ročník 2024 | číslo 4

# MAGAZÍN ČAS

neprodejné

Předali jsme
**Ocenění Vladimíra Lista za rok 2024**

**Kybernetická bezpečnost:**
Jak na ochranu dat

V platnost vstoupila
**nová edice ČSN 33 2130**

foto: freepik.com

**www.agenturacas.gov.cz**
**www.magazin-cas.cz**

Elektronická verze

# Obsah




**MAGAZÍN ČAS 4/2024**
Čtvrtletník
Tištěný náklad 9000 ks
Vychází dne 31. 12. 2024
Vydává: Česká agentura pro standardizaci s.p.o., se sídlem 110 00 Praha 1, Biskupský dvůr 1148/5, IČO: 06578705
Zaregistrováno MK ČR pod evidenčním číslem MK ČR E 23480
ISSN 2694-6912 (Print),
ISSN 2694-6920 (Online)
Předseda redakční rady: Karel Novotný
Tajemnice: Petra Londová
Redakční rada: Patrik Frk, Zdenka Slaná, Lubomír Keim, Ivana Kolínská, Jiří Nouza, Daniel Novotný, Jan Mládek, Filip Žežulka




Podmínky přijímání příspěvků:
Přijímáme pouze původní příspěvky (příspěvky dosud jinde nepublikované), a to elektronicky na e-mailovou adresu redakce.


Email: redakce.magazin@agenturacas.gov.cz
www.agenturacas.gov.cz
www.magazin-cas.cz

# Úvodní slovo

Vážení čtenáři,
rok 2024 se blíží ke svému závěru a my vám přinášíme poslední letošní vydání Magazínu ČAS. Tento rok byl plný zajímavých událostí, nových výzev a významných úspěchů v oblasti standardizace, které nás posouvají vpřed.
Jedním z nejvýznamnějších okamžiků letošního roku bylo slavnostní předávání Ocenění Vladimíra Lista, které se řadí mezi nejprestižnější události v oblasti technické normalizace v České republice a koná se jednou za dva roky. Česká agentura pro standardizaci ocenila osobnosti, jež svými aktivitami přispěly k rozvoji a popularizaci standardizace, a zároveň vyzdvihla autory studentských prací, které mají přímou vazbu na technické normy ČSN. Tento slavnostní akt připomíná odkaz zakladatele československé technické normalizace, prof. Dr. Ing. Vladimíra Lista, podporuje nové generace odborníků a zvyšuje povědomí o důležitosti standardizace pro naši společnost.
Jedním z hlavních témat tohoto čísla je kybernetická bezpečnost, která dnes patří mezi klíčové výzvy digitální doby. Evropské nařízení NIS2 a nový zákon o kybernetické bezpečnosti přinášejí zásadní změny, jež ovlivní organizace napříč sektory. Klíčovou roli přitom hrají technické normy, které nastavují jasná pravidla a pomáhají zajistit bezpečnost dat a informačních systémů. Technické normy, jako je ČSN EN ISO/IEC 27001 pro řízení bezpečnosti informací, jsou základním nástrojem pro ochranu nejen firem, ale i veřejných institucí a jednotlivců. V článku se podrobněji zaměříme na to, jak implementace těchto norem přispívá ke zvládání kybernetických hrozeb.

Dalšími tématy jsou shrnutí událostí tohoto roku v oblasti zavádění metody BIM do českého stavebnictví a modernizace spisové služby pomocí atestace eSSL, která před rokem přibyla do portfolia činností naší agentury. Věříme, že v tomto vydání najdete inspiraci a užitečné informace.
Rok 2024 byl pro Českou agenturu pro standardizaci rokem pokroku a úspěšné spolupráce. Děkujeme vám, našim čtenářům a partnerům, za vaši důvěru a podporu. Do roku 2025 vstupujeme s odhodláním pokračovat v naší misi a budovat povědomí o významu standardizace v každodenním životě.
Přejeme vám klidné a spokojené vánoční svátky a mnoho úspěchů v novém roce 2025.

*redakce*


# Slavnostní udílení ocenění Vladimíra Lista

## Česká agentura pro standardizaci ocenila osobnosti, které přispěly k rozvoji a popularizaci standardizace, i autory studentských prací.

Dne 20. listopadu 2024 proběhl v Kaiserštejnském paláci v Praze 21. ročník předávání Ceny a Čestných uznání Vladimíra Lista. Tato prestižní ocenění jsou udělována od roku 2002 a kladou si za cíl vyzdvihnout osobnosti, jež významně přispívají k rozvoji a popularizaci technické normalizace. Ceny nesou jméno zakladatele československé technické normalizace, prof. Dr. Ing. Vladimíra Lista (1877–1971), jehož odkaz zůstává inspirací i v současnosti.

Letošní laureáti byli oceněni v několika kategoriích. Cenu Vladimíra Lista obdržel Michael Solar za celoživotní významný a mnohostranný přínos v oblasti technické normalizace, především v oboru nanotechnologií. Čestné uznání Vladimíra Lista si odnesli tři odborníci: David Korpas za oblast zdravotnických prostředků, Petr Kuklík za přínos v oboru dřevěných konstrukcí a Martina Pavlínková za práci v oblasti plastů.

V kategorii nejpřínosnější původní ČSN vydaná v letech 2023/2024 – Cena ČSN & Research and Innovation byla oceněna norma ČSN 73 1901-4 *Navrhování střech – Část 4: Vegetační střechy*, kterou vypracoval Výzkumný ústav pozemních staveb – Certifikační společnost, s. r. o., a kolektiv.

Novinkou letošního ročníku bylo Ocenění za propagaci a rozvoj standardizace, kterou získali Gustav Chwistek a Miroslav Miler za dlouhodobý a významný přínos v této oblasti.

Pozornost byla tradičně věnována také studentům. V soutěži o nejlepší studentskou práci s vazbou na technické normy ČSN v kategorii diplomových prací zvítězil Jakub Nosek s prací „Poloautomatický krimpovací stroj“. Čestné uznání si odnesly Helena Havelková a Michaela Keňová. V kategorii bakalářských prací zvítězil Petr Šebelle za práci „Výpočet šířky trhlin pro železobetonové konstrukce“.

Čestné uznání obdržel Martin Lysek.

Ocenění laureátům předávali generální ředitel České agentury pro standardizaci Zdeněk Veselý a předseda Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví Jiří Kratochvíl.

Zdeněk Veselý při této příležitosti zdůraznil: „*Standardizace je nezbytným základem pro inovace, efektivitu a bezpečnost ve všech oblastech průmyslu a veřejného sektoru. Česká agentura pro standardizaci se od svého vzniku neustále vyvíjí, přizpůsobuje novým výzvám a rozšiřuje svou působnost, což je možné díky schopným a angažovaným zaměstnancům. Kromě naší hlavní činnosti, kterou je tvorba technických norem, se dnes zaměřujeme i na klíčové oblasti, jako je implementace metody BIM do českého stavebnictví a atestace elektronických systémů spisových služeb.*“

Jiří Kratochvíl vyjádřil potěšení nad tím, že v České republice se daří za účasti všech zainteresovaných stran budovat v České agentuře pro standardizaci silnou normalizační organizaci, která se vhodně inspiruje ve svém fungování obdobnými organizacemi v Evropě. Předseda ÚNMZ zároveň připomněl nezastupitelnou roli technických norem v technickém vzdělávání. I v této oblasti jsou úřad a agentura velmi progresivní.

*Mgr. Zdeněk Veselý, generální ředitel ČAS*

# Seznam laureátů pro rok 2024

## Cena Vladimíra Lista

**RNDr. Michael Solar, Csc.**, za celoživotní významný a mnohostranný přínos pro rozvoj technické normalizace, zejména v oboru nanotechnologií

## Čestné uznání Vladimíra Lista

**Ing. David Korpas, Ph.D.**, za dlouhodobý významný přínos pro rozvoj technické normalizace v oblasti zdravotnických prostředků


**Doc. Ing. Petr Kuklík, CSc.**, za dlouhodobý významný přínos pro rozvoj technické normalizace v oboru dřevěných konstrukcí


**Ing. Martina Pavlínková** za dlouhodobý významný přínos pro rozvoj technické normalizace v oblasti plastů

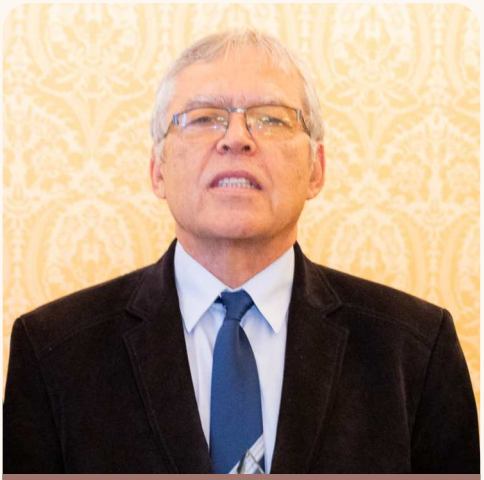
## Ocenění za nejpřínosnější původní ČSN vydanou v r. 2023/2024 – CENA ČSN & Research and Innovation

norma **ČSN 73 19 01-4** *Navrhování střech – Část 4: Vegetační střechy*

**Výzkumný ústav pozemních staveb – Certifikační společnost, s. r. o., ocenění převzal Ing. Lubomír Keim, CSc.**

## Ocenění za propagaci a rozvoj standardizace

**doc. RNDr. Miroslav Miler, DrSc.**



**Ing. Gustav Chwistek**

# Studentské práce s vazbou na technické normy ČSN

### Diplomová práce

**Ing. Jakub Nosek** 1. místo za práci
*„Poloautomatický krimpovací stroj“*

### Diplomová práce

**Ing. Michaela Keňová** čestné uznání za práci
*„Audit projektu Nová budova ekonomické fakulty VŠB-TUO z pohledu standardu ČSN EN ISO 19650“*

### Diplomová práce

**Ing. Helena Havelková** čestné uznání za práci *„Zavádění shody s vyhláškou o kybernetické bezpečnosti do společnosti pomocí softwarového nástroje“*

### Bakalářská práce

**Bc. Petr Šebelle** 1. místo za práci *„Výpočet šířky trhlin pro železobetonové konstrukce“*

### Bakalářská práce

**Bc. Martin Lysek** čestné uznání za práci
*„Měření topného faktoru tepelného čerpadla“*

# Kybernetická bezpečnost pro laiky

**Už druhý rok sleduji různé fámy a zmatky kolem zavedení NIS2 a nového zákona o kybernetické bezpečnosti (nZKB). Ti, kterých se to týká, jsou rozděleni na dva hlavní názorové proudy. Jedni se tváří, že se jich to zatím netýká, a druzí hořekují, co je to zase za novinku a kolik to bude stát peněz. A pak je malá skupinka zasvěcených, kteří se připravují. Ale pojďme popořádku.**

V první řadě tu kybernetická bezpečnost byla, je a bude, a na tom se nic nemění. A důvod, proč tu je, souvisí s tím, že se změnil svět. Kolem stěn kanceláří už nejsou sloupové skříně plné šanonů, do banky téměř nechodíme, a plno poboček už ani nemá pokladnu. Tam, kde se nám to hodí, jsme se přizpůsobili velmi rychle, a vnímáme to jako velkou úsporu času nebo zjednodušení. Vyhledat fakturu z minulého roku je otázka několika vteřin, a člověk se ani nemusí zvednout ze své židle. Zaplatit dětem kroužek ve škole dokážeme na několik kliknutí, a přitom ani nemusíme do banky, ani dítě nemusí nosit hotovost do školy. Platíme kartami, používáme mobily, během zlomku vteřiny vyhledáváme informace, necháme se vést online navigací, která hledá nejrychlejší cestu. Náš život se změnil. Změnili jsme svoje chování. A ač to neradi slyšíme, změnit se musí i naše odpovědnost.

Zkusím opět jednu názornou paralelu. Jakmile se začal na počátku 20. století rozmáhat automobilismus, objevily se první semafory a postupně přibývaly. Můžeme se na to dívat tak, že slouží k omezování volného pohybu chodců, ale také, že zavedly pravidla vzájemného chování mezi vozidly a mezi vozidly a chodci. A patrně většina lidí si uvědomuje, že jedním z hlavních důvodů bylo zajištění bezpečnosti. A vznikly i dopravní předpisy. Ano, je pravdou, že regulují, někoho omezují, občas i něco komplikují, ale hlavně nastavují pravidla chování. Rozumný člověk by stejně nepřebíhal křižovatku, po níž jede mnoho vozidel. A pro ty ostatní je tu pravidlo, že se prostě nepřechází na červenou. A upřímně, vnímá to někdo tak, že vlastně omezujeme chodce a oni ztrácejí svůj čas? Že mohli být o několik minut dříve doma? Patrně ne, protože je nám přirozené dodržet pravidlo, které nás sice na chvilku omezí v cestě, avšak zajišťuje, že domů dorazíme bezpečně.

Ale zpět ke kybernetické bezpečnosti. Věřte, že autor tohoto článku viděl již mnoho situací, nad kterými zůstává rozum stát. Od PINu napsaného fixou na druhé straně platební karty přes používání křestního jména uživatele jako hesla až po nalepený lísteček s heslem na monitoru v kanceláři, kam může přijít kdokoliv. Přesto lze říci, že většina uživatelů se chová zodpovědně, dodržuje pravidla a dbá na bezpečí své i svých dat. Jenže svět se rychle mění a s narůstající digitalizací narůstají i hrozby a rizika. A protože většina populace s informačními technologiemi přichází do styku pravidelně

(i mobilní telefon je informační technologie, a to i ten tlačítkový), bylo nutné zavést jednotná pravidla, která nastaví chování uživatelů a firem v digitálním světě.

## Proč se to týká i mne?

Určitě se vyplatí zamyslet se nad tím, kdo by vlastně mohl mít důvod na vás kyberneticky útočit. Motivací je mnoho, od toho, že se někdo chce jen tak pochlubit tím, co dokáže, až po opravdové hackery, které zajímají vaše data, jež mohou prodat, nebo díky nim dokonce získat přístup ke službám, které používáte, v krajním případě i přímo k finančním prostředkům. Často jsou mezi útočníky lidé, s nimiž jste měli nějaký konflikt a oni se tímto způsobem mstí a znepříjemňují vám život. Případně vás chtějí přímo poškodit. Ale stejně tak to mohou být různí aktivisté, kteří jen chtějí poukázat na to, jak jednoduché je některá bezpečnostní opatření obejít. Nejtvrdší skupinou jsou pak organizované zločinné skupiny, teroristé, nebo dokonce týmy podporované některými státy.

První, nad čím by se měl každý zamyslet, je právě tato oblast. Měli bychom být schopni kriticky vyhodnotit, co nás může ohrozit a proč by z toho mohl mít někdo nějaký prospěch. Každá bezpečnostní technologie znamená náklady, její překonání také není zadarmo, a tomu by měla odpovídat úroveň ochrany, kterou se rozhodneme využít. A je dobré si uvědomit i to, že čím bezpečnější technologie, čím vyšší úroveň ochrany, tím většinou uživatelsky méně přívětivé používání. Často je to jeden z důvodů, proč začneme některé z bezpečnostních opatření obcházet. Prostě hledáme co nejjednodušší způsob používání dané technologie. Jeden příklad za všechny: někdo si nainstaluje bezpečný komunikátor do svého mobilního telefonu, aby nikdo nemohl odposlouchávat hovory. A protože po něm komunikátor jednou za čas chce zadání PINu, tak je přece nejjednodušší použít stejný, který používá pro odemčení svého zařízení. A takový PIN se při troše dobré vůle dá odkoukat, a pak už jen stačí na chvíli nechat telefon na stole a útočník se dostane i k soukromé komunikaci v bezpečném komunikátoru. Důvod je jednoduchý, používání více PINů je složitější a často nepraktické. V hlavě si začnete argumentovat tím, že vás to omezuje v používání, a protože se vám v minulosti stejně nikdy nic nestalo, tak se nestane ani v budoucnosti. A to je jeden z mnoha příkladů, kdy zjednodušení si života, a občas i lenost, jsou základem toho, že jednou může přijít velký průšvih. A aby nepřišel, rozhodl se stát nastavit pravidla pro odvětví, která jsou důležitá, neřkuli kritická, a jejichž napadení by mohlo mít fatální následky.

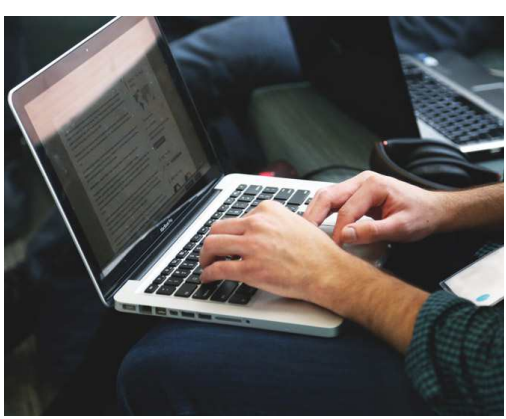
## Trochu nudné teorie

Právě těmito pravidly se měla od 17. října 2024 stát implementace evropského nařízení NIS2. Zatím z důvodu legislativních průtahů neplatí, ale předpokládá se, že od 1. ledna2025 bude platit nový zákon o kybernetické bezpečnosti, včetně prováděcí vyhlášky, a tím pádem budou pravidla přenesena i do naší legislativy. Podobně vzniklo v bankovnictví nařízení DORA (Digital Operational Resilience Act), které stanovuje jednotné požadavky na bezpečnost sítí a informačních systémů organizací působících ve finančním sektoru a jejich dodavatelů. A nesmíme zapomenout ani na nařízení CRA (Cyber Resiliency Act), které stanovuje pravidla pro

uvádění produktů nebo softwaru s digitální složkou na trh, rámec požadavků na kybernetickou bezpečnost všech fází vývoje a údržby těchto produktů a povinnost poskytovat péči po celou dobu životního cyklu těchto výrobků. Že nejde o nic nového, lze prokázat i tím, že již dlouhou dobu množství firem svou bezpečnost řídí podle ISO norem ze skupiny 27 000, které nastavují rámec pro systémy řízení bezpečnosti informací. A i bez ISO norem existují zavedená pravidla a oborové standardy, které používá široká odborná veřejnost.

## Co je vlastně kybernetická bezpečnost?

Na první pohled by se mohlo zdát, že je to něco úzce spjatého s digitálním světem, ale často se také používá termín „bezpečnost informací“, a tam už je na první pohled jasné, že je to trochu širší oblast. Bezpečnost informací by měla být zaměřena na všechny druhy informací po celou dobu jejich životnosti (a to třeba včetně likvidace). Ač se to může zdát divné, je nutné řešit bezpečnost informací, které jsou například i jen v hlavě nebo na papíře. Zkuste si představit, že nějakou důležitou informaci pro chod firmy má v hlavě jeden jediný člověk. A ten se na dovolené zraní a zůstane několik dní v nemocnici. Z toho plyne, že do bezpečnosti informací nezapočítáváme jen to, že by se někdo neoprávněný mohl k informaci dostat, ale i to, že někdo zcela oprávněný se najednou k dané informaci dostat nemůže. A protože terminologie není sjednocená, často pod KB myslíme bezpečnost informací obecně, ale přesto je dobré o ní mluvit v širším kontextu.



## Legrace končí

Donedávna byla bezpečnost informací nebo kybernetická bezpečnost tak trochu dobrovolná. Dokud se nic nestalo, býval tento obor často podinvestovaný, jelikož spadal do obecné kategorie neustále hladových rozpočtů na informační technologie. A když se něco stalo, bylo většinou již pozdě. Protože ze dne na den neseženete vyškolené lidi, ze dne na den nenakoupíte a nenastavíte moderní bezpečnostní řešení, stejně tak se ze dne na den nezmění chování vašich uživatelů. Čím delší byla doba zanedbávání a ignorování této oblasti, tím složitější a bolestivější je náprava. A právě proto byla vedena odborná diskuze, která vyústila v evropské nařízení NIS2 a nový zákon o kybernetické bezpečnosti. Pro mnoho firem nejde o velkou změnu, jelikož si uvědomovaly rizika a snažily se je pokrýt. Pro část firem je to recept, jak si zkontrolovat stav své bezpečnosti informací a uvědomit si, co je důležité ještě dotáhnout. A pro ty ostatní je to jediný způsob, jak je donutit, aby se chovaly zodpovědně.

**V kostce řečeno jde o několik důležitých oblastí, kterým je nezbytné věnovat pozornost. V prvé řadě je nutné:**

- stanovit bezpečnostní politiku;
- integrovat kybernetickou bezpečnost do všech procesů;
- alokovat odpovídající zdroje;
- stanovit bezpečnostní role;
- školit zaměstnance, prokazatelně se seznamovat se stavem řízení kybernetické bezpečnosti.

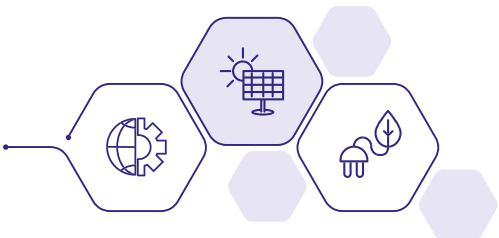
Tím, že jde o důležitou oblast, která je navíc regulována zákonem a vyhláškou, navrhli předkladatelé i velmi citelné postihy, ať již jde o pozastavení výkonu funkce pro statutární orgány na dobu nejméně šesti měsíců, ztrátu všech certifikací, pokutu až do výše 10 milionů eur nebo 2 % z celosvětového obratu, či v krajním případě trestní stíhání. A to vše je podtrženo reputačními dopady, jelikož kromě přímých škod z možného útoku existuje řada nepřímých škod, které mohou mít na danou společnost ještě dalekosáhlejší dopady než samotné sankce.

