**Poznatky z kontrol**

(aktualizace 2023)

Podle § 143 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zákon“), Národní bezpečnostní úřad (NBÚ) kontroluje, jak orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby (dále jen "kontrolované osoby") dodržují právní předpisy v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Podle § 143 odst. 6 zákona lze v případě kontroly, která zasahuje do oblasti působnosti Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), přizvat jeho zástupce.

Kontrolní činnost NBÚ se trvale zaměřuje na orgány státu a držitele osvědčení podnikatele, a to na:

- podnikatele s formou přístupu dle § 20 odst. 1 písm. a) zákona,

- podnikatele s formou přístupu dle § 20 odst. 1 písm. b) zákona,

- podnikatele, kteří učinili Prohlášení podnikatele pro přístup k utajované informaci stupně utajení Vyhrazené.

V části osmé zákona, konkr. v § 148 až 156 je uveden výčet přestupkových jednání kontrolovaných osob, který se týká oblastí ochrany utajovaných informací, tedy obecných povinností, personální bezpečnosti, průmyslové bezpečnosti, fyzické bezpečnosti, administrativní bezpečnosti, registru utajovaných informací poskytovaných v mezinárodním styku, kryptografické ochrany a bezpečnosti informačních systémů.

Kontrolované osoby se při nakládání s utajovanými informacemi mohou dále dopustit i pochybení, která sice nejsou přestupkem dle zákona, která jsou ale porušením ustanovení uvedených v souvisejících předpisech (vše v platném znění). Těmito předpisy jsou:

* Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti;
* Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti;
* Vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací;
* Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků;
* Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací;
* Vyhláška č. 523/2005 Sb., o bezpečnosti informačních systémů a certifikaci stínících komor.

Níže jsou uvedeny jak nejčastější, tak některé konkrétní nedostatky, které byly zjištěny při kontrolní činnosti Úřadu v posledních letech.

**Nedostatky v oblasti OBECNÉ a PERSONÁLNÍ bezpečnosti**

NESPLNĚNÍ ZÁKONNÝCH POVINNOSTÍ VŮČI NÁRODNÍMU BEZPEČNOSTNÍMU ÚŘADU:

* neoznámení zřízení a obsazení pozice bezpečnostního ředitele;
* nezaslání jednoho výtisku poučení u držitele osvědčení pro přístup k utajovaným informacím stupně utajení Důvěrné a vyšší;
* neoznámení ukončení pracovního poměru držitele osvědčení pro přístup k utajovaným informacím stupně utajení Důvěrné a vyšší.

NEDOSTATKY OBECNÉHO CHARAKTERU:

* nezpracování přehledu míst nebo funkcí, na kterých je nezbytné mít přístup k utajovaným informacím;
* nevedení evidence fyzických osob, které mají přístup k utajované informaci;
* nezpracování evidence neoprávněného nakládání s utajovanými informacemi (mít připravenou tabulku);
* umožnění přístupu k utajovaným informacím osobě, která je sice držitelem osvědčení nebo oznámení, ale nebyla poučena;
* absence písemného záznamu o zániku platnosti oznámení dle § 9 odst. 3 písm. b) až d) f), h) nebo i) zákona;
* neškrtnutí jednoho z paragrafů, podle kterého byla osoba poučena, na výtisku Poučení v případě použití obecného formuláře;
* poskytnutí utajované informace osobě, která nesplňovala podmínky pro přístup k utajované informaci příslušného stupně.

*Doporučení pro přístup k UI stupně VYHRAZENÉ*:

- vytvářet písemný záznam o tom, kdy bylo provedeno opakované ověřování splnění podmínek pro vydání oznámení, a to buď po pěti letech na původní oznámení, které spolu s poučením zůstává v platnosti, nebo na samostatný list, aby měl poskytovatel utajované informace jistotu, že v případě oznámení staršího pěti let bylo ověření splnění podmínek pro vydání oznámení skutečně provedeno.

- v případě zániku oznámení je i s poučeními a záznamy o zániku platnosti ukládat po dobu alespoň 3 let, aby bylo možno při případné kontrole doložit, že držitel oznámení v předmětné době splňoval podmínky přístupu k utajované informaci stupně Vyhrazené.

**Nedostatky v oblasti PRŮMYSLOVÉ bezpečnosti**

OBECNÉ:

* nezaslání jednoho výtisku Prohlášení podnikatele;
* neaktualizování bezpečnostní dokumentace;
* nezaslání aktualizované bezpečnostní dokumentace podnikatele na NBÚ;
* u držitelů osvědčení podnikatele neoznámení změn provedených v obchodním rejstříku;
* uložení utajovaných dokumentů u podnikatele i po skončení platnosti jeho osvědčení či prohlášení (dokumenty nutno vrátit původci či dalšímu subjektu dle zákona).

