експлоатация на предварително определено място.*

Съществени изисквания

Съществените изисквания за устройствата не са променени, но някои от изискванията за неподвижно монтирани инсталации и прилагането на добра инженерна практика вече не се съдържат в Приложение I, а в текста на директивата (член 19).

Формално несъответствие

Определени са случаите на формално несъответствие (член 40):

- *а) маркировката „CE“ е нанесена в нарушение на член 30 от Регламент (ЕО) № 765/2008 или на член 17 от Директива 2014/30/ЕС*
- *б) не е нанесена маркировка „CE“*
- *в) не е съставена ЕС декларация за съответствие*
- *г) неправилно съставена ЕС декларация за съответствие*
- *д) непълна или липсваща техническа документация*
- *е) информацията, посочена в член 7, параграф 6 или член 9, параграф 3, липсва, не е вярна или е непълна*
- *ж) не е изпълнено някое друго административно изискване, предвидено в член 7 или член 9.*

В правомощията на надзор на пазара е да изиска от съответния икономически оператор да коригира несъответствието или да предприеме всички необходими мерки да ограничи или да забрани предоставянето на устройство на пазара, или да осигури неговото изземване или изтегляне от пазара.

Процедури за оценяване на съответствието

Съответствието на дадено устройство със съществените изисквания, установени в приложение I, се доказва чрез една от следните процедури за оценяване на съответствието:

- *а) „вътрешен производствен контрол“, описан в приложение II*
- *б) „ЕС изследване на типа“, следвано от съответствие с типа въз основа на „Вътрешен производствен контрол“, описани в приложение III.*

Производителят и в двата случая прилага процедура „вътрешен производствен контрол“, но може да избере процедурата „ЕС изследване на типа“ (приложение III на директивата), като има право да ограничи прилагането й до някои аспекти на съществените изисквания, при условие че за останалите аспекти се прилага процедура „вътрешен производствен контрол“ (приложение II).

Задължения на икономическите оператори

Подробно са конкретизирани задълженията на икономическите оператори (производител, упълномощен представител, вносител, дистрибутор) въз основа на задълженията им, определени в Новата законодателна рамка.

Случаи, при които задълженията на производителите се прилагат и към вносителите и дистрибуторите:

Вносител или дистрибутор се счита за производител, когато пуска електрически съоръжения на пазара със своето име или търговска марка или променя електрически съоръжения, които са пуснати на пазара, по такъв начин, че съответствието с директива може да бъде засегнато.

Техническа документация

Съдържанието на техническото досие включва в допълнение извършен „анализ и оценка на риска(овете)“ като част от техническата документация.

Техническата документация трябва да обхваща, доколкото това е необходимо, проектирането, производството и експлоатацията на съоръжението. Техническата документация трябва да включва най-малко следните елементи:

- *а) общо описание на устройството*
- *б) конструктивни и производствени чертежи и схеми на компонентите, сглобените единици, електрическите вериги и др.*
- *в) описанията и обясненията, необходими за разбиране на тези чертежи и схеми и за действието на устройството*
- *г) списък на хармонизираните стандарти, приложени изцяло или частично, описания на решенията, приети за изпълнение на съществените изисквания на директивата. При частично приложени хармонизирани стандарти техническата документация посочва частите, които са приложени*
- *д) резултати от извършените проектни изчисления, проведените изследвания и др.*
- *е) протоколи от изпитвания.*

Информация относно използването на устройството

Устройството се придружава от информация относно специфичните предпазни мерки, които следва задължително да се вземат при сглобяването, монтажа, поддържането или използването на устройството, за да се гарантира, че когато бъде пуснато в действие, устройството ще е в съответствие със съществените изисквания, приложими за него.

Устройство, което отговаря на изискванията за използване в промишлена среда, но при работа в жилищна среда не отговаря на съществените изисквания, се придружава от ясно обозначение за това ограничение за използване, което се нанася, ако е подходящо, и върху опаковката.

В инструкциите, придружаващи устройството, трябва да се съдържа информация, необходима за използването на устройството по предназначение.

ЕС декларация за съответствие

Декларацията за съответствие се съставя по образец, установен в приложение IV, като съдържа елементите, посочени в модулите на приложения II и III, в зависимост от прилаганата процедура и се актуализира редовно. Тя трябва да бъде преведена на езика или езиците, изисквани от държавата членка, в която устройството се пуска или предоставя на пазара.

Трябва да бъде включена подходяща идентификация на устройството, която да е достатъчна, за да позволи проследяването му (това може да включва достатъчно ясно цветно изображение, когато това е необходимо за идентификация на устройството).

Задълженията на производителя за нанасяне на маркировка „CE“ и съставяне на писмена „ЕС декларация за съответствие“ могат да бъдат изпълнявани от негов упълномощен представител, от негово име и на негова отговорност, при условие че са посочени в пълномощието.

Идентификация на икономическите оператори

По искане на органите за надзор на пазара икономическите оператори идентифицират:

- *а) всеки икономически оператор, който им е доставил дадено устройство*
- *б) всеки икономически оператор, на когото са доставили дадено устройство.*

Икономическите оператори следва да могат да предоставят тази информация в продължение на 10 години, след като устройството им е било доставено, и в продължение на 10 години, след като те са доставили устройството.


БДС
Българският институт за стандартизация Ви честити Коледните и Новогодишни празници и Ви пожелава ползотворна 2017 г.!