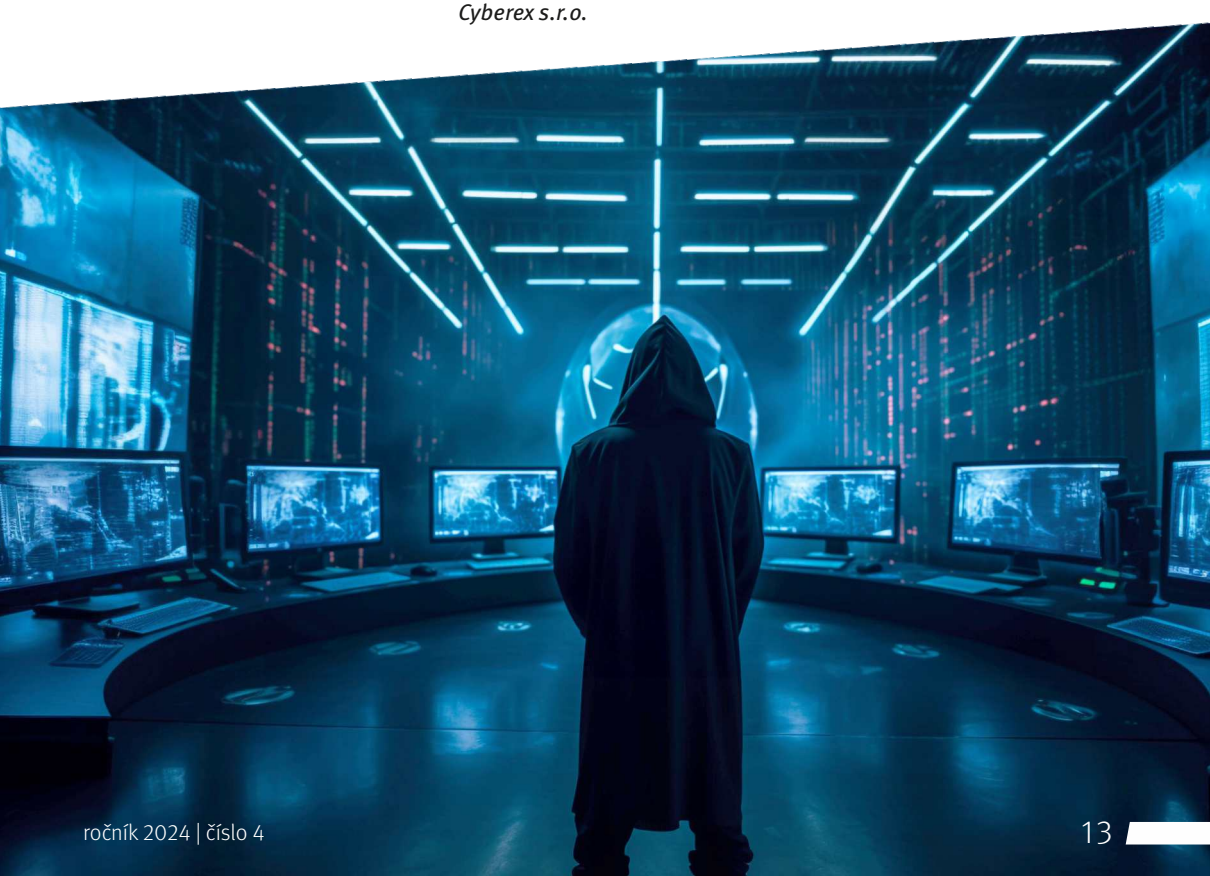
## Závěrem

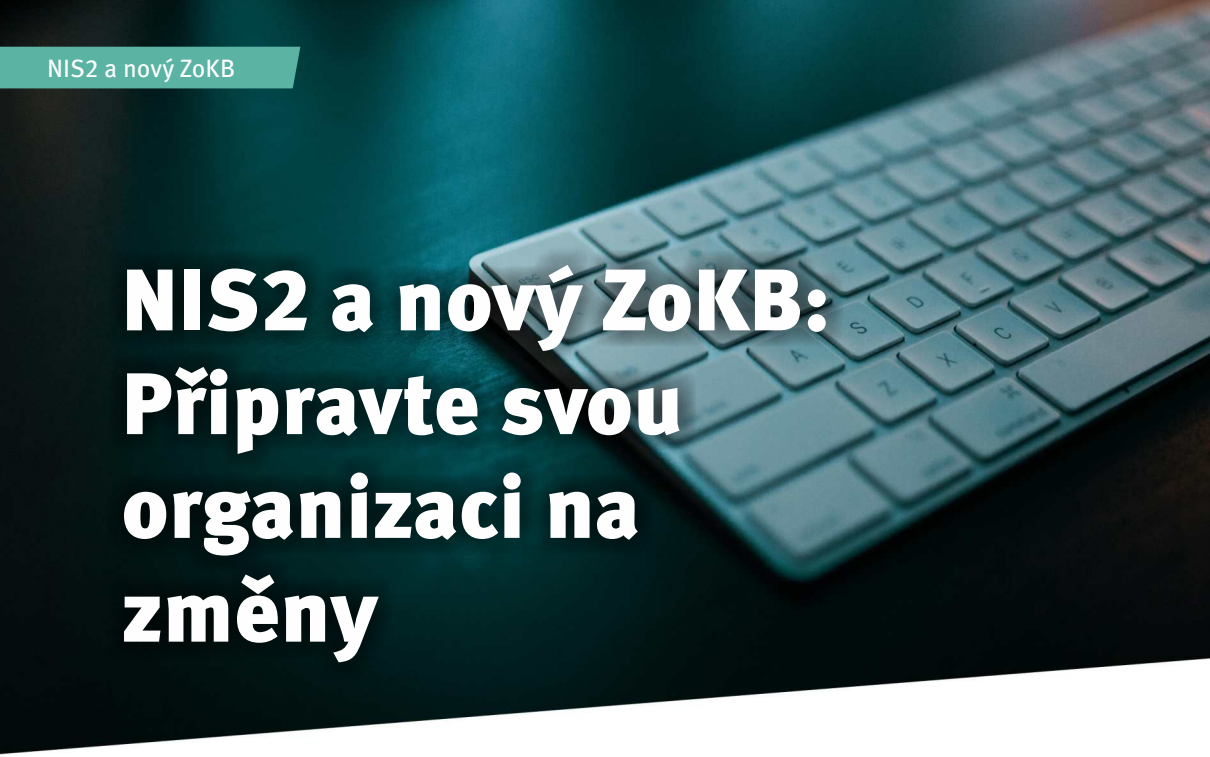
Kybernetická bezpečnost není strašákem pro toho, kdo se snaží chovat obecně zodpovědně. Mnoho firem již dlouho uvažuje nad kontinuitou svého podnikání, definuje potenciální rizika a navrhuje opatření, jak těmto rizikům předcházet a zabránit. Patří to k podnikání stejně jako například sledování nákladů a výnosů, práce s lidskými zdroji nebo návratnost investic. Stejně tak nás běžně používané služby, jakými jsou internetové bankovnictví, bankovní identita, vzdálené přístupy k různým službám, platby na internetu apod., dovedly k určité ostražitosti, opatrnosti a zodpovědnosti. Pravidla kybernetické bezpečnosti jsou tu proto, abychom se naučili s touto problematikou pracovat zcela přirozeně a aby se stala součástí našeho chování. Protože jen tak budeme moci klidněji usínat s pocitem, že jsme udělali vše pro to, aby se nás problémy se zneužitím informací netýkaly. A za ten pocit to přece stojí!

*Ing. Jiří Berger*
*Cyberex s.r.o.*

*Autor Ing. Jiří Berger, MBA je znalcem v oboru kybernetika, zabývá se kybernetickou bezpečností a bezpečností informací a je zakladatelem společnosti Cyberex s.r.o., která se specializuje na problematiku kybernetické bezpečnosti od prevence přes školení, včetně školení top managementu, až po návrh a implementaci jednotlivých opatření, a v neposlední řadě i na řešení bezpečnostních incidentů.*







# NIS2 a nový ZoKB: Připravte svou organizaci na změny

## 1) Co je to KB a jak na ni?

Kybernetická bezpečnost (KB) je ochrana systémů, sítí a programů před digitálními útoky. Tyto útoky mají často za cíl přístup k citlivým informacím, jejich změnu nebo zničení, vydírání uživatelů nebo přerušení běžného provozu.

Důležitým momentem celé problematiky kybernetické a informační bezpečnosti (KIB) je fakt, že za ni zodpovídá statutární zástupce, nezávisle na tom, zda organizace spadá, nebo ne pod zákon o kybernetické bezpečnosti (ZoKB). V případě realizace úspěšného hackerského útoku zde existuje řada rizik, a to od reputačního přes rizika finančních ztrát po riziko úniku osobních údajů a mnoho dalších.

Pro zajištění kybernetické bezpečnosti je důležité používat silná hesla, pravidelně aktualizovat software, zálohovat data a být obezřetný při otevírání e-mailů a odkazů.

## 2) Proč bychom měli KB řešit? – pro sebe, nikoli pro zákon

Kybernetická bezpečnost je důležitá pro ochranu našich osobních a pracovních dat. Nejde jen o dodržování zákonů, ale o ochranu sebe a své organizace před potenciálními hrozbami. Kybernetická bezpečnost je stálý proces, který vyžaduje neustálou pozornost a aktualizaci, aby byla zajištěna ochrana před novými typy útoků.

Hlavním cílem regulace kybernetické bezpečnosti je dosáhnout toho, aby důležité organizace zaváděly preventivní kroky k posílení své kybernetické bezpečnosti. Jedná se o klíčový krok pro předcházení, zjištění a zmírňování dopadů případných kybernetických bezpečnostních incidentů. Tento požadavek, reprezentovaný povinností zavádět tzv. bezpečnostní opatření, je ústředním smyslem existence zákona o kybernetické bezpečnosti, a ne jinak je tomu také v případě existence směrnice NIS2.

Jak říká náš přední odborník na KB a zarputilý šiřitel problematiky kybernetické a informační bezpečnosti Ing. Aleš Špidla: „*Ona totiž kybernetická a informační bezpečnost není otázkou zákonů, ale otázkou pudu sebezáchovy. A pro útočníky neexistují malé cíle, často o velikosti cíle nemají ani tušení, pro ně je to kořist, která se dá vydírat.*“

V současné době již schválená evropská směrnice pro bezpečnost sítí a informací, známá pod zkratkou NIS2, dost výrazně mění a zpřísňuje pohled na zajištění kybernetické a informační bezpečnosti

obecně. Rozšiřuje záběr regulace na mnohonásobně větší počet subjektů, které dosud pod regulaci kybernetické a informační bezpečnosti nespadaly, a to ze současných cca 360 na budoucích minimálně 6000 subjektů. Zkušenosti ze Slovenské republiky však ukazují, že jich bude spíše 10–15 tisíc.
Organizace pak budou muset zavést organizační a technická opatření, tak jak jsou definována v ZoKB a upřesněna v navazujících předpisech, zejména pak ve vyhlášce o kybernetické bezpečnosti (VoKB). Zatím není úplně jasné, jak bude vypadat definitivní znění nového ZoKB, nicméně to vůbec nebrání tomu, aby se organizace otázkami KIB intenzivně zabývaly už teď.

## 3) Co a proč je NIS2 a nZoKB? – jak to bude u nás

NIS2 je směrnice Evropské unie, která posiluje požadavky na kybernetickou bezpečnost pro klíčové sektory, jako jsou energetika, doprava, zdravotnictví a digitální infrastruktura. Zákon o kybernetické bezpečnosti v České republice pak stanovuje pravidla a povinnosti pro organizace, aby zajistily ochranu svých systémů a dat. Týká se to zejména organizací, které poskytují důležité služby nebo spravují kritickou infrastrukturu.
Dosavadní regulace kybernetické bezpečnosti byla v České republice koncipována pro poměrně úzkou skupinu několika stovek nejdůležitějších a nejvýznamnějších organizací s velkým dopadem na celou společnost. Směrnice NIS2 přináší nový pohled a pro Českou republiku nutnost přizpůsobit se těmto změnám.
NIS2 navazuje na předchozí směrnici NIS1 z roku 2016 a reaguje na rychlý vývoj v oblasti kybernetické bezpečnosti. Ukazuje se totiž, že rizika spojená s digitalizací jsou tak rozsáhlá, že mohou zásadním způsobem narušit chod státu a ovlivnit životy, bezpečnost i zdraví lidí. I proto se s NIS2 významně rozšiřuje okruh firem a organizací, jejichž kybernetické zabezpečení bude muset splňovat zákonem stanovené parametry.
Tím zákonem bude právě nový ZoKB (nZoKB) a související vyhlášky vznikající pod taktovkou Národního úřadu pro kybernetickou bezpečnost (NÚKIB).
Schválenou podobu nového ZoKB bychom měli znát v prvním kvartálu roku 2025, ale základní obrysy nových povinností v kyberbezpečnosti jsou už jasné – český zákon totiž musí vycházet z již schválené směrnice NIS2.
Nový zákon o kybernetické bezpečnosti (nZoKB) představuje aplikaci směrnice Evropského parlamentu a Rady EU s číslem 2022/2555, kterou ale známe spíše pod označením NIS2 (z anglického Network and Information Security). Směrnice NIS2 vstoupila v platnost 16. ledna 2023 a členské státy EU mají na její přenos do své legislativy 21 měsíců. To znamená nejpozději do 17. října 2024.
Aby organizace splňovala požadavky zákona o kybernetické bezpečnosti (v České republice je to zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů), je třeba implementovat řadu opatření. Tato opatření se dělí na technická, organizační a procesní.
Implementací těchto opatření organizace zajistí, že bude splňovat požadavky zákona o kybernetické bezpečnosti a zároveň posílí svou celkovou bezpečnostní odolnost.

## 4) Jaký je rozdíl oproti předchozímu stavu? – priority, povinné subjekty, regulovaná služba

Nový ZoKB zavádí nové povinnosti pro tisíce firem a organizací. Zásadním rozdílem oproti stávajícímu stavu je to, že nový ZoKB se primárně nezaměřuje na jednotlivé informační systémy, ale na služby.

Končí dříve používané pojmy jako:
- VIS a KII, PZS, PDS a s nimi spojené role,
- správce systému,
- významný dodavatel,
- významný dodavatel – provozovatel.

A nastupují nové pojmy jako:
- regulovaná služba (služba splňující kritéria uvedená v zákoně nebo v kriteriální vyhlášce),
- poskytovatel regulované služby,
- poskytování regulované služby v režimu vyšších nebo nižších povinností.

Další podstatnou změnou oproti aktuálně platné

legislativě je zásadní rozšíření okruhu firem a organizací, které budou muset splňovat zvýšené nároky na kybernetickou bezpečnost svého provozu. Okruh těchto subjektů vyjmenovává vyhláška o regulovaných službách, která stanovuje, že tzv. povinnými osobami jsou především:

- poskytovatelé služeb elektronických komunikací a souvisejících sítí,
- významné sítě,
- kritická informační infrastruktura,
- významné informační systémy,
- provozovatelé základních služeb,
- poskytovatelé digitálních služeb,
- orgány veřejné moci využívající služeb poskytovatelů cloud computingu.

V rámci každého oboru je stanoven proces tzv. sebeurčení, kdy se organizace musí sama rozhodnout, zda je povinnou osobou ve smyslu zákona.
Organizace poskytující regulované služby jsou v návrhu zákona podle své velikosti rozděleny do dvou úrovní a platí pro ně režim nižších a vyšších povinností. Organizace v nižším režimu si mohou vystačit s určením jedné osoby odpovědné za řízení a rozvoj kybernetické bezpečnosti a vytvořením dokumentace k souvisejícím opatřením (rozsah řízení kybernetické bezpečnosti, školení uživatelů, pravidla pro řízení přístupových oprávnění, tvorbu hesel atd.).

Pro větší organizace v režimu vyšších povinností představuje splnění nových povinností vytvoření výboru pro řízení kybernetické bezpečnosti a sestavení nového týmu. Výbor musí mít nejméně tři členy: dva zástupce vrcholného vedení společnosti a manažera kybernetické bezpečnosti. Výbor pak určuje obsazení čtyř bezpečnostních rolí: manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, garanta aktiva a auditora kybernetické bezpečnosti.
Ačkoli se klasifikace povinných osob liší podle odvětví, zjednodušeně lze říci, že se nový zákon vztahuje na společnosti označené jako „základní subjekty“ a „důležité subjekty“, kdy základními subjekty jsou organizace s 250 a více zaměstnanci a obratem 50 milionů eur nebo rozvahou 43 milionů eur. Mezi důležité subjekty patří společnosti s více než 50 zaměstnanci a ročním obratem nebo rozvahou 10 milionů eur. Současně je ale možné, že i menší firma či organizace bude spadat do kategorie vyšších povinností z důvodu povahy své činnosti.
Bezpečnostní opatření se navíc nevztahují jen přímo na poskytované služby, ale i na související informační systémy nebo databáze, což znamená nové povinnosti i pro subdodavatele, respektive jejich výběr.
V praxi to znamená nutnost prověřovat a zajišťovat bezpečnost v rámci celého dodavatelského řetězce – u každého přímého dodavatele a poskytovatele služeb. Používáte-li například nějaké cloudové služby od externího dodavatele nebo si necháváte vyvíjet vlastní aplikace a systémy na míru, pak i váš dodavatel musí splňovat příslušné požadavky na kyberbezpečnost dle zákona.
Z vyhlášky o regulovaných službách vyplývá, že zatímco dnes platí povinnost zavést opatření v oblasti kyberbezpečnosti pro několik stovek podniků, s platností nZoKB se bude regulace týkat několika tisíc firem a organizací.
V neposlední řadě je třeba také říci, že dodržování opatření stanovených novým zákonem o kybernetické bezpečnosti může kdykoli zkontrolovat NÚKIB, a v případě pochybení jsou stanoveny i sankce. Finanční postih může dosáhnout výše až 10 milionů eur nebo až 2 % z celosvětového čistého obratu společnosti. Osobní odpovědnost manažerů

znamená, že jim může být pozastaven podíl na řízení společnosti.

## 5) Co bych měl začít dělat?

V první řadě by vedení organizace mělo jasně deklarovat, že se chce kybernetickou a informační bezpečností zabývat. Základem by měla být znalost vlastní informační infrastruktury a toho, co v organizaci mám a jaké činnosti a služby vykonávám. Někde musí být uloženy aktuální informace o tom, jaké služby jsou zajišťovány nebo podporovány a jakými technologiemi.

Dále pak je potřeba si udělat jasno v tom, jaká bezpečnostní opatření jsou již v organizaci zavedena, a porovnat to s tím, co o nich říká VoKB nebo Minimální bezpečnostní standard. VoKB hovoří o organizačních opatřeních a technických opatřeních. Aktuální opatření je třeba přiměřeně popsat tak, aby byl obraz stávající situace jasný a zřetelný. Pokud si vytvoříte pravdivý obraz o vašich aktuálních opatřeních v rámci organizace, potom můžete vytvořit plán zavádění opatření, ve kterém si stanovíte postup, jak identifikované nedostatky odstranit. Vhodným nástrojem pro tuto činnost je například tzv. maturity model.

Následně bychom měli provést vstupní analýzu kybernetické bezpečnosti v organizaci, která je také někdy nazývána GAP analýzou. Toto je komplexní proces, který zahrnuje několik kroků, zjištění aktuálního stavu kybernetické bezpečnosti a provedení tzv. health checku pro ověření stavu funkčnosti informačních systémů. Tento proces vám pomůže zjistit, jaké máte nyní zabezpečení a co je potřeba zlepšit, aby vaše organizace splňovala nové požadavky zákona.

Dalším důležitým krokem je pak projít procesem sebeurčení a stanovit, zda organizace je tzv. poskytovatelem regulovaná služby, kdy regulovanou službou je služba, o které tak rozhodl NÚKIB podle § 6 odst. 2. nZoKB. Organizace tedy musí zhodnotit odvětví působnosti, a pokud spadá do regulovaného odvětví, musí zhodnotit svoji velikost. V případě nejasností o tom, jestli regulace podle zákona o kybernetické bezpečnosti dopadne na vaši organizaci, je možno využít také portál Národního úřadu pro kybernetickou bezpečnost, na kterém najdete orientační kalkulačku.

Před vlastním zaváděním bezpečnostních opatření je potřeba stanovit v organizaci tzv. rozsah řízení kybernetické bezpečnosti, který je vymezen v § 12 nZoKB. Součástí stanovení rozsahu je také vedení dokumentovaných záznamů o určení aktiv, resp. evidence primárních a podpůrných aktiv, kdy poskytovatel regulované služby provede následující úkony:

a) Určí všechna svá primární aktiva.
b) Posoudí, zda primární aktiva souvisí s poskytováním regulované služby.
c) U primárních aktiv podle písmene b) určí podpůrná aktiva.

Následně pak na základě § 13 a 14 nZoKB organizace zavede a bude provádět bezpečnostní opatření v závislosti na tom, do jakého režimu povinností spadá. Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.

Poskytovatel regulované služby v režimu vyšších povinností zavádí bezpečnostní opatření daná obsahem návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Poskytovatel regulované služby v režimu nižších povinností zavádí bezpečnostní opatření daná obsahem návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Při zavádění funkčního procesu řízení kybernetické bezpečnosti v organizaci se doporučuje využívat nasazení automatizovaných prostředků, jakými je například systém DAS eCyS firmy DATRON, které výrazně zefektivní a zpřehlední tuto činnost.

## 6) Jak to lidi naučit a kdo za KB zodpovídá? – vzdělávání, nejlepší je prevence

Při zavádění organizačních a technických opatření nesmíme zapomenout na osvětu a vzdělávání uživatelů. Ti jsou totiž tou největší hrozbou pro kybernetickou a informační bezpečnost v každé organizaci. A útočníci na to spoléhají. Bylo vypracováno jakési základní bezpečnostní desatero toho, co by měl každý uživatel vědět o tom, jak se nechovat. Je to ten úplný základ, se kterým by se měl seznámit každý zaměstnanec hned při nástupu. Toto sezná-

mění musí být prokazatelné stejně jako např. BOZP. Dále doporučujeme vzdělávání doplnit a prohloubit e-learningovým kurzem NÚKIB Dávej kyber, který je zcela zdarma a pokrývá celou problematiku kybernetické a informační bezpečnosti na uživatelské úrovni. O absolvování dostane uživatel certifikát, který je dokladem pro jeho zaměstnavatele.