**Nedostatky v oblasti FYZICKÉ bezpečnosti**

OBECNÉ:

* nepřehlednost projektu fyzické bezpečnosti díky množství dodatků a oprav;
* výkresová dokumentace, která je součástí projektu fyzické bezpečnosti, neodpovídá skutečnému stavu rozmístění technických prostředků v zabezpečené oblasti;
* seznam osob s oprávněním vstupu do objektu a zabezpečené oblasti chybí nebo není aktualizován;
* absence tabulky použitých technických prostředků;
* špatně zpracovaná tabulka bodového ohodnocení zabezpečené oblasti v projektu fyzické bezpečnosti;
* bodové hodnocení úschovných objektů v projektu fyzické bezpečnosti neodpovídá jejich typu;
* neuložení kopií certifikátů používaných/instalovaných technických prostředků u projektu fyzické bezpečnosti;
* absence zápisu o posouzení shody u technického prostředku typu (dveře, mříže, úschovný objekt).

KONKRÉTNÍ ZJIŠTĚNÍ:

* instalace vstupních dveří do zabezpečené oblasti byla provedena v rozporu s certifikátem technického prostředku (nutno dodržet směr otevírání);
* cylindrické vložky u dveří ze strany napadení vyčnívaly o více než 3 mm (nutno otočit nebo vyměnit);
* absence certifikovaného kování u uzamykatelného systému zabezpečené oblasti;
* absence zařízení elektrické požární signalizace v zabezpečené oblasti kategorie Tajné;
* nedoložení platných certifikátů některých technických prostředků nebo doložení certifikátu jiného typu;
* chybné nakonfigurování systému elektronické kontroly vstupů;
* nefunkční hlášení systému elektronické kontroly vstupů;
* zobrazení nouzového signálu pouze vizuálně bez zvukového signálu;
* nenapojení systému elektronické kontroly vstupů na stanoviště ostrahy;
* u skartačního stoje nesplnění požadavku na velikost odpadních částic (pak nutno zajistit další zničení metodou spálení, roztavení, drcení nebo rozvláknění a tuto metodu dodatečného zničení popsat v projektu fyzické bezpečnosti).

**Nedostatky v oblasti ADMINISTRATIVNÍ bezpečnosti**

UTAJOVANÝ DOKUMENT (dále též „UD“):

* nepředložení UD ke kontrole (ztráta);
* nezaevidování doručeného UD;
* zpracování UD na necertifikovaném informačním systému;
* neočíslování listů nebo stran a nesešití či pevné nespojení listů UD;
* nesprávné nebo chybějící povinné náležitosti vlastního UD: správně umístěný stupeň utajení, název původce, číslo jednací ve správném formátu, datum vzniku, číslo výtisku, počet listů, počet příloh a počet jejich listů, příp. druh a počet nelistinných příloh (samostatně utajované a neutajované);
* chybná evidence UD (např. tech. výkresů) uložených v deskách – pokud na deskách není nalepen list utajovaného dokumentu (např. průvodní list), desky by neměly obsahovat náležitosti UD (počet listů, počet příloh, číslo výtisku atd.) a mělo by na nich být 1 x označení stupně utajení (analogie jako v případě obálky), jinak by se jednalo o první list UD a celý obsah by musel být označen jako jeho přílohy, případně by desky samy musely tvořit jednu z příloh;
* nezrušení stupně utajení na UD s označením „utajovat do odpojení příloh“, popř. absence záznamu o odpojení příloh o jejich přeevidování;
* nezaevidování / nepřeevidování odpojené utajované přílohy pod nové číslo jednací;
* nevytvoření kontrolního listu u přeevidované přílohy;
* nevyznačení zrušení stupně utajení na UD, absence či neúplný záznam o zrušení stupně utajení;
* neuvedení záznamu o vyhotovení kopie nebo výpisu na UD;
* neprovedení záznamu (písemného souhlasu přímo nadřízené osoby) o vytvoření kopie na předmětném UD stupně utajení Tajné nebo Důvěrné (platí i pro případ, kdy se vyhotovuje kopie neutajované přílohy takového UD);
* neprovedení záznamu (písemného souhlasu přímo nadřízené osoby) o vytvoření výpisu z utajované přílohy (v případě, kdy se vytiskne obsah, byť jediného souboru z CD, které tvořilo přílohu UD);
* neoprávněné vyznačení stupně utajení;
* stanovení nižšího stupně utajení vytvořeného dokumentu, než byl stupeň utajení přílohy;
* nevyznačení stupně utajení na obálce nebo obalu, ve kterých byl vložen UD;
* zrušení stupně utajení bez souhlasu původce;
* neoznámení zrušení stupně utajení všem adresátům UD;
* započtení doručeného rozdělovníku vyhotoveného na samostatném listu do počtu listů UD nebo jeho zaevidování jako příloha, aniž by ho jako přílohu označil původce UD;
* nesprávné přeevidování odpojené přílohy doručeného utajovaného dokumentu (nelze evidovat jako vlastní UD);
* chybné zaevidování vráceného dokumentu (vrácený utajovaný dokument je de facto utajovaným dokumentem doručeným, kdy se původní adresát/příjemce změnil v odesílatele a dokument má nové/jejich č.j.);
* nezaevidování omylem doručeného utajovaného dokumentu.