Nejlepší prevencí v oblasti KB je tedy pravidelné vzdělávání. Zaměstnanci by měli být pravidelně školeni o aktuálních hrozbách a bezpečnostních postupech. V praxi se ukazuje, že můžete mít zavedena špičková bezpečnostní opatření, ale pokud uživatelé nevědí, jak je dodržovat, tak jsou prakticky k ničemu a peníze utracené za bezpečnostní technologie jsou ztracenou investicí.

No a kdo za to všechno zodpovídá? Za kybernetickou bezpečnost v organizaci je pak obvykle odpovědný bezpečnostní manažer nebo IT oddělení, které dohlíží na implementaci a dodržování bezpečnostních opatření.

Zásadní novinkou nZoKB je zavedení osobní odpovědnosti managementu společnosti za dodržování nařízení zákona, což je opatření jasně směřující ke zvýšení povědomí o rizicích a kyberbezpečnosti na úrovni nejvyššího vedení podniků a organizací.

Dodržování opatření stanovených novým zákonem o kybernetické bezpečnosti může kdykoli zkontrolovat NÚKIB, a v případě pochybení jsou stanoveny i sankce. Finanční postih může dosáhnout výše až 10 milionů eur nebo až 2 % z celosvětového čistého obratu společnosti. Osobní odpovědnost manažerů znamená, že jim může být pozastaven podíl na řízení společnosti.

## 7) Kdy mám hotovo? – nikdy, KB je permanentní proces

Zajištění odpovídající úrovně kybernetické a informační bezpečnosti v organizaci je komplexní záležitost, do které patří organizační opatření, technická opatření, vzdělávání uživatelů a vědomá snaha se neustále zlepšovat.

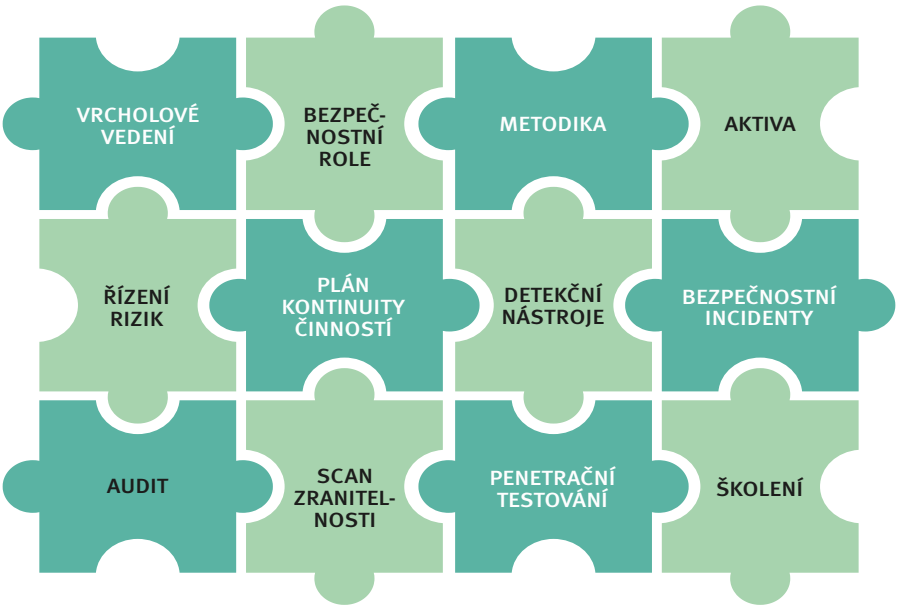
Technologie a hrozby se neustále vyvíjejí, takže je důležité pravidelně aktualizovat bezpečnostní opatření a provádět audity, aby byla vaše organizace vždy chráněna. Nutné je tedy neustálé sledování a odpovídající reakce na neustále se vyvíjející trendy v oblasti kybernetické a informační bezpečnosti.

Bez toho to prostě nejde. Kybernetická bezpečnost je nikdy nekončící proces – je to nekonečný příběh. Je třeba si uvědomit, že bezpečnostní opatření nezavádíme kvůli naplnění zákonných požadavků, ale především pro svoji ochranu, bezpečí a zabránění následným škodám.

## 8) Jaká jsou doporučení? – metodiky, osnovy, návody

Existují různé metodiky, osnovy a návody, které vám mohou pomoci zlepšit kybernetickou bezpečnost vaší organizace. Doporučuje se například dodržovat standardy jako ISO/IEC 27001, které poskytují rámec pro řízení bezpečnosti informací. Důležitým pomocníkem a partnerem při zavádění KB může být také Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který velmi intenzivně vydává nejrůznější doporučení a metodické materiály.

Pro organizace nepodléhající opatřením v rámci nZoKB vydal NÚKIB Minimální bezpečnostní standard – přehledový podpůrný materiál, který pak nabízí zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti. Tento materiál je možno využít především tam, kde s nastavováním zabezpečení teprve začínají, protože ke kybernetické bezpečnosti přistupuje návodným doporučením.




## 9) Co dělal dál? – informační strategie, politiky, plány, kontroly, audity, testy

Pro udržení připravenosti organizace na kybernetické hrozby je důležité mít informační strategie, politiky, plány, pravidelné kontroly, audity a testy. Tyto nástroje vám pomohou identifikovat slabá místa a zajistit, že vaše bezpečnostní opatření jsou účinná a aktuální.

Základním předpokladem systematického přístupu ke kybernetické bezpečnosti je podpora ze strany vrcholového vedení při jejím prosazování. Je potřeba vyčlenit potřebné zdroje, stanovit bezpečnostní role, vytvořit přiměřené bezpečnostní politiky a dokumentaci, včetně jejich schválení, a následně kontrolovat jejich dodržování.

Vrcholové vedení musí projevit dostatečnou podporu a přidělit přiměřené zdroje (finanční, lidské, technické) potřebné k zavedení a udržování principů vedoucích ke zvyšování kybernetické bezpečnosti a určit osobu odpovědnou za kybernetickou bezpečnost, včetně stanovení jejích povinností, odpovědností a pravomocí. Tato role je odpovědná za řízení a rozvoj kybernetické bezpečnosti, průběžnou kontrolu stavu kybernetické bezpečnosti, dohlížení na naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením.

Je třeba si uvědomit, že povinnosti firem a organizací spadajících do režimu vyšších povinností podle nového nZoKB budou výrazně náročnější než v případě splnění požadavků regulace GDPR, a zavedení všech požadovaných opatření bude trvat několik měsíců. Proto je již nyní nejvyšší čas nastudovat si návrh zákona o kybernetické bezpečnosti a souvisejících vyhlášek, a vytvořit si akční plán splnění nových požadavků. Firmy a organizace spadající pod vyhlášku o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností požadavky nového zákona obvykle splní vydáním a kontrolou dodržování bezpečnostních směrnic a proškolením odpovědných osob. Implementace výše uvedených opatření pomůže organizacím zajistit, že budou připraveny čelit současným i budoucím kybernetickým hrozbám a současně dosáhnou souladu s novým zákonem o kybernetické bezpečnosti a směrnicí NIS2, což poskytne ochranu důležitým aktivům a informacím organizace.

*Ctirad Mareš*
*Datron a.s.*

# Novinky ze světa TN

## Kybernetická bezpečnost

**ČSN EN IEC 62859 (35 6646)** *Jaderné elektrárny – Systémy kontroly a řízení – Požadavky na koordinaci jaderné a kybernetické bezpečnosti*

Tento dokument poskytuje rámec pro řízení interakcí mezi bezpečností a kybernetickou ochranou systémů jaderných elektráren (JE), přičemž zohledňuje stávající normy SC 45A, které se těmito otázkami zabývají, a specifika jaderných programovatelných digitálních systémů I&C. V tomto dokumentu (stejně jako v IEC 62645) se kybernetická bezpečnost týká prevence, detekce a reakce na škodlivé činy páchané digitálními prostředky (kybernetické útoky). V tomto kontextu nezahrnuje úvahy týkající se nezlovolných akcí a událostí, jako jsou náhodná selhání, přírodní události nebo lidské chyby (s výjimkou těch, které snižují kybernetickou bezpečnost). Tyto aspekty mají samozřejmě prvořadý význam, ale zabývají se jimi jiné dokumenty a normy SC 45A, a v tomto dokumentu nejsou považovány za související s kybernetickou bezpečností. Tento dokument stanovuje požadavky a pokyny pro: začlenit ustanovení o kybernetické bezpečnosti do jaderných architektur a systémů I&C, které jsou zásadně přizpůsobeny bezpečnosti; vyhnout se potenciálním konfliktům mezi ustanoveními o bezpečnosti a kybernetické bezpečnosti; pomoci identifikovat a využít potenciální synergie mezi bezpečností a kybernetickou bezpečností.

**ČSN EN IEC 62645 (35 6684)** *Jaderné elektrárny – Systémy kontroly, řízení a elektrického napájení – Požadavky na kybernetickou bezpečnost*

Tento dokument stanovuje požadavky a poskytuje pokyny pro vývoj a řízení účinných programů počítačové bezpečnosti pro programovatelné digitální systémy I&C. Nedílnou součástí těchto požadavků a pokynů je kritérium, že program bezpečnosti programovatelného digitálního systému I&C elektrárny je v souladu s požadavky příslušné země.

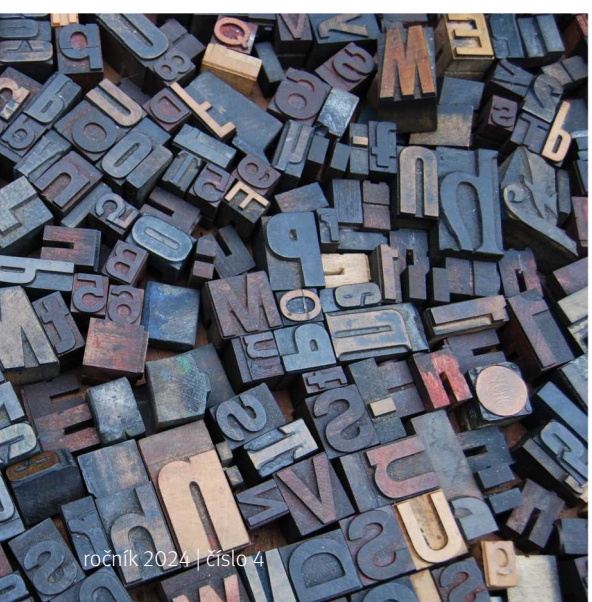
## Stavebnictví

**ČSN 73 5720** *Vězeňské stavby*

Tato norma stanovuje podmínky pro navrhování a výstavbu nových staveb, provádění stavebních úprav a údržby stávajících objektů, včetně veške-

rých vnějších a vnitřních stavebně technických zabezpečení, poplachových a bezpečnostních systémů a provozně dispozičních požadavků pro vězeňské stavby, pokud tak není stanoveno jinými normami nebo příslušnými právními předpisy. Jedná se zejména o části staveb a funkční celky, které touto normou nejsou výhradně řešeny a které jsou řešeny podle příslušných předpisů a norem (např. administrativa, sklady, stravovací provozy, zdravotnická zařízení).

**ČSN EN ISO 41011** *Facility management – Slovník*
Tento dokument definuje termíny používané v normách pro facility management. Mezinárodní normy pro facility management (FM) vypracované technickou komisí ISO/TC 267 popisují charakteristiky facility managementu a jsou určeny pro použití v soukromém i veřejném sektoru. Mezinárodní spolupráce při přípravě těchto mezinárodních norem identifikovala společné postupy, které lze uplatnit v nejrůznějších tržních odvětvích, organizačních typech, procesních činnostech a zeměpisných oblastech, a jejich zavedení pomůže: zlepšovat kvalitu, produktivitu a finanční výkonnost; zvyšovat udržitelnost a snižovat negativní dopad na životní prostředí; vytvářet funkční a motivující pracovní prostředí; udržovat soulad s předpisy a zajišťovat bezpečná pracoviště; optimalizovat výkonnost a náklady během životního cyklu; zlepšovat odolnost a relevantnost; úspěšněji prezentovat identitu a image organizace.



**ČSN EN ISO 41017** *Facility management – Pokyny k připravenosti na mimořádné události a řízení epidemie*
Tento dokument poskytuje obecný návod pro organizace, jak plánovat, zmírňovat a/nebo řídit rizika a dopady epidemické události za účelem ochrany zdraví, bezpečnosti a pohody zařízení. Tento dokument je použitelný pro všechny organizace, plně nebo částečně fungující, obnovující činnost nebo nově fungující.

## Mezinárodní elektrotechnický slovník

**ČSN IEC 60050-631 (33 0050)** *Mezinárodní elektrotechnický slovník (IEV) – Část 631: Systémy pro akumulaci elektrické energie*
Tato část IEC 60050 uvádí obecnou terminologii týkající se systémů pro akumulaci elektrické energie a obecné pojmy týkající se konkrétních aplikací a příslušných technologií. Má status horizontální normy v souladu s pokynem IEC 108 směrnice pro zajištění konzistentnosti (vzájemného souladu) publikací IEC – *Použití horizontálních norem*. Tato terminologie je konzistentní s terminologií zpracovanou v ostatních odborných částech IEV.

**ČSN IEC 60050-651/A1 (33 0050)** *Mezinárodní elektrotechnický slovník – Část 651: Práce pod napětím*
Tato změna nahrazuje dosavadní termíny 651-22-11 a 651-23-01 a doplňuje zcela nový oddíl 651-27 *Ochrana před obloukovým výbojem*.

## Elektrické spotřebiče pro domácnost a podobné účely

**ČSN EN IEC 60335-1 ed. 4 (36 1055)** *Elektrické spotřebiče pro domácnost a podobné účely – Bezpečnost – Část 1: Obecné požadavky*
Tato norma se zabývá bezpečností elektrických spotřebičů pro domácnost a podobné účely, jejichž jmenovité napětí nepřesahuje 250 V u jednofázových spotřebičů a 480 V u ostatních spotřebičů, včetně spotřebičů napájených stejnosměrným proudem a spotřebičů na baterie. Tato norma platí pro spotřebiče, které nejsou určeny pro používání v normálních domácnostech, ale které se přesto

mohou stát zdrojem nebezpečí pro osoby, jako jsou spotřebiče určené pro používání neznalými osobami v obchodech, ve spotřebním průmyslu a v zemědělství. V možné míře pojednává tato norma o běžných nebezpečích představovaných spotřebiči, se kterými se setkávají všechny osoby v domácnosti a blízkém okolí. Obecně však nebere v úvahu osoby (včetně dětí), jimž fyzická, smyslová nebo mentální neschopnost nebo nedostatek zkušeností a znalostí zabraňuje v bezpečném používání spotřebiče bez dozoru, nebo poučení a hru dětí se spotřebičem. Další požadavky mohou být nutné pro spotřebiče určené pro používání ve vozidlech nebo na palubách lodí či letadel. V mnoha zemích jsou předepsány doplňující požadavky národními zdravotnickými úřady, úřady zodpovědnými za ochranu bezpečnosti práce, vodohospodářskými a podobnými úřady.

## Informační technologie

**ČSN EN ISO/IEC 27006-1 (36 9790)** *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti – Část 1: Obecně*

Tato norma stanovuje požadavky na certifikační orgány, které provádějí audit a certifikaci systémů managementu informační bezpečnosti (ISMS). Tento dokument doplňuje obecné požadavky na orgány provádějící audit a certifikaci systémů managementu podle ČSN EN ISO/IEC 17021-1:2016 o další požadavky, které jsou specifické pro audit a certifikaci systémů managementu informační bezpečnosti (ISMS). Dodržování těchto požadavků má zajistit, aby certifikační orgány prováděly certifikaci ISMS kompetentně, konzistentně a nestranně, a tím usnadnit uznávání certifikací těchto orgánů na národní i mezinárodní úrovni. Text v tomto dokumentu se řídí strukturou ČSN EN ISO/IEC 17021-1:2016.

**ČSN ISO/IEC 20924 (36 9020)** *Internet věcí (IoT) a digitální replika – Slovník*

Tato norma poskytuje definici internetu věcí a digitální repliky společně se souborem termínů a definic. Tento dokument je terminologickým základem pro internet věcí a digitální repliku.

## Elektroenergetika

**ČSN EN IEC 60567 ed. 4 (34 6725)** *Olejem plněná elektrická zařízení – Odběr vzorků volných plynů a analýza volných a rozpuštěných plynů v minerálních olejích a jiných izolačních kapalinách – Návod*

Tato norma se zabývá technikami odběru vzorků volných plynů z plynového relé výkonových transformátorů. Jsou popsané tři metody odběru vzorků volných plynů. Techniky pro odběr vzorků oleje z olejem plněných zařízení, jako jsou výkonové a přístrojové transformátory, reaktory, průchodky, olejové kabely a olejem plněné tank-typ kondenzátory nejsou již dále zahrnuty v tomto dokumentu, ale místo toho jsou popsány v článku 4.2 IEC 60475: 2022. Před analýzou plynů rozpuštěných v oleji jsou tyto plyny nejprve vyextrahovány z oleje. Zde jsou popsány tři základní metody, jedna užívající extrakci vakuem (Toepler a částečné odplynění), další vytěsnění rozpuštěných plynů probubláváním vzorku oleje nosným plynem (stripping) a poslední rozdělení plynů mezi vzorek oleje a malý objem nosného plynu (headspace). Plyny jsou analyzovány kvantitativně po extrakci, plynovou chromatografií; je popsána metoda analýzy. Volné plyny z plynového relé jsou analyzovány bez předběžných úprav. Popisované techniky berou v úvahu na jedné straně problémy vlastní analýzám, související s přejímací zkouškou v závodě, kde obsah plynu v oleji je obecně velmi nízký, a na druhé straně problémy spojené s monitorováním zařízení v terénu, kde se může přeprava vzorků uskutečnit mimo kompresní kabinu při letecké dopravě a kde mohou existovat značné rozdíly mezi teplotou okolí elektrárny a zkušební laboratoře.

**ČSN EN IEC 60143-4 ed. 2 (35 8201)** *Sériové kondenzátory pro výkonové systémy – Část 4: Tyristorově řízené sériové kondenzátory*

Tato norma upravuje zkoušení tyristorově řízených sériových kondenzátorů (TCSC) používaných v sérii s přenosovými vedeními. Dále se zabývá otázkami, které zohledňují jmenovité hodnoty tyristorových ventilových sestav TCSC, kondenzátorů a tlumivek, jakož i charakteristiky řízení TCSC, ochranné prvky, chladicí systém a provoz systému. Norma je vydána v anglickém jazyce.

**ČSN EN IEC 63281-2-1 (30 6000)** *Elektrické přepravní prostředky – Část 2-1: Požadavky na bezpečnost a zkušební metody pro elektrické přepravní prostředky pro přepravu osob*

Tato norma stanovuje požadavky na bezpečnost a zkušební metody pro osobní elektrické přepravní prostředky. Tato norma platí pro elektricky poháněné osobní elektrické přepravní prostředky (PeT), které se používají v soukromých a veřejných prostorách, kde je ovládání rychlosti a/nebo řízení elektrické/elektronické. PeT může mít prostředky pro přepravu nákladu a může být pro soukromé nebo komerční použití (včetně služby sdílení). Tato norma neplatí pro elektrická vozidla (EV), jako jsou elektricky poháněná jízdní kola (EPAC), elektrokola, mopedy, motocykly a osobní automobily.

**ČSN CLC IEC/TS 61851-3-1 (34 1590)** *Systém nabíjení elektrických vozidel vodivým propojením – Část 3-1: Stejnosměrné napájecí zařízení EV, ve kterém ochrana spoléhá na dvojitou nebo zesílenou izolaci – Obecná pravidla a požadavky na stacionární zařízení*

Tato technická specifikace platí pro zařízení (včetně stacionárního zařízení) pro vodivý přenos elektrické energie mezi napájecí sítí a silničním elektrickým vozidlem nebo demontovatelným dobíjecím systémem pro ukládání energie (RESS) nebo RESS zabudovaným do silničního elektrického vozidla. Dále platí v případě, je-li zařízení připojeno k napájecí síti s napájecím napětím do 480 V AC nebo do 400 V DC a jmenovitým výstupním napětím do 120 V DC a kde ochrana před úrazem elektrickým proudem spočívá ve dvojité nebo zesílené izolaci a s dvojitou nebo zesílenou izolací mezi všemi vstupy a výstupy střídavého a stejnosměrného proudu.

**ČSN CLC IEC/TS 61851-3-2 (34 1590)** *Systém nabíjení elektrických vozidel vodivým propojením – Část 3-2: Stejnosměrné napájecí zařízení EV, ve kterém ochrana spoléhá na dvojitou nebo zesílenou izolaci – Zvláštní požadavky na přenosná a mobilní zařízení*

Tato technická specifikace se vztahuje na přenosná a mobilní napájecí zařízení DRI EV, u nichž je ochrana před úrazem elektrickým proudem založena na dvojité nebo zesílené izolaci a na dvojité nebo zesílené izolaci mezi všemi AC a DC vstupy a výstupy se jmenovitým vstupním napětím nejvýše 250 V AC a výstupním napětím nejvýše 120 V DC. Dokument se vztahuje zejména na jednotky VCU určené jako součást přenosných a mobilních napájecích zařízení DRI EV, přenosná a mobilní napájecí zařízení DRI EV podle souboru IEC 61851-3 určená k instalaci a/nebo použití v nadmořské výšce do 2000 m a přenosná a mobilní napájecí zařízení DRI EV pro vodivý přenos elektrické energie mezi napájecí sítí a elektrickým silničním vozidlem/RESS podle souboru IEC 61851-3 určená k připojení k vozidlům, kde je napájecí obvod vozidla chráněn před úrazem elektrickým proudem dvojitou nebo zesílenou izolací.

**ČSN CLC IEC/TS 61851-3-4 (34 1590)** *Systém nabíjení elektrických vozidel vodivým propojením – Část 3-4: Stejnosměrné napájecí zařízení EV, ve kterém ochrana spoléhá na dvojitou nebo zesílenou izolaci – Obecné definice a požadavky na komunikaci CANopen*

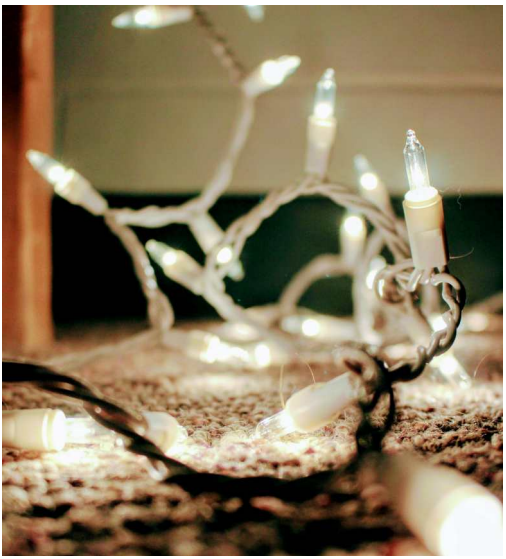
Tato technická specifikace se vztahuje na komunikaci CANopen pro přenos elektrické energie vodivým propojením mezi napájecí sítí a elektrickým silničním vozidlem nebo přemístitelným dobíjecím

systémem pro ukládání energie (RESS) nebo palubními systémy elektrického silničního vozidla pro ukládání energie (RESS). Základní profil aplikace pro systémy řízení spotřeby energie (EMS) se mimo této normy dále skládá z IEC/TS 61851-3-5, IEC/TS 61851-3-6 a IEC/TS 61851-3-7.

**ČSN EN 50716 (34 2680)** *Drážní zařízení – Požadavky na vývoj softwaru*
Tato norma stanovuje postupy a technické požadavky pro vývoj softwaru pro programovatelné elektronické systémy pro použití v řídicích a zabezpečovacích aplikacích, v aplikacích na palubách kolejových vozidel. Norma není určena pro použití v oblasti napájení elektrické trakce (pevné instalace) nebo pro napájení a řízení běžných aplikací, např. napájení stanic pro kanceláře, obchody. Na tyto aplikace se obvykle vztahují normy pro distribuci energie a/nebo jiná než železniční odvětví a/nebo místní právní rámce. Norma platí výhradně pro software a vzájemné působení mezi softwarem a systémem, jehož součástí je software.

## Svítidla

**ČSN EN IEC 60598-2-20 ed. 4 (36 0600)** *Svítidla – Část 2-20: Zvláštní požadavky – Světelné řetězy*
Tato norma specifikuje požadavky na světelné řetězy vybavené sériovými, paralelními nebo kombinovanými sériově/paralelně připojenými světelnými zdroji pro použití uvnitř nebo venku při napájecím napětí nepřesahujícím 250 V. U kombinací, kde jsou zahrnuta světelná lana (známé také jako utěsněné světelné řetězy), viz IEC 60598-2-21. Tento dokument se vztahuje na světelné řetězy s pevnými nebo odnímatelnými přídavnými nástavci, například okrasnými nebo dekorativními. Na světelné řetězy vybavené násuvnými objímkami se vztahují příslušné požadavky tohoto dokumentu. Tento dokument se zabývá následujícími světelnými řetězy: trvale instalovanými světelnými řetězy, dočasně instalovanými světelnými řetězy a dočasně instalovanými řetězy chráněného osvětlení (TPL). U světelných řetězů s nenormalizovanými světelnými zdroji (například světelné zdroje násuvného typu) jsou tyto světelné zdroje považovány za součást světelného řetězu, a v důsledku toho jsou zahrnuty do zkoušení.



## Točivé elektrické stroje

**ČSN CLC IEC/TS 60034-31 (35 0000)** *Točivé elektrické stroje – Část 31: Výběr energeticky účinných motorů, včetně aplikací s proměnnými otáčkami – Směrnice k použití*
Tato technická specifikace poskytuje návod s technickými a ekonomickými aspekty pro aplikace energeticky účinných elektrických AC motorů. Platí pro výrobce motorů, OEM (výrobce originálních zařízení), koncové uživatele, regulační a zákonodárné orgány a další zainteresované strany. Tento dokument se vztahuje na všechny elektrické stroje zahrnuté v IEC 60034-1, IEC 60034-30-1 a IEC/TS 60034-30-2. Byly aktualizovány odkazy na příslušné normy a údaje o světovém trhu s průmyslovými motory.

**ČSN EN IEC 60034-30-3 (35 0000)** *Točivé elektrické stroje – Část 30-3: Třídy účinnosti vysokonapěťových střídavých motorů (IE kód)*
Tato norma specifikuje třídy účinnosti pro trojfázové vysokonapěťové asynchronní motory nakrátko s pevnými otáčkami v souladu s IEC 60034-1, které mají jmenovité napětí přesahující 1000 V, avšak nepřesahující 11 kV, a jmenovitý výkon od 200 kW do 2000 kW. Tento dokument zajišťuje globální harmonizaci energetických tříd účinnosti trojfázových asynchronních motorů nakrátko se jmenovi-

tým napětím nad 1000 V. Jde o motory s přímým připojením na síť, které jsou provozovány při pevných otáčkách při napájení sinusovým napětím o kmitočtu 50 Hz nebo 60 Hz.

## Pohotovostní a výstražné systémy

**ČSN EN 50726-1 (33 4597)** *Pohotovostní a výstražné systémy – Část 1: Pohotovostní a výstražné reakční systémy (EDRS) – Základní požadavky, povinnosti, odpovědnosti a činnosti*

Tato norma se vztahuje na plánování, instalaci, uvádění do provozu, provoz a údržbu pohotovostního a výstražného reakčního systému. Pohotovostní a výstražný reakční systém je součástí celkového řešení pro řešení konkrétních událostí, jako jsou mimořádné události nebo krize. Tento dokument specifikuje:

- technické procesy a odpovědnosti za podporu všech postupů od registrace události (stav nouze, nebezpečí) až po její konečné zpracování;
- technické řízení rizik, včetně definice bezpečnostních/zabezpečovaných cílů a organizace pracovního postupu, jakož i nezbytné specifikace týkající se souboru managementu technických rizik;
- související povinnosti, odpovědnosti a činnosti jako součásti integrovaného procesu managementu celkových rizik k dosažení cílů bezpečnosti a zabezpečení, efektivity a účinnosti, jakož i bezpečnosti/zabezpečení dat a systému;
- tři různé stupně bezpečnosti/zabezpečení s příslušnými funkcemi produktu požadovanými k jejich dosažení;
- základní požadavky na pohotovostní a výstražné reakční systémy (EDRS) ve veřejných budovách, jako jsou vzdělávací zařízení (např. školy, univerzity), vládní zařízení, školky a podobná zařízení;
- odpovědnosti podle platných národních zákonů o bezpečnosti a ochraně zdraví při práci, a tedy zejména řeší odpovědnost zaměstnavatelů.

## Prostředí s nebezpečím výbuchu

**ČSN EN IEC 60079-31 ed. 3 (33 2320)** *Výbušné atmosféry – Část 31: Zařízení chráněné proti vznícení prachu závěrem „t“*

Tato norma platí pro zařízení chráněná závěrem a omezením teploty povrchu, která jsou určena pro použití ve výbušných atmosférách s prachem. Stanoví požadavky pro navrhování, konstrukci a zkoušení Ex-zařízení a Ex-součástí. Tento dokument doplňuje a modifikuje obecné požadavky IEC 60079-0. Jestliže je požadavek tohoto dokumentu v rozporu s požadavkem IEC 60079-0, má přednost požadavek uvedený v tomto dokumentu. Tento dokument neplatí pro prachy výbušnin, které k hoření nepotřebují vzdušný kyslík, ani pro pyroforické látky. Tento dokument neplatí pro Ex-zařízení nebo Ex-součásti určené pro použití v podzemních částech dolů, jakož i v těch částech povrchových instalací těchto dolů, které jsou ohroženy důlním plynem a/nebo hořlavým prachem. Tento dokument nezohledňuje žádná nebezpečí vyplývající z uvolňování hořlavých nebo toxických plynů z prachu. Tento dokument neobsahuje požadavky pro Ex-zařízení používaná v prostorech, kde se může vyskytovat hořlavý prach a výbušné plynné atmosféry, ať už současně, nebo odděleně. Požadavky pro výbušné plynné atmosféry lze nalézt v jiných částech souboru norem IEC 60079. Návod pro Ex-zařízení, která mají být použita tam, kde se hořlavý prach a výbušné plynné atmosféry vyskytují současně (hybridní směsi), lze nalézt v IEC 60079-14. Jestliže Ex-zařízení musí splňovat další environmentální podmínky, například ochranu proti vniknutí vody a odolnost proti korozi, mohou být nutná dodatečná opatření, která neovlivní nepříznivě integritu závěru.

**ČSN EN IEC 60079-17 ed. 5 (33 2320)** *Výbušné atmosféry – Část 17: Prohlídky a údržba elektrických instalací*

Tato norma se zabývá uživateli a zahrnuje pouze ty faktory, které přímo souvisejí s prohlídkami a údržbou elektrických instalací zvlášť navržených pro nebezpečné prostory, kde je nebezpečí způsobeno výbušnou atmosférou. Norma je vydána v anglickém jazyce. Připravuje se překlad do českého jazyka.

## Ochrana před bleskem

**ČSN EN IEC 62561-5 ed. 3 (35 7605)** *Součásti systému ochrany před bleskem (LPSC) – Část 5: Požadavky na revizní skříně a provedení zemničů*

Tato norma stanovuje požadavky a zkoušky pro

revizní skříně zemničů (skříně zemničů) instalované v zemi a pro průchodky zemničů.

**ČSN EN IEC 62561-7 ed. 3 (35 7605)** *Součásti systému ochrany před bleskem (LPSC) – Část 7: Požadavky na směsi zlepšující uzemnění*
Tato norma stanovuje požadavky a zkoušky na směsi zlepšující uzemnění snížením rezistance zemnicího systému.

## Kabely a vodiče

**ČSN EN 50655-1 ed. 2 (34 7116)** *Elektrické kabely – Příslušenství – Materiálové vlastnosti – Část 1: Identifikace pro pryskyřičné směsi*
Tato norma specifikuje zkušební metody a požadavky na identifikaci polymerovatelné reagující pryskyřičné směsi bez rozpouštědel, určené k použití pro elektrickou izolaci a/nebo mechanickou ochranu v příslušenství kabelů, na které se vztahuje EN 50393, HD 629.1 a HD 629.2, pro nízké a střední napětí až do 20,8/36 (42) kV.

## Zkoušení vlivů prostředí

**ČSN EN IEC 60721-3-9 (03 8900)** *Klasifikace podmínek prostředí – Část 3-9: Klasifikace skupin parametrů prostředí a jejich stupňů přísnosti – Mikroklimata uvnitř výrobků*
Tato norma klasifikuje skupiny mikroklimatických podmínek, kterým mohou být součástky (základní díly, sestavy, vestavěné jednotky) vystaveny uvnitř výrobků používaných v klimatických podmínkách klasifikovaných v IEC 60721-3-3 a v IEC 60721-3-4.

## Svařování

**ČSN EN ISO 15610 (05 0315)** *Stanovení a kvalifikace postupů svařování kovových materiálů – Kvalifikace na základě vyzkoušených svařovacích materiálů*
Norma je součástí skupiny norem zabývajících se specifikací a kvalifikací postupů svařování, jejichž podrobnosti jsou uvedeny v příloze A normy ISO 15607:2019. Norma specifikuje, jak lze postup svařování kvalifikovat na základě vyzkoušených svařovacích materiálů. Rozšiřuje požadavky uvedené v ISO 15607. Norma ČSN EN ISO 15610 navíc udává rozsah kvalifikace.

## Drážní aplikace

**ČSN EN 45545-4 (28 0160)** *Drážní aplikace – Protipožární ochrana drážních vozidel – Část 4: Požadavky na konstrukci drážních vozidel z hlediska požární bezpečnosti*
Norma specifikuje požadavky na požární bezpečnost konstrukce drážních vozidel pro pokrytí cílů uvedených v EN 45545-1:2013. Opatření a požadavky stanovené v tomto dokumentu jsou zaměřeny na ochranu cestujících a personálu v drážních vozidlech v případě požáru na palubě minimalizací rizika vzniku požáru, na zpomalení rozvoje požáru a na řízení pohybu požárních zplodin přes drážní vozidlo za účelem napomáhat evakuaci. V rámci předmětu tohoto dokumentu nejsou uvedena opatření, která zajistí záchranu drážních vozidel v případě požáru.

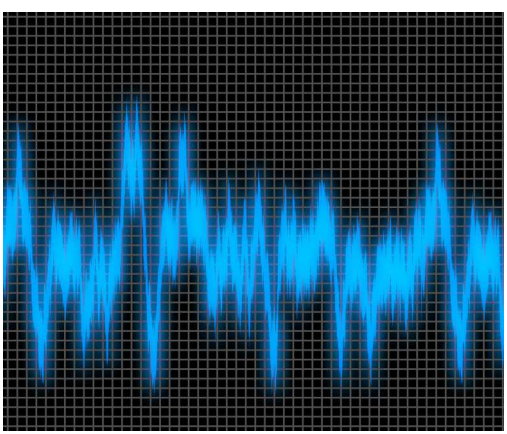
## Potrubí

**ČSN 13 0072 (13 0072)** *Bezpečnostní označení potrubí podle provozní látky*
Norma platí pro označování nadzemního potrubí v budovách a vně budov v průmyslu a energetice. Norma se nemusí používat u rekonstrukcí a dostaveb. Norma neplatí pro ostatní budovy (např. pro obytné nebo administrativní budovy), může se však přiměřeně použít pro označování potrubí v kotelnách, strojovnách a předávacích stanicích tepla, které jsou součástí těchto budov. Tato norma se může použít také pro označování potrubí v kolektorech, kolektorových podchodech a technických chodbách, pro které platí ČSN P 73 7505. Norma specifikuje bezpečnostní označení potrubí podle

provozních látek. Dále specifikuje označování souvisících nebezpečí za účelem prevence nehod a havárií a snižování rizik pro zdraví. Norma není určena pro označování potrubí uložených v zemi.

## Akustika

**ČSN EN ISO 16032 (73 0538)** *Akustika – Měření hladiny akustického tlaku z technických zařízení nebo činností v budovách – Technická metoda*
Norma specifikuje technickou metodu měření hladin akustického tlaku v místnostech, z technických zařízení instalovaných v budově. Zabývá se konkrétně měřením hluku ze sanitárních zařízení, mechanického větrání, technických zařízení pro vytápění a chlazení, výtahů, odpadních instalací, topných zařízení, ventilátorů, čerpadel a jiných pomocných obslužných zařízení a motoricky poháněných vrat garáží. Lze ji použít i pro měření hluku z jiných typů zařízení nebo činností v budově, např. hluku ze sportovních zařízení nebo restaurací.



## Kotle

**ČSN 07 0710 (07 0710)** *Parní, horkovodní a kapalinové kotle – Provozní pravidla*
Norma určuje základní podmínky nutné k zajištění bezpečného a hospodárného provozu kotlů. Provozem kotlů se rozumí souhrn činností nutných k využívání kotelního zařízení. Provoz podle této normy zahrnuje souhrn všech činností, nutných k využívání kotelního zařízení, nejen vlastní provoz, ale i preventivní i provozní údržbu. Norma platí pro provoz kotlů s nejvyšším pracovním/dovoleným tlakem vyšším než 0,5 bar a s teplotou vody převyšující bod jejího varu při tomto tlaku. Norma obsahuje zvlášť podrobné pokyny pro provoz, obsluhu a údržbu kotlů. Pokyny mají zajišťovat bezpečnou práci i prevenci rizik, včetně opatření k všeobecně známým nebezpečím vyplývajících z šetřených událostí. Významné jsou i organizační pokyny pro obsluhu i provádění revizí a zkoušek kotlů. Norma řeší uvádění kotlů do provozu, řízení provozu a jejich odstavování z provozu, dále přípravu revizí a zkoušek kotlů a vedení provozních záznamů.

## Výtahy

**ČSN EN 81-70+A1 (27 4003)** *Bezpečnostní předpisy pro konstrukci a montáž výtahů – Zvláštní úprava výtahů určených pro dopravu osob a osob a nákladů – Část 70: Přístupnost výtahů, včetně osob s omezenou schopností pohybu a orientace*
Norma stanovuje minimální požadavky na bezpečný a nezávislý přístup a používání výtahů osobami s omezenou schopností pohybu a orientace.

**ČSN EN ISO 16001 (27 8016)** *Strojní zařízení pro zemní práce – Systémy detekce předmětů a pomůcky pro výhled – Požadavky na provedení a zkoušky, z prosince 2024*
Norma stanovuje obecné požadavky a popisuje metody pro hodnocení a zkoušení provedení systémů detekce předmětu (ODS) a pomůcek pro výhled (VA) používaných na strojích pro zemní práce. Platí pro stroje definované v ISO 6165. ODS, VA nebo obojí lze použít k rozšíření přímého výhledu obsluhy nebo nepřímého výhledu pomocí zrcátek. Kromě toho mohou být ODS a/nebo VA použity k poskytnutí dalších prostředků detekce předmětu nebo výhledu, např. tam, kde ergonomická hlediska omezují účinnost přímého výhledu a aby se zabránilo opakovanému otáčení hlavy a horní části těla.

**ČSN 69 0012 (69 0012)** *Tlakové nádoby stabilní – Provozní pravidla, z prosince 2024*
Norma platí pro provoz, obsluhu, údržbu, opravy, provádění revizí a zkoušek tlakových nádob stabilních a jejich bezpečnostní a tlakové výstroje.

Stanoví základní podmínky pro uvádění nových tlakových nádob stabilních do provozu a pro opakované uvádění do provozu po odstavení, opravách, rekonstrukcích, přemístění, poruchách a haváriích apod. Stanoví též podmínky pro jejich umístění. Vztahuje se na tlakové nádoby stabilní, jejichž nejvyšší pracovní tlak přesahuje 0,5 bar a které obsahují plyny, páry nebo žíravé, toxické a výbušné kapaliny skupiny 1 podle příslušného právního předpisu o jakékoliv teplotě nebo jakékoliv kapaliny o teplotě převyšující jejich bod varu při tlaku 0,5 bar, včetně vyvíječů páry typu pára/pára a typu horká voda / pára a vyvíječů páry bez nebezpečí přehřátí.

## Výrobky pro zdravotní péči

**ČSN EN ISO 13408-1** *Aseptické zpracování výrobků pro zdravotní péči – Část 1: Obecné požadavky*

Tento dokument specifikuje obecné požadavky na procesy, programy a postupy pro vývoj, validaci a průběžnou kontrolu aseptického zpracování výrobků pro zdravotní péči a nabízí k nim návod.

Tento dokument obsahuje požadavky a návody týkající se aseptického zpracování jako celku.

Specifické požadavky a návody pro různé specializované procesy a metody související se sterilizační filtrací, lyofilizací, technologiemi čištění na místě (Clean In Place, CIP), sterilizací na místě (Sterilization In Place, SIP) a izolátorovými systémy jsou uvedeny v dalších částech souboru ISO 13408.

## Překlad a tlumočení

**ČSN ISO 20539** *Překlad, tlumočení a související technologie – Slovník*

Tento dokument definuje termíny pro mezinárodní normy týkající se překladu, tlumočení a související technologie.

## Požární bezpečnost svíček

**ČSN EN 17885** *Příslušenství svíček – Specifikace požární bezpečnosti a bezpečnostní štítky výrobků*

Tento dokument stanovuje požadavky a zkušební metody požární bezpečnosti příslušenství svíček, a také bezpečnostní informace a požadavky na zobrazování bezpečnostních informací.

Bezpečnostní požadavky a zkušební metody uvedené v tomto dokumentu jsou určeny k pokrytí většiny běžných rizik.

Tento dokument nestanovuje požadavky nebo zkušební metody méně běžných rizik vznikajících z nepředvídatelné kombinace příslušenství se svíčkami.

## Systémy managementu bezpečnosti a ochrany zdraví při práci

**ČSN ISO 45003** *Systémy managementu bezpečnosti a ochrany zdraví při práci – Psychické zdraví a bezpečnost při práci – Směrnice pro řízení psychosociálních rizik*

Tento dokument poskytuje směrnice pro řízení psychosociálních rizik v rámci systému managementu bezpečnosti a ochrany zdraví při práci (BOZP) založených na ISO 45001. Umožňuje organizacím předcházet pracovním úrazům a špatnému zdravotnímu stavu svých zaměstnanců a dalších zainteresovaných stran, a podporovat duševní pohodu při práci.

Je použitelný pro organizace všech velikostí a ve všech odvětvích pro vývoj, zavádění, udržování a neustálé zlepšování bezpečnosti a ochrany zdraví na pracovišti.

# S ČSN jsou vaše data pečlivě zamčená

ČSN EN 17640
Metodika hodnocení kybernetické bezpečnosti pro ICT produkty

ČSN EN ISO/IEC 27001
Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

ČSN EN ISO/IEC 27007
Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN ISO/IEC 29128-1
Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Ověřování kryptografických protokolů – Část 1: Rámec

ČSN P CEN/CLC ISO/IEC/TS 23532-1
Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Požadavky na kompetenci laboratoří pro testování a hodnocení bezpečnosti IT – Část 1: Hodnocení podle ISO/IEC 15408

# Normy kybernetické bezpečnosti a ochrany dat

***Cílem tohoto článku je seznámit čtenáře s normami v oboru informační a kybernetické bezpečnosti. Mezinárodní a evropské normy uvedené v tomto článku jako příklady norem z tohoto oboru jsou zavedeny v ČSN překladem.***

Tvorba norem v oboru informační a kybernetické bezpečnosti, ochrany informací a informačních a komunikačních technologií je předmětem činnosti mezinárodní technické komise ISO/IEC/JTC 1/SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí* a evropské technické komise CEN/CLC/JTC 13 *Kybernetická bezpečnost a ochrana dat*. V současné době tyto dvě technické komise spravují celkem 258 vydaných platných technických norem, specifikací a zpráv.

Tyto normy se zabývají metodami, technikami a postupy zaměřenými na bezpečnost a ochranu dat a soukromí, management bezpečnosti, hodnocení bezpečnosti, metodiku zachycování bezpečnostních požadavků, management rizik, management identit, audity a certifikace systémů managementu informační bezpečnosti, kryptografické protokoly apod.

Kybernetická bezpečnost je často definována jako ochrana lidí, společnosti, organizací a národů před kybernetickými riziky.

Termínem „bezpečnost informačních systémů" se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením nebo kolapsem, a to neoprávněnou činností nebo činností nedůvěryhodné osoby a vlivem neplánované události. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

Rozvoj informačních a komunikačních technologií, který se dotýká téměř všech oborů činnosti, klade vysoké nároky na zavádění nových technologií, procesů a zpracování elektronických dokumentů. Svět internetu je ale velice zranitelný a je vystaven různým kybernetickým útokům, jejichž cílem je například zcizení dat, zašifrování dat s cílem získat výkupné, zneužití získaných dat a aplikací apod.

Každá organizace bez ohledu na svou velikost nebo na předmět činnosti je těmto útokům vystavena. Je proto nezbytné, aby si organizace s ohledem na svou činnost a své cíle stanovila požadavky na informační bezpečnost a přijala taková opatření, která jí riziko takového útoku sníží.

Technické normy, vypracované výše uvedenými technickými komisemi, tyto požadavky definují a poskytují pokyny pro jejich implementaci.

**ČSN ISO/IEC 24745 (36 9887)** *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Ochrana biometrických informací*

Tato norma se zabývá ochranou biometrických informací v rámci požadavků na důvěrnost, integritu a obnovitelnost/odvolatelnost během uchovávání a přenosu. Poskytuje požadavky a doporučení pro bezpečný management a zpracování biometrických informací v souladu s ochranou soukromí.

Tento dokument specifikuje:

- analýzu hrozeb a protiopatření souvisících s biometrikou a modely aplikací biometrických systémů;
- bezpečnostní požadavky na bezpečné propojení biometrické reference (BR) a odkazu na identitu (IR);
- modely aplikací biometrických systémů s různými scénáři pro ukládání a porovnávání biometrických referencí;
- pokyny pro ochranu soukromí jednotlivce při zpracování biometrických informací.

**ČSN EN ISO/IEC 27005 (36 9790)** *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti*

Tato norma obsahuje pokyny, které mají organizacím pomoci:

- splnit požadavky ISO/IEC 27001 týkající se opatření k řešení rizik v oblasti informační bezpečnosti;
- provádět činnosti v oblasti managementu rizik informační bezpečnosti, zejména posuzování a ošetření rizik informační bezpečnosti.

**ČSN EN ISO/IEC 27006-1 (36 9790)** *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti – Část 1: Obecně*

Tato norma specifikuje požadavky na orgány provádějící audit a certifikaci ISMS. Uvádí obecné požadavky na tyto orgány, které jsou označovány jako certifikační orgány. Dodržování těchto poža-

davků má zajistit, aby certifikační orgány prováděly certifikaci ISMS kompetentně, konzistentně a nestranně, čímž se usnadní uznávání těchto orgánů a akceptace jejich certifikací na národní a mezinárodní úrovni.
Požadavky a pokyny pro orgány provádějící audit a certifikaci systémů managementu stanovuje ISO/IEC 17021-1. Pokud tyto orgány hodlají být v souladu s ISO/IEC 17021-1 s cílem provádění auditů a certifikace systémů managementu informační bezpečnosti (ISMS) v souladu s ISO/IEC 27001, jsou zásadní některé další požadavky a pokyny k ISO/IEC 17021-1. Ty poskytuje tento dokument.
Text dokumentu se řídí strukturou ISO/IEC 17021-1.

**ČSN ISO/IEC 27035-1 (36 9799**) *Informační technologie – Management incidentů informační bezpečnosti – Část 1: Principy a proces*
Tato norma je základem souboru ISO/IEC 27035. Představuje základní koncepty, principy a procesy s klíčovými činnostmi managementu incidentů informační bezpečnosti, které poskytují strukturovaný přístup k přípravě na incidenty, jejich detekci, podávání zpráv o incidentech, posuzování incidentů a k odezvě na ně a uplatňování získaných poznatků.
Pokyny k procesu managementu incidentů informační bezpečnosti a jeho klíčovým činnostem uvedené v této normě jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu. Tato norma je použitelná pro externí organizace poskytující služby managementu incidentů informační bezpečnosti.

**ČSN ISO/IEC 27035-2 (36 9799)** *Informační technologie – Management incidentů informační bezpečnosti – Část 2: Směrnice pro plánování a přípravu odezvy na incidenty*
Tato norma se zaměřuje na management incidentů informační bezpečnosti, který je v ISO/IEC 27000 uveden jako jeden z kritických faktorů úspěchu systému managementu informační bezpečnosti.
Mezi plánem organizace, jak řešit incident, a připraveností organizace na incident může být velký rozdíl. Tato norma se zabývá vývojem postupů pro zvýšení důvěry ve skutečnou připravenost organizace reagovat na incident informační bezpečnosti. Toho je dosaženo řešením politik a plánů souvisících s managementem incidentů, jakož i procesem vytváření týmu pro odezvu na incidenty a zlepšováním jeho výkonnosti v průběhu času přijímáním získaných zkušeností a hodnocením.
Pokyny uvedené v této normě jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu. Tato norma je použitelná i pro externí organizace poskytující služby managementu incidentů informační bezpečnosti.

**ČSN ISO/IEC 27035-3 (36 9799)** *Informační technologie – Management incidentů informační bezpečnosti – Část 3: Směrnice pro činnosti odezvy na incidenty ICT*
Tato norma poskytuje směrnice pro odezvu na incidenty informační bezpečnosti v rámci činností ICT v oblasti bezpečnosti. Tento dokument se nejprve zabývá provozními aspekty činností ICT v oblasti bezpečnosti z hlediska lidí, procesů a technologií. Dále se zaměřuje na odezvu na incidenty informační bezpečnosti v rámci činností ICT v oblasti bezpečnosti, včetně detekce incidentů informační bezpečnosti, podávání zpráv, třídění, analýzy, odezvy, omezení, eliminace dopadu, obnovy a uzavření incidentů informační bezpečnosti.
Zásady uvedené v tomto dokumentu jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu.

**ČSN ISO/IEC 27102 (36 9720)** *Správa a řízení bezpečnosti informací – Směrnice pro pojištění kybernetických rizik*
Tato norma poskytuje směrnice při zvažování pojištění kybernetických rizik jako doplňku opatření informační bezpečnosti v rámci účinného přístupu k ošetření rizik. Kybernetické hrozby a kybernetické útoky, kterým musí čelit různé organizace, jsou stále četnější a sofistikovanější, a jejich dopady na organizaci mohou mít velice vážné důsledky. Pojištění kybernetických rizik nenahrazuje celkový systém řízení rizik a opatření informační bezpečnosti organizace, ale mělo by být považováno za jeho důležitou součást, která zvy-

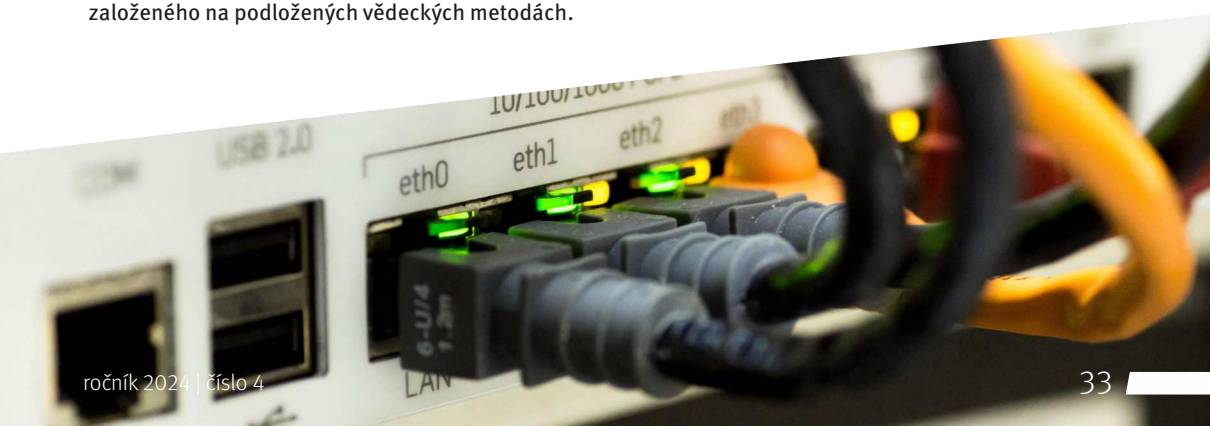
šuje odolnost organizace a snižuje dopady kybernetického incidentu. Tato norma je použitelná pro organizace všech typů a velikostí.

**ČSN P ISO/IEC TS 27110 (36 9773)** *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro vývoj rámce kybernetické bezpečnosti*
Tato norma specifikuje pokyny pro vývoj rámce kybernetické bezpečnosti. Kybernetická bezpečnost představuje v souvislosti s používáním propojených technologií naléhavý problém. Nástroje, které pomáhají organizacím nebo jednotlivcům při činnostech a komunikaci v oblasti kybernetické bezpečnosti, se nazývají rámce kybernetické bezpečnosti. Tento dokument stanovuje minimální sadu konceptů při tvorbě rámce kybernetické bezpečnosti. Je určen zejména pro tvůrce rámců kybernetické bezpečnosti bez ohledu na typ, velikost nebo činnost jejich organizací.

**ČSN ISO/IEC 29128-1 (36 9707)** *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Ověřování kryptografických protokolů – Část 1: Rámec*
Tato norma ustanovuje rámec specifikací pro ověřování kryptografických protokolů podle nejlepších akademických a oborových postupů.
Mnoho kryptografických protokolů nedosáhlo svých zamýšlených bezpečnostních cílů kvůli své složitosti a obtížné implementaci při dosažení požadovaných funkčních a bezpečnostních požadavků. Tato obtížnost znamená, že protokoly je nutné pečlivě analyzovat za účelem nalezení chyb v jejich návrhu. Cílem tohoto dokumentu je standardizovat metodu pro analyzování protokolů navrhováním jasně definovaného rámce ověřování založeného na podložených vědeckých metodách.
Tento dokument navrhuje postup standardizace analogický k tomu, který již existuje v rámci kryptografických algoritmů. Národní a mezinárodní orgány používají procesy hodnocení, které pomáhají zajistit, že standardizovaný kryptografický algoritmus splňuje konkrétní bezpečnostní požadavky, pro které byl navržen. Podobný proces pro kryptografické protokoly by poskytl důvěru, že ověřený protokol splňuje stanovené bezpečnostní vlastnosti a je možné jej použít v systémech, které jsou z hlediska bezpečnosti kritické.
Navržený proces ověřování je založen na nejmodernějších technikách modelování protokolů a využívá přísnou logiku, matematiku a počítačovou vědu. Je navržen tak, aby poskytl objektivní důkaz, že protokol splňuje jeho stanovené bezpečnostní cíle. Ověření není zárukou bezpečnosti; stejně jako u každého modelování jsou výsledky omezeny rozsahem a kvalitou modelu a použitými nástroji.

**Závěr**
Kybernetické incidenty mohou nastat kdykoli a mají různé dopady na organizace. Informace a aktiva organizace jsou stále vystaveny riziku útoku, protože kybernetické hrozby se stávají všudypřítomnými a jsou neustále sofistikovanější.
Cílem technických norem je poskytnout metody, postupy a opatření týkající se předcházení rizik kybernetického útoku, a poskytnout reference pro zavedení takových opatření, která dopady případného kybernetického útoku sníží.

*Ing. Miroslav Škop*
*referent Oddělení elektrotechniky*
*Česká agentura pro standardizaci*



# K 1. lednu 2025 nabyla účinnosti nová edice normy ČSN 33 2130

***Zásadně přepracované vydání české technické normy řešící navrhování, provádění a rekonstrukce vnitřních elektrických rozvodů ve všech druzích staveb se nově zabývá také parkováním elektrických vozidel v podzemních a hromadných garážích a problematikou obnovitelných zdrojů energie, tedy fotovoltaikou.***

ČSN 33 2130 ed. 4:2024 *Elektrické instalace nízkého napětí – Vnitřní elektrické rozvody* byla vydána k 1. prosinci 2024 ve Věstníku ÚNMZ č. 12/24. Účinnosti nabyla k 1. lednu 2025 a plně nahradila dosud platnou ČSN 33 2130 ed. 3 z prosince 2014, která byla k tomuto datu zrušena.

Norma reaguje na probíhající rozvoj a používání nových technologií spojených s obnovitelnými zdroji elektrické energie a elektromobilitou. Jedním z jejích cílů je další zvýšení bezpečnosti osob bez elektrotechnické kvalifikace a spolehlivosti elektrických rozvodů používaných při každodenní činnosti.

Norma je rozdělena do samostatných kapitol zabývajících se jednotlivými oblastmi vnitřních elektrických rozvodů. Norma zejména uvádí nové požadavky na přípravu a montáž:

- obnovitelných zdrojů (zejména s ohledem na fotovoltaické systémy) ve stavbách pro bydlení a ve stavbách občanské výstavby;
- rozvodů elektrické infrastruktury pro nabíjení (dobíjení) elektrických vozidel ve hromadných garážích;
- rozvodů elektrické infrastruktury pro nabíjení (dobíjení) elektrických kol, koloběžek nebo jiných obdobných dopravních prostředků, které nejsou považovány za elektrická vozidla;
- rozvodů elektronických komunikací s ohledem na platné legislativní dokumenty v oblasti osob se zdravotním postižením.

*„Přepracované vydání normy zachovává kontinuitu s předchozími verzemi a současně reaguje na nově vznikající podmínky spojené s rozvojem elektromobility a obnovitelných zdrojů elektrické energie. Odborné veřejnosti, tedy projektantům, elektrotechnikům a revizním technikům v oboru elektro, přináší jasná, konkrétní a v praxi aplikovatelná pravidla zvyšující bezpečnost uživatelů,“* vysvětluje Ing. Pavel Vojík, pracovník České agentury pro standardizaci, tajemník TNK 22 *Elektrotechnické předpisy* a soudní znalec v oboru elektrotechnika.

Přepracována byla i některá původní ustanovení, zejména s ohledem na vývoj v oblasti elektrotechniky v období od posledního vydání normy (2014). Došlo k významovému zpřesnění některých termínů a k jejich uvedení do souladu s platnou legislativou, byly také doplněny nové termíny jako např. ochranný prostor sporáku (varné desky). U všech definovaných termínů je nově uveden jejich ekvivalent v anglickém jazyce.

Předplatitelé normu získají v rámci aplikace ČSN online, zakoupit ji ale bude možné také jednotlivě v e-shopu České agentury pro standardizaci, a to jak v tištěné, tak elektronické podobě.

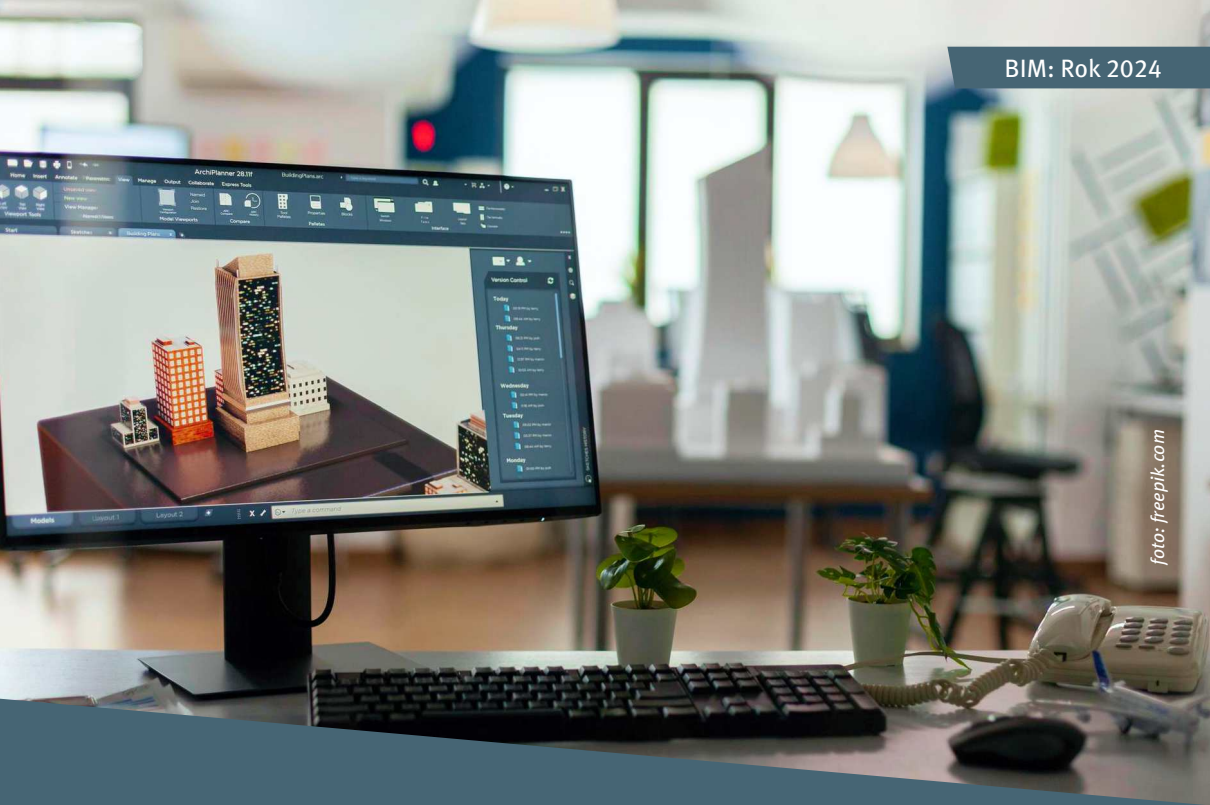


foto: freepik.com

# BIM: Rok 2024 se nesl ve znamení přípravy legislativních změn

***Na svém jednání 6. listopadu 2024 schválila vláda návrh zákona o správě informací o stavbě a vystavěném prostředí. Byla tak završena intenzivní práce pracovních skupin Ministerstva průmyslu a obchodu a České agentury pro standardizaci. Již v červenci 2024 přitom byla schválena Aktualizace Koncepce zavádění metody BIM v České republice a zahájeny byly práce na kartách opatření dle Implementačního plánu Aktualizace. Ovšem práce se nezastavily ani v jiných oblastech a bylo dosaženo významného pokroku také u Datového standardu staveb (DSS) nebo v Programu pilotních projektů BIM.***

Již v lednu 2023 představila ředitelka odboru Koncepce BIM České agentury pro standardizaci Eva Kaiserová plán, jak výrazně aktivizovat práce na realizaci vládní Koncepce zavádění metody BIM do veřejné správy (Koncepce BIM). Stalo se tak v období, kdy vláda na svém jednání 21. prosince 2022 usnesením číslo 1087/22 uložila Ministerstvu průmyslu a obchodu připravit znění Aktualizace Koncepce zavádění metody BIM v České republice. Rok 2023 byl tak z velké části vyplněn snahou o zefektivnění prací na realizaci Koncepce BIM, ale i o znovunavázání spolupráce s klíčovými stakeholdery tak, aby výstupy připravované Českou agenturou pro standardizaci byly v souladu s postojem klíčových stavařských organizací, jako jsou profesní komory, svazy či spolky. Úspěch v této oblasti otevřel prostor pro spolupráci s dalšími experty, a tím i k urychlení a zefektivnění prací na realizaci Koncepce. Pozitivní výsledky se začaly objevovat již v průběhu roku 2023 a naplno se práce projevily v roce 2024, kdy se podařilo dosáhnout několika velmi zásadních milníků.

## Koncepce musí odrážet změny v sektoru stavebnictví

Původní dokument Koncepce zavádění metody BIM v České republice začal vznikat již někdy v průběhu roku 2016, či možná ještě dříve. Přijat byl vládním usnesením číslo 682/2017. Realizace tohoto usnesení pak začala s rokem 2018. Od té doby prošla společnost, legislativa, ale i stavebnictví, a vlastně i samotná metoda BIM poměrně radikální proměnou. Původní zaměření zejména na informační modelování staveb (a pojetí zkratky BIM jako Building Information Modeling) se změnilo směrem k pojetí metody BIM jako správy informací o stavbě, i proto se dnes zkratka spíše vysvětluje jako Building Information Management. Samotná metoda BIM si v průběhu let vydobyla poměrně silné postavení v soukromém sektoru, kde – zejména u velkých stavebních projektů – má již své nezastupitelné místo.

Máme za sebou ale i několik úspěšných veřejných výstavbových projektů s využitím metody BIM. V roce 2022 připraven a v roce 2023 schválen vládou ČR věcný návrh takzvaného zákona o BIM, tedy v dnešním znění zákona o správě informací o stavbě a vystavěném prostředí a o změně zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů. Tento věcný záměr prošel připomínkovým řízení, které přineslo několik velmi důležitých poznatků od veřejných zadavatelů. Na základě všech těchto zkušeností uložila vláda 21. prosince 2022 ministru průmyslu a obchodu připravit znění Aktualizace Koncepce zavádění metody BIM.

Současně ale došlo k řadě posunů také na mezinárodní scéně, především byl vydán mezinárodní soubor technických norem ČSN EN ISO 19650 *Organizace a digitalizace informací o budovách a inženýrských stavbách, včetně informačního modelování staveb (BIM) – Management informací s využitím informačního modelování staveb*, a další standardy a technické normy např. v oblastech datových slovníků, klasifikačních systémů, úrovně informačních potřeb a požadavků na informace nebo šablon vlastností stavebních předmětů, včetně související oblasti stavebních výrobků. Došlo také ke globálnímu uplatnění konceptů otevřených datových formátů, služeb a procesů pro tvorbu, správu a výměnu informací, známých pod označením openBIM, jehož rozvoji se věnuje mezinárodní asociace buildingSMART, zastoupená ve většině členských zemí Evropské unie, a od roku 2021 i v České republice.

Na úkolu promítnout tyto trendy do vládního strategického dokumentu začala pracovat expertní skupina Ministerstva průmyslu a obchodu společně s experty České agentury pro standardizaci, která je odborným partnerem MPO při realizaci Koncepce BIM. Jak uložila vláda, na přípravě Aktualizace Koncepce BIM se podílely také další zainteresované instituce, zejména Český úřad zeměměřický a katastrální (ČÚZK), spolek Odborná rada pro BIM – BuildingSMART Česká republika (czBIM), ale také Česká komora autorizovaných inženýrů a techniků činných ve výstavbě (ČKAIT), Česká komora architektů (ČKA), Svaz podnikatelů ve stavebnictví (SPS), a samozřejmě také další zainteresované resorty. Zavádění metody BIM, jako jedné z nejdůležitějších cest k digitální budoucnosti stavebnictví, je totiž součástí mnohem širšího plánu na digitalizaci veřejné správy a co největší části agend státu.

## Strategický plán do roku 2027 s výhledem do budoucna

Text Aktualizace Koncepce BIM tak vznikal za intenzivní diskuze s klíčovými stakeholdery a také odbornou stavařskou veřejností. Před předložením vládě prošel samozřejmě standardním meziresortním připomínkovým řízením, ze kterého vzešlo více než 200 podnětů. Po jejich vypořádání byl text předložen vládě. Ta jen přijala usnesením usnesení č. 519 ze dne 24. července 2024.

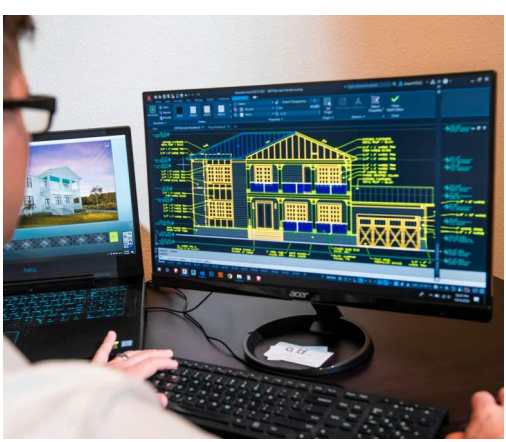
Znění Aktualizace Koncepce zavádění metody BIM v České republice tak reflektuje všechny výše zmíněné fenomény. Současně byla jeho struktura koncipována tak, aby splňovala požadavky na vládní strategické dokumenty. Co je ale klíčové, současně s textem Aktualizace Koncepce BIM byl přijat také Implementační plán, který určuje postup realizace Aktualizace Koncepce BIM. Ten obsahuje tři strategické oblasti: Management informací pro optimalizaci přípravy a provádění staveb, Podpora digitalizace správy a údržby pro efektivní užívání a provoz staveb a Podpora digitalizace agend souvisejících se stavbami a s vystavěným prostředím. Pro každou z těchto oblastí byly vytyčeny Strategické cíle, kterých je celkem deset, a na ně následně navázáno celkem třicet devět opatření.

V souladu s úkoly, které vyplývají ze zmíněného dokumentu, oslovila Česká agentura pro standardizaci ve spolupráci s Ministerstvem průmyslu a obchodu širokou odbornou veřejnost, aby mohly být zahájeny práce na přípravě návrhu karet opatření a sestavila Realizační týmy opatření za účelem zpracování návrhu karet opatření. Do Realizačních týmů opatření obdržela ČAS nominaci přibližně sedmdesáti expertů. Návrh karet opatření bude připraven do konce listopadu 2024 a od 1. ledna 2025 budou karty opatření sloužit jako rámcový podklad pro realizaci Implementačního plánu.

## Zákon o BIM vstupuje do legislativního procesu

Zásadním milníkem roku 2024 z pohledu veřejné správy bylo ale přijetí návrhu zákona o správě informací o stavbě a vystavěném prostředí a o změně zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů. Tedy dlouho očekávaný zákon o BIM vstupuje jako vládní návrh zákona do konečné fáze legislativního procesu. Znamená to, že nyní čeká na projednání v Poslanecké sněmovně, a následně i v Senátu Parlamentu ČR. Klíčové je, že tento návrh byl k jednání vlády předložen 26. září 2024 bez rozporu. Vláda jej pak – jak již bylo zmíněno – přijala 6. listopadu 2024 svým usnesením číslo 760/24.

Do tohoto bodu vedla poměrně dlouhá a také náročná cesta. Již v roce 2022 byl připravován věcný záměr tohoto zákona. K němu se sešlo velké množství připomínek, a teprve po jejich vypořádání mohl být předložen vládě. Ta věcný záměr schválila usnesením číslo 298 v květnu 2023. Na základě tohoto usnesení zpracovalo Ministerstvo průmyslu a obchodu ve spolupráci s Českou agenturou pro standardizaci a dalšími partnery návrh paragrafového znění zákona. Návrh zákona vychází z Koncepce BIM a z Aktualizace Koncepce BIM týkající se zavedení povinnosti použití metody BIM pro nadlimitní veřejné zakázky na stavební práce financované z veřejných rozpočtů. Jeho cílem je vytváření informační základny pro hospodárné, efektivní a účelné nakládání se stavbou a správu a rozvoj vystavěného prostředí. Současně chce také stanovit jednotné standardy a postupy pro vytváření informačního modelu stavby a vystavěného prostředí. Zavádí tak závaznou legislativní úpravu vztahující se ke správě informací o stavbě a informačnímu modelu stavby a k problematice vystavěného prostředí.



Klíčové je stanovení povinných osob, což je uvedeno v paragrafu 3 hlavy II. Ten stanovuje, že povinnou osobou pro účely tohoto zákona je

a) Česká republika, která ji plní prostřednictvím organizační složky státu, jíž přísluší se stavbou hospodařit;
b) státní příspěvková organizace;
c) státní podnik;
d) státní organizace;
e) vyšší územní samosprávný celek, pokud není stavba svěřena k hospodaření jiné osobě;
f) příspěvková organizace zřízená vyšším územním samosprávným celkem;
g) jiná právnická osoba podle § 4 odst. 1 písm. e) zákona o zadávání veřejných zakázek s výjimkou
    1. právnické osoby, kterou převážně financuje, může v ní uplatňovat rozhodující vliv nebo jmenuje nebo volí více než polovinu členů v jejím statutárním nebo kontrolním orgánu obec,
    2. právnické osoby, která zadává sektorové veřejné zakázky podle § 151 zákona o zadávání veřejných zakázek.

Je samozřejmé, že před předložením vládě musel návrh zákona projít řádným meziresortním připomínkovým řízením, které probíhalo od 6. května 2024 do 9. června 2024. Ministerstvo průmyslu a obchodu navrhlo 317 připomínek, z toho 193 připomínek bylo zásadních. Všechny byly řádně vypořádány. V říjnu 2024 pak návrh zákona projednala Legislativní rada vlády a komise pro RIA se souhlasným stanoviskem. Také všechny jejich připomínky byly zapracovány.

## Datový slovník jako klíčový pilíř Datového standardu stavby

I když práce na Aktualizaci Koncepce BIM a návrhu zákona o BIM byly velmi důležité, přirozeně se nemohly zastavit ani práce v jiných oblastech. Jedním z klíčových úkolů plynoucích z Aktualizace Koncepce zavádění metody BIM v České republice je vytvoření Datového standardu staveb. K tomuto cíli se Česká agentura pro standardizaci výrazně přiblížila, když připravila Datový slovník, který je hlavním pilířem celého DSS, a především otevírá cestu k vytváření skutečně použitelných Datových standardů stavby a Datových standardů organizace. Tedy datových standardů odpovídajících potřebám konkrétního projektu. Označení slovník není v případě Datového slovníků vůbec náhodné. Jeho používání je vlastně obdobné tomu, co známe třeba při učení cizího jazyka. Existují obrovské několikasvazkové slovníky obsahující téměř všechna (nebo všechna) slova toho kterého jazyka a k nim české ekvivalenty. Najdeme tak v něm překlad úplně každého slova, které bychom mohli při používání cizího jazyka potřebovat. Takový velký slovník je jistě praktickým pomocníkem, ale pokud se rozhodneme vyrazit například na turistický výlet, pravděpodobně pro nás bude naprostá většina slovíček z takového obrovského slovníku úplně zbytečná. Během prohlížení památek, návštěv v restauracích a třeba pobytu v hotelu bude totiž využitelná jen malá část slovní zásoby jazyka. Prostě celou řadu slovíček potřebovat nebudete. Proto raději sáhnete po malém turistickém slovníčku. Vejde se nejspíše do kapsy, obsahuje mnohem méně slov, ale budou to přesně ta slova, která využijete pro konkrétní „účel užití“, tedy turistiku.

Datový slovník je pak onen obrovský lexikon. Je to totiž seznam všech stavebních předmětů, se kterými se můžete během výstavbového projektu setkat. A nezáleží na tom, jestli jde o stavební prvek, jako jsou dveře či okna, nebo například stěnu, místnost či celou stavbu. Co je ale v tomto směru klíčové, je, že každý stavební předmět má určité vlastnosti. Proto je mu přiřazena takzvaná datová šablona, která právě tyto vlastnosti obsahuje. A jde skutečně o všechny vlastnosti, které se ke konkrétnímu stavebnímu předmětu vážou po celou dobu životního cyklu stavby.

Které vlastnosti jsou relevantní, se totiž mění také v čase. Přitom jedním z klíčových přínosů metody BIM je skutečnost, že dokážeme udržet kontinuitu jednou vložených informací po celou dobu životního cyklu stavby. Samozřejmě, že jiné informace ke stavebnímu prvku přidává (a využívá) projektant při dokumentaci pro stavební povolení, jiné při tvorbě dokumentace skutečného provedení stavby, a později jiné informace bude potřebovat a vkládat facility manager při přebírání již hotové stavby.

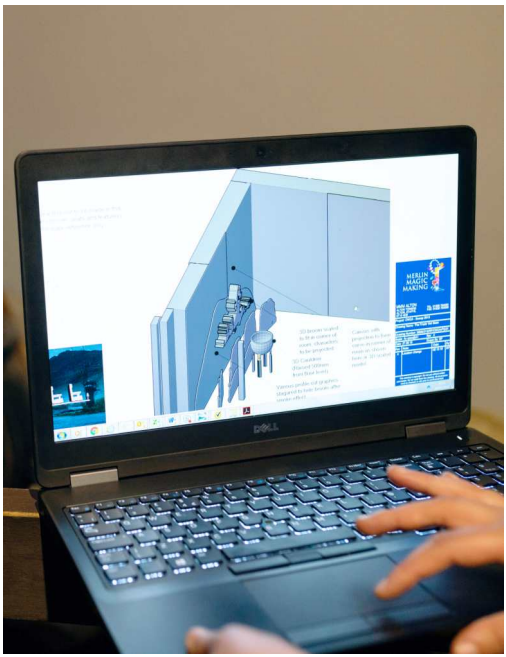
Nicméně, jakmile je jednou stavební prvek do projektu vložen, z Datového slovníku je k němu přiřazena datová šablona obsahující všechny vlastnosti. Byť v daném okamžiku vidí konkrétní aktér jen některé z nich. Ty, které má vyplnit, nebo ty, které jsou pro něj relevantní.

## Každá stavba je jiná, proto potřebujeme Datový standard stavby

Nemůže existovat stavba, která by obsahovala všechny existující stavební předměty. Něco takového není možné. A proto, tak jako existuje turistický slovníček v případě cizího jazyka, tak z Datového slovníku může vzniknout Datový standard stavby. Jak poslední slovo vypovídá, jde o datový standard přizpůsobený potřebám konkrétní stavby. Podobně si může například organizace vytvořit Datový standard organizace, přizpůsobený svým konkrétním potřebám. Co je ale zásadní, tyto dílčí datové standardy jsou výběrem stavebních prvků z Datového slovníku.

Proč je to tak důležité? Tento přístup totiž umožní přizpůsobit datový standard jedinečnosti každé stavby, ale současně zachovat udržitelnost strojové čitelnosti informací. Jedná se totiž vždy o výběr stavebních předmětů a jejich vlastností, které jsou relevantní pro daný typ stavby a jejích částí (prostor umístění a systém, ve kterém se nachází daný stavební předmět na úrovni komponenty ovlivňuje rozsah informací, které jsou pro takto umístěnou komponentu relevantní) a zohledňují úroveň informačních potřeb (UIP z anglického LOIN).

Zjednodušeně řečeno, v Datovém standardu stavby využijeme relevantní stavební předměty a jejich datové šablony. Také obsah datových šablon v konkrétním Datovém standardu stavby bude závislý například na druhu stavby. Je dost pravděpodobné, že ventil v jaderné elektrárně bude mít trochu jiné vlastnosti než ventil topení v rodinném domku. Nicméně pracujeme se standardizovanou strukturou informací – stále máme jeden stavební předmět (ventil) a jeho datovou šablonu. I když z této datové šablony vybereme jen část vlastností, nijak to neovlivní strojovou čitelnost informace. Struktura datové šablony se totiž nemění.



## Datový standard staveb získává pevný základ

Poměrně často zaznívá z odborné veřejnosti námitka, že nelze vytvořit Datový standard staveb vzhledem k individuálním potřebám každé jedné stavby. Vytvoření Datového slovníku nás ale k tomuto cíli přibližuje, protože jde o klíčovou část DSS. Datový standard staveb je totiž komplex skládající se ze čtyř základních komponent. Tou první je právě Datový slovník, který nám dává možnost pracovat s negrafickými (alfanumerickými) informacemi. Datový slovník bude doplněn jakýmsi grafickým manuálem, tedy Požadavky na tvorbu IMS a DiMS. Ten stanoví pravidla pro práci s grafickými informacemi.

Aby bylo možné vytvářet skutečně funkční Datové standardy stavby, musí být doplněny ještě o další dvě důležité komponenty. První z nich jsou smluvní dokumenty (sem patří například BIM Protokol či BEP) a druhou, ovšem nikoli méně důležitou, jsou metodiky, které bude Česká agentura pro standardizaci postupně vydávat. Datový standard staveb bude pak souhrnem těchto komponent.

# Atestace elektronických systémů spisových služeb

Do portfolia činností, které Česká agentura pro standardizaci zajišťuje, přibyla před rokem úplně nová aktivita, kterou jsou atestace elektronických systémů spisových služeb. O co jde a k čemu je to dobré?

Nejprve je potřeba vysvětlit, co spisová služba je. Zjednodušeně řečeno, jde o souhrn činností, které se týkají zajištění odborné správy dokumentů, a to od jejich vytvoření či doručení až po jejich vyřízení a uložení, resp. vyřazení. Kořeny pravidel vedení spisové služby nalezeme ve způsobu vykonávání byrokracie už od dob Rakouska-Uherska. Právě od této doby je v naší veřejné správě používán systém na evidenci celého životního cyklu dokumentů, záznamů, spisů apod., z něhož se vyvinula i dnešní spisová služba. V minulosti se používala v papírové podobě, dnes existuje řada počítačových aplikací na řešení této problematiky. Ty označujeme pojmem elektronický systém spisové služby, zkráceně eSSL.

Pravidla vedení spisové služby jsou pro všechny úřady (ale správněji bychom měli napsat veřejnoprávní původce, kterými jsou nejen úřady) v zásadě stejná. Stanovuje je zákon o archivnictví a spisové službě a jeho prováděcí vyhlášky. Spolu s rozvojem elektronizace a vedení spisové služby s využitím eSSL k nim přibyl také Národní standard elektronických systémů spisových služeb (NSESSS), což je již téměř technická norma, která velmi podrobně stanovuje, jakou funkčnost tyto elektronické systémy musí mít. Tento způsob kodifikace zajišťuje, že na trhu můžeme najít celou řadu softwarových řešení, které by dané specifikace měly splňovat, a přitom není nijak omezeno jejich konkurenční působení.

Až donedávna však nebyl žádný způsob, jak by si mohli veřejnoprávní původci ověřit, zda systém, který používají nebo právě pořizují, skutečně všem pravidlům odpovídá a umožní jim vést spisovou službu přesně tak, jak mají. Změnou archivního zákona byl tedy zaveden institut atestací, jejichž cílem je právě ověřit soulad dané eSSL s požadavky zákona, vyhlášky a národního standardu. Vykonáváním atestací byla ze strany Ministerstva vnitra, do jehož kompetence vedení spisových služeb spadá, pověřena právě Česká agentura pro standardizaci.

Příprava procesu atestací nebyla nijak jednoduchou záležitostí. Na přípravě legislativy i metodiky se podíleli nejen odborníci z Ministerstva vnitra, Národního archivu a atestačního střediska, ale i dodavatelé eSSL v rámci pracovní skupiny ICT

Unie. Odborná diskuze na toto téma byla dlouhá, někdy i bouřlivá, ale výsledkem je konsensuální řešení, které je použitelné pro praxi.

Jak již bylo řečeno, cílem bylo v rámci atestačního procesu nastavit takové podmínky, které jednak ověří všechny požadavky, stanovené zákonem, vyhláškou a národním standardem eSSL a jednak zaručí objektivní a transparentní hodnocení všech atestovaných systémů. I proto byly všechny požadavky převedeny do konkrétních testovacích scénářů, které budou pro všechny atestované spisovky stejné, a navíc se s nimi každý může seznámit na webových stránkách atestačního střediska. Pravidla atestací byla stanovena s ohledem na jejich maximální objektivitu a transparentnost a jsou dostupná všem na webových stránkách agentury. Díky tomu se každý dodavatel spisových služeb může na atestaci detailně připravit.

Proces přípravy atestačního prostředí prošel i úspěšnou certifikací shody systému managementu a kvality s požadavky ČSN EN ISO 9001:2016.

Zatím je předčasné hodnotit, jak atestace přispějí ke kultivaci a zlepšení výkonu této agendy v České republice. Každopádně by měly posílit právní jistoty původců při výběru toho správného softwaru a ukázat směr, kterým se může digitalizace ubírat při zachování nastavených standardů a konkurenčního prostředí.

## Pravidla atestací, stanovená v zákoně č. 499/2004 Sb., o archivnictví a spisové službě

### § 69c

(1) Atestační středisko provede atestaci na základě objednávky a postupem, za podmínek a za úplatu stanovených ministerstvem.

(2) Atestační středisko provede atestaci do 3 měsíců ode dne objednání atestu. Není-li možné provést atestaci v této lhůtě, atestační středisko o tom ještě před uplynutím lhůty vyrozumí toho, kdo atestaci objednal, a sdělí mu, do kdy bude atestace provedena.

(3) Splňuje-li elektronický systém spisové služby požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu, vydá atestační středisko tomu, kdo atestaci objednal, písemný atest. Atestační středisko současně zveřejní atest na svých internetových stránkách a zašle jej ministerstvu, které oznámí jeho vydání ve Věstníku ministerstva.

(4) Nesplňuje-li elektronický systém spisové služby požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu, vyrozumí o tom atestační středisko toho, kdo atestaci objednal, a ministerstvo a sdělí jim důvody nesplnění požadavků.

### § 69d

(1) Atest platí 2 roky ode dne jeho vydání.

(2) Změní-li se v průběhu platnosti atestu požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 nebo národního standardu, atest nadále platí. Změní-li se v průběhu platnosti atestu elektronický systém spisové služby, atest nadále platí, vyrozumí-li ten, kdo atestaci objednal, ministerstvo a atestační středisko, které atest vydalo, o změnách v elektronickém systému spisové služby a zároveň prohlásí, že elektronický systém spisové služby nadále splňuje požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu.

(3) Má-li ministerstvo důvodné pochybnosti, zda elektronický systém spisové služby splňuje v době platnosti atestu požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu, a nejde-li o situaci podle odstavce 2 věty první, uloží atestačnímu středisku provést na náklady atestačního střediska revizi atestu. Na revizi atestu se použijí ustanovení tohoto zákona o postupu, podmínkách a lhůtách provedení atestace obdobně.

(4) Splňuje-li elektronický systém spisové služby nadále požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu, atestační středisko o této skutečnosti vyrozumí ministerstvo.
(5) Nesplňuje-li již elektronický systém spisové služby požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu, atestační středisko vyrozumí ministerstvo a toho, kdo atestaci objednal, o této skutečnosti a sdělí jim důvody nesplnění požadavků. Atestační středisko současně zneplatní atest, zveřejní informaci o zneplatnění atestu na svých internetových stránkách a zašle ji ministerstvu, které ji zveřejní ve Věstníku ministerstva, a tomu, kdo atestaci objednal.

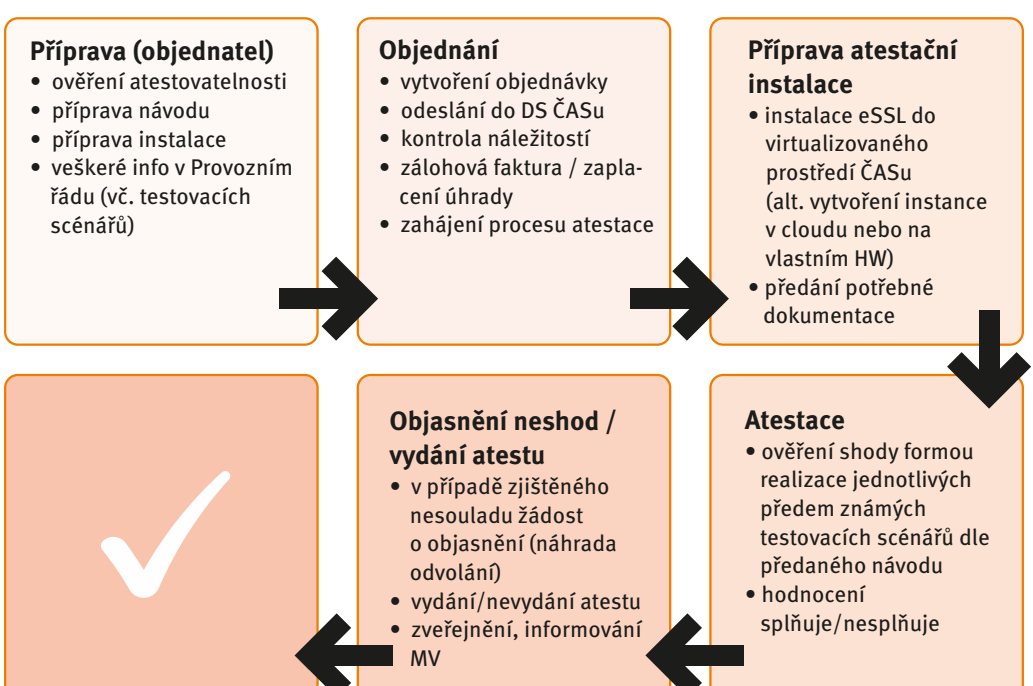
**1. 7. 2025**

- Zakazuje se nabízet nebo dodávat veřejnoprávním původcům elektronický systém spisové služby, který nesplňuje požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu a u kterého není splnění těchto požadavků potvrzeno atestem (§ 69e zákona)

**1. 1. 2027**

- Veřejnoprávní původci mohou využívat pouze elektronické systémy spisové služby, které splňují požadavky tohoto zákona, vyhlášky podle § 70 odst. 1 a národního standardu a u kterých je splnění těchto požadavků potvrzeno atestem. (§ 63 odst. 3 zákona)

## Jak bude atestace probíhat?




*Petr Stiegler*
*Oddělení atestací elektronických spisových služeb*
*Česká agentura pro standardizaci*


# Aktuality

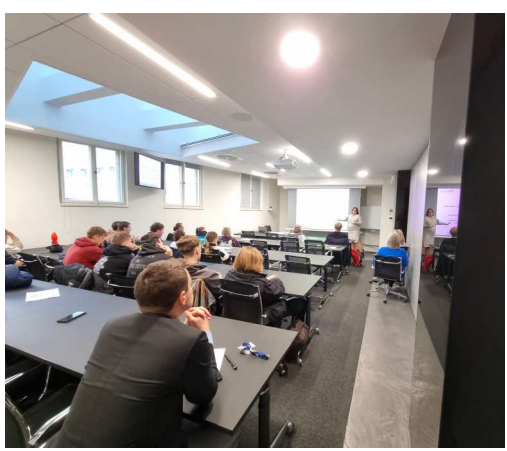
## Česká agentura pro standardizaci na Mezinárodním strojírenském veletrhu v Brně

Česká agentura pro standardizaci se v říjnu zúčastnila 65. ročníku Mezinárodního strojírenského veletrhu na brněnském výstavišti, kterého se stalo součástí 1386 vystavujících firem a navštívilo ho více než 55 tisíc návštěvníků.

Zástupci ČAS byli připraveni zodpovědět dotazy týkající se technických norem, jejich tvorby a možnosti přístupu k těmto normám. Návštěvníci se mohli dozvědět o aktuálních trendech v oblasti standardizace a pro zpestření si mohli vyzkoušet interaktivní formu – vědomostní kvíz, který prověřil jejich znalosti o technických normách a standardizačních procesech.


V rámci veletrhu pak ČAS ve spolupráci s ÚNMZ uspořádala odborný seminář s názvem Nové nařízení Evropského parlamentu a Rady (EU) 2023/1230 o strojních zařízeních. Seminář zahájil Ing. Jiří Kratochvíl, předseda ÚNMZ. Následoval Ing. Josef Kadlec, který představil činnost ÚNMZ a roli Odboru státního zkušebnictví. Hlavní část semináře byla věnována novinkám, které přineslo nařízení (EU) 2023/1230 o strojních zařízeních. Ing. Jitka Futerová se zaměřila na digitální návod k použití a digitální EU prohlášení o shodě. Dále diskutovala o nových technologiích, jako jsou autonomní mobilní stroje a umělá inteligence, a povinnosti, které tyto inovace přinášejí výrobcům strojních zařízení. Tomáš Velát se zaměřil na harmonizované evropské normy (hEN) a jejich vztah k novému nařízení. Vysvětlil, jakým způsobem jsou harmonizované normy propojené s legislativními požadavky, jaké jsou požadavky na jejich zpracování a jaký časový rámec je stanoven pro revizi stávajících norem a tvorbu nových.

Seminář zakončila Ing. Ivana Kolínská, která informovala účastníky o možnostech přístupu k technickým normám a ochraně autorských práv při jejich užívání. Seminář se setkal s velkým zájmem a účastníci si odnesli cenné informace o tom, jaké změny v oblasti strojních zařízení nařízení (EU) 2023/1230 přináší a jak se mohou na nové povinnosti připravit.



## Spolupráce se středními školami: Seznamujeme studenty středních škol s technickými normami

Česká agentura pro standardizaci zahájila nový projekt exkurzí pro studenty středních škol, jehož cílem je seznámit mladou generaci s technickými normami a významem standardizace. První exkurze se uskutečnila začátkem prosince a účastnili se jí studenti čtvrtého ročníku průmyslové střední školy Letohrad, zaměřené na obory dopravní, stavební a geodézie. Exkurzi zahájil předseda ÚNMZ Jiří Kratochvíl, který studentům přiblížil roli ÚNMZ a provázanost s činnostmi ČAS. Ředitelka oddělení standardizace Zdena Slaná studenty seznámila s podstatou standardizace, procesem tvorby norem, fungováním technických normalizačních skupin a přiblížila také význam standardizace na národní, evropské i globální úrovni. Vedoucí oddělení péče o zákazníky Ivana Kolínská představila systém distribuce norem a pravidla zacházení s normativními dokumenty a publikacemi. Na závěr exkurze studenty čekal vědomostní kvíz, který prověřil jejich znalosti. V příštím roce plánujeme v tomto projektu pokračovat a nabídnout podobné exkurze i dalším středním školám, aby se co nejvíce studentů mohlo seznámit s klíčovou rolí standardizace ve společnosti.

# Generální zasedání ISO 2024

## Formování budoucnosti prostřednictvím technických norem

Motem letošního generálního shromáždění ISO (ISO GA), které proběhlo na počátku září, bylo prolamování hranic (breaking borders). Toto téma odráží nutnost překonávat výzvy, které přesahují hranice, jako je změna klimatu, ztráta biodiverzity a technologický pokrok. Týdenního jednání se zúčastnilo více než 10 000 lidí, osobně i online, z více než 170 zemí.

Setkání ukázalo, jak mohou mezinárodní technické normy podporovat udržitelný a inkluzivní růst, využití a odpovědné zavádění umělé inteligence a utvářet budoucnost lidského kapitálu. Akce posloužila jako výkonná platforma pro zapojení různých hlasů napříč sektory, povzbuzení spolupráce a podpora inovativních řešení, která překračují geografické a oborové hranice.

Na zahajovacím ceremoniálu vystoupili prominentní řečníci, včetně Luise Carlose Reyese Hernándeze, kolumbijského ministra obchodu, průmyslu a cestovního ruchu, Héctora Aranga, prezidenta ICONTEC, a představitelů ISO. Všichni se shodli, že žijeme v nejisté době, která vyžaduje nové přístupy a nápady, odvahu a inovace.


*Vedoucí delegací členů ISO*

## Transformativní potenciál AI

Jedním z nejdůležitějších workshopů na ISO GA byl transformativní potenciál umělé inteligence (AI). Nosným tématem byla klíčová role mezinárodních technických norem při urychlování inovací řízených umělou inovací a zároveň zdůraznění významu odpovědné umělé inteligence. Během tří setkání účastníci diskutovali o potenciálu umělé inteligence jako katalyzátoru růstu a globálního pokroku, zejména v oblastech zdravotnictví a robotizace.

**Klíčové poznatky workshopu:**

- Umělá inteligence má obrovský potenciál, ale je třeba ji vyvíjet a zavádět zodpovědně a bezpečně – odpovědí jsou technické normy a sdílení pravidel správné praxe.
- Nástroje umělé inteligence vyvolávají silnou odezvu mezi uživateli, podniky a tvůrci politik. Existuje naléhavá potřeba jasných, konzistentních norem, které lze univerzálně použít v různých odvětvích.
- Nezačínáme od nuly. Můžeme se poučit z desetiletí zavádění standardů v jiných oblastech, zejména v IT.
- Data jsou klíčová! Mít silná data je zásadní nejen pro provozní úspěch, ale také pro udržení důvěry veřejnosti v systémy AI.

## Prosazování globální udržitelnosti prostřednictvím technických norem

Na dalším jednání se sešli odborníci na udržitelnost, kteří diskutovali kritické výzvy současnosti: odolnost vůči klimatu, oběhové hospodářství a přechod na udržitelnou energii. Opět byla zdůrazněna zásadní role mezinárodních norem při řízení transformativních řešení, podpoře meziodvětvové spolupráce a škálování přeshraničního dopadu s cílem urychlit opatření v oblasti klimatu.

**Nejdůležitější závěry diskuze:**

- Normy ISO spolu s vládními nařízeními a politikami mohou urychlit přijetí využití obnovitelné energie, zlepšit energetickou účinnost a podpořit technologický pokrok.
- Kulturní kontext je vším. Je důležité komunikovat na národní a regionální úrovni, aby se nám podařilo změnit myšlení, a podpořili jsme tak zavádění osvědčených postupů.
- Nejedná se jen o vytváření nejlepších technických norem, musíme udělat více, abychom jejich výhody dokázali vysvětlit trhu, průmyslu a tvůrcům politik.

## Nové pokyny ISO/UNDP pro udržitelné cíle OSN

Ve středu 11. září 2024 ISO a Rozvojový program OSN (UNDP) vydaly společně vůbec první mezinárodní pokyny, které mají podnikům a organizacím pomoci plnit cíle udržitelného rozvoje OSN (SDG). Tento významný dokument nabízí praktický návod pro organizace všech velikostí a sektorů, jak systematicky řídit a optimalizovat svůj dopad na udržitelný rozvoj.

Tento Pokyn ISO/UNDP PAS 53002:2024 *Guidelines for contributing to the United Nations Sustainable Development Goals (SDGs)* je zdarma ke stažení na webových stránkách ISO.

## LDE Award

Na letošním generálním shromáždění prezident ISO předal cenu Lawrence D. Eichera (LDE) odborníkům z technické komise ISO/TC 309 *Řízení a správa organizací*. Je důkazem odhodlání výboru podporovat osvědčené postupy a podporovat globální spolupráci v této kritické oblasti.

*LDE Award: Vedení komise ISO/TC 309, prezident ISO Dr. Sung Hwan Cho, ISO Secretary-General Sergio Mujica a Javier Garcia, ISO Vice-President technical management*

## Nový prezident ISO

Klíčovým vrcholem jednání byla volba nových členů Rady a příštího prezidenta ISO. Tím byl zvolen Dr. Khaled Soufi, předseda Egyptské organizace pro standardizaci a kvalitu (EOS), který se ujme funkce v roce 2026.

*Předseda ÚNMZ, Ing. J. Kratochvíl*


princezna Anna

# 88. generální zasedání IEC

V Edinburghu proběhlo 88. generální zasedání IEC (Mezinárodní elektrotechnická komise) za účasti více než 1200 expertů a zástupců národních normalizačních organizací z téměř 90 zemí. Dalších přibližně 450 se připojilo online.

Cílem jednání byla diskuze o nových a inovativních způsobech řešení konkrétních environmentálních, sociálních a správních výzev prostřednictvím aplikací mezinárodních norem a systému posuzování shody.

Jedním z hlavních témat bylo usnadnění přechodu k propojené a plně elektrické společnosti prostřednictvím technických norem a posuzování shody, kde budou různé sektory jako energetika, zdravotnictví a mobilita elektrifikovány a digitalizovány, aby poskytly více ekonomických příležitostí pro každého. Na základě celosvětového přístupu k dostupné, obnovitelné a udržitelné energii bude digitálně propojená společnost stále více využívat technologie, jako je umělá inteligence nebo účinná dekarbonizaci energetických infrastruktur.

Setkání bylo o to významnější, že si letos připomínáme 200. výročí narození lorda Kelvina, zakládajícího prezidenta IEC. Bylo proto docela příhodné, že letošní generální zasedání proběhlo ve Skotsku, kde se lord Kelvin z Largsu (vlastním jménem William Thomson) zabýval matematickou analýzou elektřiny, formuloval první a druhý termodynamický zákon a zasloužil se o rozvoj vznikajícího oboru fyziky. Byl zvolen prezidentem Královské společnosti a jako první britský vědec byl povýšen do Sněmovny lordů.

Kromě oficiálního programu IEC zorganizovala pořádající národní normalizační organizace Velké Británie BSI (The British Standards Institution) řadu zasedání pokrývajících čtyři tematické oblasti zaměření:

- City-to-City Exchange: rozvoj měst v otázkách cirkularity, udržitelnosti, vzájemného propojení nebo bezpečnosti;
- AI Technology & Standards Summit: příležitosti a výzvy umělé inteligence;
- Quantum Technology Symposium: využití kvantové technologie;
- Enabling a Net Zero Future: podpora cílů Net Zero prostřednictvím technických norem.

*zleva: Ing. Jiří Kratochvíl, předseda ÚNMZ, a Ing. Petr Kubeš, národní sekretář IEC*

Vrcholem generálního zasedání bylo vůbec první IEC Community Symposium, které bylo živě přenášeno na YouTube. Významní odborníci z rozvojových i rozvinutých zemí zkoumali osvědčené postupy, příležitosti a výzvy spojené s integrací obnovitelné energie do elektrické sítě.

„*Technologie má obrovský potenciál měnit životy k lepšímu a být silou dobra. Budování důvěry v nové technologie vyžaduje samozřejmě i koordinaci a spolupráci při tvorbě norem jako záruk, které pomohou přinést akceptaci a ekonomický přínos. Jsme potěšeni, že můžeme být hostiteli letošního generálního zasedání, kde představíme význam mezinárodních norem pro průmysl, akademickou sféru, regulátory trhu i veřejnost takovým způsobem, který nám pomůže zahájit diskuzi o rizicích, ale zejména příležitostech, globálního přechodu k plně elektrické a propojené společnosti,*“ řekl Scott Steedman, generální ředitel Standardizace, BSI.

Jednou z nejvýznamnějších událostí generálního zasedání byla návštěva královské princezny Annny. Ve svém projevu zdůraznila význam této čtyřdenní akce pro podporu inovací, udržitelnosti a globální spolupráce při realizaci vize IEC o plně elektrické a propojené společnosti. Upozornila zejména na závazek IEC zajistit, aby se do procesu standardizace zapojily hlasy ze všech koutů světa. Ocenila také program IEC pro mladé profesionály a jeho úsilí o propagaci standardizace a podporu žen v kariéře v oborech STEM.

Princezna Anna vyjádřila obdiv nad trvalým významem IEC a její schopností podporovat globální spolupráci ve stále složitějším světě.

## Cena lorda Kelvina

IEC udělila svou výroční cenu lorda Kelvina kanadskému inženýrovi Eliasi Ghannoumovi. Toto ocenění získal za výjimečný a dlouhodobý přínos světové elektrotechnické normalizaci.

Elias Ghannoum má více než 50 lety zkušeností v oblasti nadzemních přenosových vedení, mezi jeho odborné znalosti patří navrhování a optimalizace vysokonapěťových přenosových vedení a stožárů a analýzy konstrukcí a poruch.

Během své dlouholeté kariéry poskytoval pan Ghannoum inženýrské služby pro více než 60 provozovatelů přenosových soustav a veřejných služeb v Kanadě, Řecku, Indii, Jižní Africe, USA a Brazílii. Jeho zapojení do tvorby norem trvá více než 45 let.

Lord Kelvin byl raným zastáncem větrné energie a pevně věřil, že „život a duše vědy jsou v její praktické aplikaci“, kterou lze využít ve prospěch lidstva. IEC je důstojným nástupcem jeho odkazu v prosazování vlivu technologií pro lepší, inkluzivnější a udržitelnější svět. Díky svému 118 let starému dědictví, globální komunitě a platformě založené na konsensu má IEC jedinečnou pozici, aby podpořila tuto pozitivní změnu a pomohla tvořit udržitelnější budoucnost.


*zleva: Jo Cops, prezident IEC, a Elias Ghannoum*


# Nový a jednotný návod, jak zavést a řídit v organizaci ESG

***ESG reporting je v EU novou legislativní povinností pro řadu velkých firem. Pochopitelně se to dotýká i jejich hodnotového řetězce. ESG však není jen evropským výmyslem, jak se řada lidí mylně domnívá, setkáte se s ním i v jiných končinách. Přístupů k němu je mnoho a organizace jsou často zmatené a tápou, jak vše sladit, zejména tehdy, pokud třeba podnikají na celosvětovém trhu.***
***Proto jsme v rámci mezinárodního týmu připravili pod BSI a ISO jednotný postup pro implementaci a účinné řízení ESG v globálním kontextu. Oficiální verze je zdarma ke stažení na stránkách ISO organizace a byla představena dne 14. listopadu 2024 v rámci summitu COP 29 v Baku.***

## IWA 48:2024 *Framework for implementing environmental, social and governance (ESG) principles*

Organizace potřebují různé nástroje nejen pro zveřejňování, ale i pro integraci udržitelnosti do svých každodenních operací. Jinými slovy potřebují pomoci s tím, jak jednotlivé oblasti, které považují za významné, mají řešit v praxi.

Tento mezinárodní rámec poskytuje strukturu a návod, jak začlenit ESG aspekty do kultury organizace a jejího každodenního provozu. Zkrátka jak ESG řídit. Až dosud totiž chyběl mezičlánek mezi požadavky a reportingem.

Pokrývá všechny prvky ESG a nabízí integrovaná řešení s měřitelnými KPIs i hodnocením úrovně vyspělosti v rámci organizace. Abyste mohli měřit, a následně vykazovat svou ESG výkonnost. Primárně jde právě o dosažení výkonnosti v oblastech ESG s kvalitním reportingem, ne o reporting samotný.

Stěžejní je tedy správné uchopení governance (řízení a správy organizace). Faktoru, který jednoznačně ovlivní to, jakých výsledků dosáhnete ve všech oblastech ESG. V dokumentu najdete i příklady cílů udržitelnosti a souvisejících opatření. K řízení jednotlivých oblastí ESG nabízí i odkazy na relevantní ISO standardy, které můžete využít ve své praxi, a to jen z části, nebo zcela. ISO standardy jsou tvořené lidmi z praxe a také praxí mnoha milionů organizací prověřené, navíc uznávané v dodavatelsko-odběratelských vztazích napříč zeměmi i kontinenty. ISO knihovna je dnes plná inspirace.

**Co najdete v obsahu?**

- zásady a principy, které musíte v ESG začlenit do firemní kultury, a způsoby tohoto začlenění;
- rizika a příležitosti ESG;
- odpovědnost a transparentnost;
- jak identifikovat a zapojit zúčastněné strany;
- způsob, jak přistoupit k hodnocení materiality (významnosti);
- klíčové ukazatele výkonnosti ESG a jejich úrovně podle priorit;
- příklady cílů i opatření;
- leadership v ESG, včetně tzv. konstruktivní výzvy, komunikace, organizační kultury apod.;
- audit a reporting ESG;
- neustálé zlepšování.

**Jaké jsou ambice tohoto standardu?**

- vytvořit postup ESG na základě dobré praxe z celého světa;
- pomoci organizacím integrovat ESG požadavky do řídicích a provozních procesů;
- zajistit interoperabilitu;
- pomoci malým a středním podnikům zorientovat se v různých přístupech.

IWA 48:2024 je nástroj pro transformaci vaší organizace směrem k udržitelnosti a odpovědnosti. Zároveň podporuje konzistenci, srovnatelnost a spolehlivost postupů a výkaznictví ESG na globální úrovni. Sjednocuje jazyk a principy napříč světem. Spolupráce na něm probíhala i s organizacemi EFRAG, ISSB a dalšími. Nemusíte se tedy obávat, že by šlo o materiál v rozporu s pravidly CSRD a EU výkaznictvím.

**Čím začít?**

Analýzou materiality (významnosti) ve spolupráci s relevantními zainteresovanými stranami. A následně interním auditem (GAP analýzou) vůči požadavkům na reporting.

Teprve pak můžete odpovědně plánovat své aktivity v oblasti udržitelnosti.

> Komplexní a systematický přístup k ESG pomáhá identifikovat a řešit potenciální environmentální, sociální a správní rizika dříve, než se stanou reálnými a nákladnými problémy.

*Veronika Soukupová*
*CEO S-cope*

*v.soukupova@s-cope.cz | www.s-cope.cz*
*členka mezinárodního týmu pro vývoj IWA 48 a národní technické normalizační komise pro systémy řízení ISO, autorka knihy ISO a ESG pro udržitelný růst organizací (nakladatelství Wolters Kluwer), spolupořadatelka ESG meetupů ve spolupráci s Českou tiskovou kanceláří*

# S ČSN máte kybernetickou bezpečnost pod palcem

ČSN P CEN/TS 16428
Profily biometrické interoperability
– Nejlepší praxe pro snímání najednou všech deseti otisků

ČSN EN ISO/IEC 2382-37
Informační technologie
– Slovník
– Část 37: Biometrika

ČSN EN IEC 63154
Námořní navigační a radiokomunikační zařízení a systémy
– Kybernetická bezpečnost
– Obecné požadavky, metody zkoušení a požadované výsledky zkoušek

ČSN EN IEC 62645
Jaderné elektrárny
– Systémy kontroly, řízení a elektrického napájení
– Požadavky na kybernetickou bezpečnost

ČSN EN ISO/IEEE 11073-40101
Zdravotnická informatika – Interoperabilita zařízení
– Část 40101: Základy – Kybernetická bezpečnost – Procesy posuzování zranitelností

# Pohled HZS ČR na problematiku ventilačních šachet, vzduchotechniky a obecně odvodů zplodin hoření od spotřebičů paliv

V souvislosti s problematikou požární a provozní bezpečnosti vzduchotechniky bych rád do tohoto pojmu zahrnul systémy nejen pro prostý odvod vzduchu, ale také systémy odvádějící zplodiny hoření a produkty vznikající například v kuchyňských provozech. Tyto systémy, ačkoliv jsou nepostradatelné pro komfort a hygienu, mohou v případě zanedbané údržby a opotřebení představovat významná požární rizika. To platí obzvláště v prostorách, kde se pohybuje velké množství osob, jako jsou kancelářské prostory, obytné budovy a restaurační zařízení.

Vzduchotechnické systémy jsou z technického hlediska vystaveny značné zátěži, která může vést k opotřebení materiálů a hromadění usazenin. Právě usazeniny, v podobě mastných částic nebo prachových nánosů, jsou častými příčinami požárů – mohou se proměnit v hořlavé směsi, které se za určitých podmínek snadno vznítí. Takové vznícení je o to nebezpečnější, že vzduchotechnické systémy jsou zpravidla rozvedeny po celé budově, a tudíž mohou napomáhat rychlému šíření požáru.

Hasičský záchranný sbor České republiky (HZS ČR) dlouhodobě sleduje počet požárů vzniklých ve vzduchotechnických systémech. V posledních pěti letech evidujeme přibližně 50 takových požárů ročně. Vzhledem k tomu, že k nim dochází převážně v místech s vysokou koncentrací osob, vede to často k nutnosti evakuace velkého počtu osob a značnému nasazení sil a prostředků. Tato skutečnost podtrhuje význam pravidelné údržby a kontroly vzduchotechnických zařízení, které považujeme za jeden z klíčových nástrojů prevence.

Vnímám také obdobné snahy v České republice, kde se stále více prosazuje potřeba stanovit jasná pravidla pro provoz a údržbu vzduchotechniky v souladu s technickými standardy a bezpečnostními normami. Inspirací nám může být příklad ze severní Evropy, konkrétně ze Švédska. Z mé vlastní praxe vím, že zde mají zaveden důmyslný systém čištění vzduchotechniky, kde tuto činnost vykonávají kominíci. Ti zároveň podléhají přímému dohledu samosprávních orgánů, což poskytuje důležitý garanční mechanismus pro zajištění bezpečnosti a důkladné údržby těchto zařízení.

V rámci HZS ČR považujeme za nezbytné, aby každý provozovatel vzduchotechnických systémů zajistil pravidelnou údržbu a čištění těchto zařízení, používal kvalitní materiály a komponenty odolné vůči vysokým teplotám a aby bylo možné provádět pravidelné revize a kontroly v souladu s platnými právními požadavky. Neméně důležitým aspektem je odbornost osob, které se podílejí na instalaci a údržbě těchto systémů. Pravidelná školení a vzdělávání jsou cestou k tomu, aby všichni, kdo přijdou do kontaktu s těmito systémy, byli vybaveni potřebnými znalostmi pro jejich bezpečné provozování.

Kromě důrazu na údržbu a pravidelné revize doporučujeme také zavádění detekčních systémů kouře a tepla přímo do ventilačních šachet. Takové systémy umožňují rychlé rozpoznání možného ohrožení a adekvátní reakci na vznikající riziko, což významně přispívá k ochraně osob i majetku.

Věříme, že vytvoření jednoznačných a závazných standardů, jejich dodržování a účinné vymáhání jsou zásadními kroky k zajištění vysoké úrovně požární bezpečnosti. Tyto standardy musí být nejen přijaty, ale i široce zavedeny do praxe, aby zajistily důslednou ochranu životů a zdraví obyvatel v budovách.

*David Schön*
*Hasičský záchranný sbor ČR*

# Odtahové potrubí v kuchyních

**Jaká jsou rizika, jak je to s údržbou a bezpečností, nám prozradil Dalimil Petrilák z Alkion service s.r.o., a viceprezident Evropské asociace pro čistou vzduchotechniku (EVHA).**

Pro údržbu a čištění odtahového vzduchotechnického potrubí z digestoří v restauracích by se dal použít mírně upravený slogan z reklamní kampaně, a to „Nečistíš? Vyhoříš!“. Statistiky HZS ČR i zahraniční zkušenost ukazují, že riziko požáru v mastném a znečištěném potrubí ve velké kuchyni je poměrně zásadní, a přitom současnou legislativou jen málo a nedostatečně řešené. Poznatky z terénu přitom říkají, že problém řešitelný je a je důležité o něm nejen mluvit, ale také aktivně vyvíjet snahu pro větší ochranu nejen kuchařů a zaměstnanců restaurací, ale také pro jejich hosty a obyvatele domů, ve který restaurace jsou. Požár ve vzduchotechnice je jen těžko řešitelný, a prevence je tedy klíčovým faktorem pro předcházení těmto požárům.

**Můžete nám přiblížit, jak funguje odvětrávání v průmyslových kuchyních?**
Systém funguje poměrně jednoduše a podobá se klasickému odvětrávání, které známe z domácností, jen je výrazně větší a robustnější. Digestoř zachycuje páry a výpary z vaření a odvádí je do centrálního potrubí. V potrubí je umístěný ventilátor, který může být buď přímo v potrubí, nebo na jeho konci, kde se nachází vzduchotechnická jednotka. Tento ventilátor zajišťuje, že vzduch je vyfukován ven z budovy, čímž se odvádí nežádoucí pachy a vlhkost z kuchyně.

**Je možné čistit všechny typy odtahových potrubí v kuchyních?**
To záleží na typu materiálu a přístupnosti. Většina standardně používaných materiálů, jako je pozinkovaný plech nebo moderní ALP potrubí, se dá čistit poměrně dobře. Problémem je flexibilní potrubí, tzv. „husí krky“. Tato potrubí jsou nevhodná, protože je prakticky nemožné je důkladně vyčistit a nesou s sebou další bezpečnostní rizika. V některých evropských zemích je používání tohoto flexibilního potrubí v průmyslových kuchyních dokonce zakázáno. Celkově vzato je klíčová otázka přístupnosti – některá potrubí mohou být kvůli umístění velmi těžko dostupná.

**Jak je běžně konstruováno odtahové potrubí v České republice?**
Běžnou praxí je zde bohužel instalace standardního vzduchotechnického potrubí z plechu, které se montuje klasickým způsobem a občas se spoje utěsní silikonem. Tento typ instalace ale není ideální pro kuchyně, kde se v potrubí rychle usazují mastnoty a zbytky tuků z vaření. Vhodnější je vodotěsné svařované potrubí, které se v některých evropských zemích používá častěji, protože výrazně snižuje požární riziko a také umožňuje pravidelnou a efektivní údržbu. Další variantou jsou tzv. GIF stropy, které kondenzují mastnotu přímo ve stropu, což výrazně omezuje zanášení potrubí, i když tato technologie je finančně nákladnější a údržba je složitější.

**Jak je možné, že se v potrubí usazuje tuk, i když mám nainstalované tukové filtry?**
Žádný filtr není úplně stoprocentní. Tukové filtry v digestořích obvykle dosahují účinnosti mezi 80 až 90 %, takže zbylá část mastnoty proniká do potrubí. V kuchyních, kde se často frituje nebo griluje, se pak potrubí zanáší tukem poměrně rychle, a to i přes filtry.

**Pojďme se teď blíže podívat na požární riziko. Jak velké je riziko vzniku požáru v těchto systémech?**
Riziko je bohužel vysoké. Už vrstva tuku o tloušťce 0,5 mm je vysoce hořlavá. Pokud navíc digestoř není vybavena samozhášecím systémem, čemuž tak je ve většině kuchyní, může dojít k rychlému zahoření celého odtahového systému. Experimenty ukazují, že při vrstvě tuku kolem 0,5 mm je riziko vznícení velmi vysoké, a pokud v kuchyni například dojde k flambování nebo vznícení na sporáku, oheň se může rychle šířit celým systémem.
Jsme vlastně docela v paradoxní situaci. Na jednu stranu se na požární bezpečnost klade velký důraz, řeší se hasicí přístroje na chodbách, požární ucpávky, odolnost různých materiálů nebo barev. Na druhou stranu nemáme téměř žádnou legislativu ani pravidla na část objektu, ve které je požární riziko extrémně vysoké – a tím myslím právě vzduchotechnické potrubí v restauracích a průmyslových kuchyních. Nachází se tu vysoce hořlavý materiál, v kuchyních se pracuje s ohněm a vysokými teplotami. A nikdo závazně neurčuje četnost revizí nebo čištění.

**Hrozí podobné riziko i v domácích kuchyních?**
Ano, i když v menší míře. V domácnosti se obvykle neprodukuje tolik mastnoty, takže riziko je nižší. Problémem mohou být starší systémy, například v panelových domech, kde digestoře ústí do společného svislého potrubí. To může být zaneseno zbytky mastnoty a prachu i několik desítek let, což přináší potenciální riziko.

**Co všechno se v odtahu usazuje a jak to ovlivňuje riziko požáru?**
Hromadí se zde prach, mastnota a vodní pára, která podporuje lepší přilnavost nečistot. Největší riziko představuje právě olej a tuk z vaření, který je vysoce hořlavý. Testy ze zahraničí potvrzují, že vrstva tuku o síle pouhých 0,3 mm je již velmi riziková, a při vrstvě nad 0,5 mm mluvíme o kritickém riziku.

**Pokud se tuk vznítí, jak takový požár v potrubí probíhá?**
Obvykle jde o velice rychlé rozšíření plamenů, které ventilátor dále podporuje prouděním vzduchu. Požární klapka bývá často znečištěná, což zpomaluje její zavření, a v některých případech se nezavře vůbec. Plameny se tak mohou dostat až na střechu budovy. Vysoké teploty mohou dokonce narušit strukturu plechového potrubí, což způsobí jeho propadnutí a případné šíření požáru do dalších částí budovy.
Další nebezpečnou variantou je tzv. žhnutí, kdy se nevytváří výrazné plameny, ale vrstva tuku uvnitř potrubí se zahřeje na několik stovek stupňů a začíná intenzivně doutnat. Tento proces, i když není na první pohled viditelný, může vést k šíření požáru potrubím. Žhnutí je obzvláště záludné, protože probíhá skrytě a může být snadno přehlédnuto, přesto představuje stejnou míru rizika jako klasický požár s plameny. Tepelné narušení konstrukce a rozšíření požáru tak probíhá nepozorovaně, ale s vážnými důsledky pro bezpečnost celé budovy a jejích obyvatel.

**Lze požár včas zastavit?**
Pokud je systém pravidelně čištěn a udržován, pak ano. Požární klapka plní svou funkci a zabraňuje šíření ohně. To ovšem platí pouze pro správně udržované systémy.

**Jak ovlivňuje zanesené potrubí celkové prostředí v kuchyni?**
Správně fungující vzduchotechnika má zásadní vliv na celkový provoz v restauraci. Pokud ventilátor nepracuje dostatečně nebo je potrubí znečištěné, mastné páry pronikají do prostoru kuchyně a usazují se na různých površích. Tyto páry kondenzují na chladných a kovových plochách, často také na kazetových podhledech, což vede k jejich znečištění. Výsledkem je, že veškeré vybavení a povrchy v kuchyni mohou být pokryty mastným filmem, který nejenže zhoršuje čistotu prostředí, ale také komplikuje dýchání personálu a výrazně snižuje komfort při práci.

**Pojďme se teď zaměřit na prevenci. Jak zjistím, jak silná vrstva tuku je v potrubí?**
Na začátku je potřeba revize odbornou firmou. Ta identifikuje kritická místa systému, podívá se do potrubí, změří sílu znečištění a vyhodnotí celkový stav.

**Nestačí tedy nainstalovat protipožární klapky?**
Nestačí. Protipožární klapky vyžadují pravidelnou revizi a údržbu. Tyto klapky se totiž také zanášejí mastnotou, což postupně snižuje jejich funkčnost. Jak jsem už také zmínil, ve chvíli, kdy je v potrubí silnější vrstva nečistot, nemusí být protipožární klapka dostačující.

**Jak často by mělo probíhat čištění potrubí?**
Doporučená frekvence čištění je jednou za 6–12 měsíců, ale hodně záleží na typu provozu. Například restaurace rychlého občerstvení, kde se hodně smaží, musí čistit potrubí i čtvrtletně, zatímco školní kuchyně mohou čistit jednou za dva roky.

**Může provozovatel provést kontrolu sám?**
První kontrolu by měl vždy provést specialista, který zhodnotí stav potrubí a navrhne vhodné kroky. Poté je možné, aby provozovatel prováděl kontroly sám, pokud dodrží správné postupy, například měření tloušťky usazenin. Nicméně je třeba vzít v úvahu, jak tento přístup posoudí pojišťovna nebo majitel budovy, protože na to neexistuje žádná závazná právní norma.

**Co kromě samotného čištění přispívá ke správné funkčnosti potrubí a snižuje riziko požáru?**
Klíčové je pravidelně udržovat tukové filtry v digestořích. Doporučuje se je minimálně jednou týdně umýt, ideálně v myčce na nádobí. Důležité je nikdy je nevyndávat za účelem „zlepšení tahu“, protože by to vedlo k neefektivnímu odsávání a zvýšení rizika hromadění mastnoty v potrubí. Dále je nezbytné, aby systém byl správně nastaven – zejména co se týká rychlosti a objemu odsávaného vzduchu. Pravidelná kontrola a udržování dobrého technického stavu ventilátoru jsou také zásadní.

**Je možné považovat čištění potrubí za druh pojištění? Platím malou částku, abych předešel větším škodám?**
Z finančního hlediska to tak skutečně je. Náklady na čištění potrubí jsou ve srovnání se škodami, které může způsobit požár, řádově nižší. Škody po požáru mohou dosahovat stovek tisíc, nebo i milionů korun. Hlavním důvodem však zůstává ochrana zdraví a života lidí, což je hodnota, kterou nelze vyčíslit penězi.

**Můžete nám přiblížit, jak probíhá samotný proces čištění potrubí?**
Nejdříve se provede důkladná revize a inspekce potrubního systému, aby bylo možné zjistit přístupová místa a celkový stav potrubí. Samotné čištění se obvykle provádí mimo provozní dobu restaurace, aby v kuchyni nebyl přítomen žádný personál. K čištění se používá kombinace mechanických a chemických prostředků, přičemž potrubí se většinou nemusí demontovat.

**Je možné vyčistit každý typ potrubí? Jaké jsou limity?**
Největší překážkou při čištění potrubí bývá jeho přístupnost. Problémy mohou nastat například u pevných sádrokartonových stropů nebo v místech, kde stavební prvky jako elektrické a vodovodní rozvody brání přístupu. Při projektování a stavbě se většinou nepočítá s budoucí údržbou potrubí. Na tento problém narážíme velice často a nejsou výjimkou ani případy, kdy provozovatel chce nebo

musí vyčistit potrubí na pokyn hasičů, a následně se ukáže, že čištění vyžaduje velký stavební zásah nebo náročné horolezecké výkony. Právě proto, že nikdo se na začátku nezamyslel nad tím, že bude nutná pravidelná údržba potrubí. Ve většině případů je čištění otázkou času a financí.

**Jaké technologie používáte při čištění potrubí?**
Pokud je potrubí vodotěsné, ideální metodou je jeho vypláchnutí vodou s čisticím prostředkem, což bohužel v ČR v podstatě nikde nelze použít. Proto používáme speciální čisticí pěny a gely v kombinaci s mechanickým odstraňováním tuku pomocí rotačních kartáčů a ruční práce. V některých případech využíváme i tryskání suchým ledem.

**Je chemie, kterou používáte, bezpečná? Lze čištění provádět bez ní?**
Používané chemické prostředky jsou běžně schválené a srovnatelné s prostředky na čištění grilů a sporáků. Tyto látky účinně narušují tuk a umožňují jeho rozpuštění. Existují také alternativní metody, které chemii nevyužívají, ty ale nejsou univerzálně vhodné pro každou situaci.

**Jak se nakládá s odpadem vzniklým při čištění?**
Odpad z čištění potrubí je považován za nebezpečný a jeho likvidace musí probíhat v souladu s platnou legislativou. Je zásadní, aby firma provádějící čištění měla možnost doložit, že odpad byl správně a bezpečně zlikvidován.

**Je proces čištění hygienický? Jak ovlivňuje kuchyni a její vybavení?**
Před samotným čištěním je důležité zajistit, aby v kuchyni nebyly přítomné žádné potraviny ani nádobí. Veškeré spotřebiče a vybavení musí být pečlivě zakryté, aby nedošlo ke kontaminaci mastnotou nebo chemickými látkami.

**Jak je možné, že v ČR neexistuje žádná legislativa týkající se tohoto požárního rizika?**
Na to je těžké jednoznačně odpovědět. Je to problém, který není příliš vidět. Pozitivní je, že nějaké kroky se v tomto oboru na úrovni Evropské unie podnikají a uvidíme, v jaké formě se k nám do ČR nakonec dostanou. Obecně by tlak na ochranu zdraví a života lidí měl být logickým směrem, kterým se chceme ubírat.

**Co bychom se mohli naučit od zahraničních zemí?**
Mnoho evropských zemí má propracovanou legislativu, která se snaží minimalizovat požární rizika spojená s kuchyňskými vzduchotechnikami. Velká Británie je v tomto ohledu na špici, s jasně stanovenými limity znečištění, metodikami údržby, čištění a pravidelnými kontrolami. Tyto normy vznikly mimo jiné na základě zkušeností z tragických požárů, jako byl například na letišti Heathrow v roce 1997. Podobná opatření najdeme i ve Švédsku, Finsku nebo Německu.

**Která země je v přístupu k legislativě a prevenci vzorem?**
Jednoznačně Velká Británie. Kromě toho, že mají velice dobře definované, co znamená čisté a znečištěné potrubí, tak zavedli i systém školení a certifikací pro techniky, kteří revize nebo samotné čištění provádějí. Každé čištění se navíc zadává do centrálního systému, ve kterém mohou pojišťovny nebo úřady snadno dohledat, kdy a kdo čištění v dané restauraci naposledy provedl.

**Jaký význam má volba typu potrubí pro čistotu a funkci systému? Můžete nám některé typy představit?**
Nejběžněji používaný typ je pozinkovaný plech spojený šrouby, někdy s gumovým nebo silikonovým těsněním, což není ideální pro kuchyně. Nejlépe funguje svařované kovové potrubí, které je snadno čistitelné a údržbově nenáročné. Další možností je polystyrenové ALP potrubí s hliníkovou fólií, které je lehké, ale při čištění komplikovanější, protože je relativně měkké. Flexibilní potrubí, které se často používá k propojení s digestoří, je však zcela nevhodné pro odtah kuchyňských výparů.

**Které typy potrubí jsou z hlediska praktického využití nejvhodnější?**
Nejvhodnější je svařované, vodotěsné a spádované kovové potrubí. Pro pravidelnou údržbu to znamená velice rychlé a efektivní čištění za pomoci tlakové vody s chemií a s odtokovým kanálkem. Většinou se jedná o zlomek ceny za čištění v porovnání s běžně montovaným vzduchotechnickým potrubím.

# Ceník inzerce

## Magazín ČAS

### Technická specifikace

| | |
|---|---|
| Formát: | 160 × 226 mm |
| Papír obálka: | 200–300 g/m² lesklá křída |
| Papír vnitřní strany: | 120–150 g/m² matná křída |
| Vazba: | V2 |
| Frekvence: | 4x ročně |

### Plošná barevná inzerce

Formáty inzerce uvnitř magazínu

| Formát | Rozměr | Cena |
|---|---|---|
| Celá strana | 160 × 226 mm | 18 000 Kč |
| 1/2 strany | 160 × 113 mm | 9 000 Kč |
| 1/4 strany | 80 × 113 mm | 4 500 Kč |

### Barevná zadní obálka magazínu

| Rozměr | Cena |
|---|---|
| 160 × 180 mm | 25 000 Kč |

### Vkládaná inzerce

| Formát | Rozměr | Cena |
|---|---|---|
| Celá strana | 160 × 226 mm | 6 000 Kč |
| 1/2 strany | 160 × 113 mm | 4 000 Kč |

**Ceny inzerce jsou uvedeny bez DPH**

1/1 1/2 1/4

### Slevy při opakovaném uveřejňování reklamy

2 × 15 % 3 × 20 % 4 × 25 %

### Grafické zpracování inzerátu, včetně úpravy barevných předloh

20 % z ceny inzerátu

### Podklady

Hotová inzerce: tiskové PDF, včetně spadů a ořezových značek.
Podklady pro vytvoření inzerce: textové podklady ve formátu DOC, obrazové podklady v tiskové kvalitě (rozlišení na 300 dpi) ve formátech PSD, JPEG, TIF a EPS, loga v křivkách (EPS, AI, PDF).

Sledujte nás na:

# Od 1. ledna 2025 přechází Česká agentura pro standardizaci na novou doménu


Změna se týká webové prezentace – nově jsou webové stránky dostupné na **agenturacas.gov.cz**.

Druhou změnou je úprava e-mailových adres, které mají dle požadavků nově formát **„jmeno.prijmeni@agenturacas.gov.cz“**