PŘÍKLADY:

Vytištění souboru z CD:

Utajovaný dokument, který vznikne vytištěním souboru z CD (UD v nelistinné podobě nebo příloha průvodního dopisu), se zaeviduje jako nový utajovaný dokument s tím, že se na něj vyznačí evidenční údaje dle vyhlášky a informace, z jakého CD byl vytištěn. Na přijatý průvodní dokument se zároveň doplní informace o vytištění obsahu CD vč. jeho nového č.j. a další údaje o vyhotovení výpisu.

Vytištění souboru z informačního systému:

V případě, že je utajovaný dokument doručený prostřednictvím IS doprovázen neutajovanou elektronickou zprávou (tělo e-emailu), je třeba jej zaevidovat samostatně s tím, že pokud bude vytištěna i neutajovaná elektronická zpráva (tělo e-mailu), bude v evidenci zapsána nejvýš jako doplňující údaj k evidenčním údajům o počtu listů utajovaného dokumentu. Např.:

- tělo emailu (1 list) s přílohou 1 utajovaného souboru/dokumentu o dvou listech, lze zaevidovat např. jako „2 + 1 EZ“ /elektronická zpráva/, tzn. jako 2 listy utajovaného dokumentu a přiložený vytištěný 1 list neutajovaného těla emailu;

- tělo emailu s přílohou 4 elektronických souborů, které obsahovaly utajovaný dokument o 6 listech, 2 neutajované listiny, každá o 2 listech, a 1 list neutajovaného rozdělovníku, který není původcem označen jako neutajovaná příloha, lze zaevidovat např. jako „6 + 2/4neut. + rozděl. +1EZ“.

Informace o tom, že doručený utajovaný dokument byl vytištěn z IS, se uvede formou záznamu o převodu dokumentu do listinné podoby přímo na vyhotoveném výtisku utajovaného dokumentu. Je třeba dbát na způsob tisku (oboustranný x jednostranný), aby nevznikl rozpor mezi údaji o počtech listů, příloh a jejich listů uvedených původcem a skutečným stavem. Pokud vznikne rozpor, uvede se skutečný počet vytištěných listů.

K informačnímu systému lze zavést další administrativní pomůcku (sešit) s názvem např. „Evidence tisku stupně …“, „Kniha tisku pro stupeň utajení … “ apod., kam lze zaznamenávat vytištění/zničení utajovaných dokumentů jako jsou vadné výtisky, návrhy, podklady aj.

ULOŽENÝ UTAJOVANÝ DOKUMENT

* absence rozdělovníku nebo záznamu;
* uvedení chybných či neúplných údajů v rozdělovníku;
* uvedení chybných či neúplných údajů v záznamu.

POHYB UTAJOVANÉHO DOKUMENTU:

* odeslání UD v nelistinné podobě bez průvodního dopisu;
* nedodržení zákonného postupu při předání UD, tedy např. nedoložení potvrzení o převzetí UD uvnitř organizace (podpisem v manipulační knize);
* absence zápisu v manipulační knize o vytvořeném UD (osoba, která vytváří UD, si jej zapíše do vlastní manipulační knihy, kde si následně nechá potvrdit jeho předání osobě pověřené vedením jednacího protokolu, která zajišťuje jeho odeslání, případně jiné osobě);
* nedoložení potvrzení o převzetí zásilky k přepravě držitelem poštovní licence;
* neuvedení všech údajů na stvrzence o převzetí UD příjemcem;
* neřešení závady doručené zásilky s odesilatelem;
* zapůjčení UD stupně utajení Tajné bez písemného souhlasu odpovědné osoby nebo bezpečnostního ředitele;
* nevrácení vypůjčeného UD k zápůjční knize pro účely fyzické kontroly, která je povinně prováděna v lednu každého roku.

ADMINISTRATIVNÍ POMŮCKY OBECNĚ:

* nesplnění formálních a obsahových požadavků (např. chybějící kolonky, chybné názvy);
* neuvedení v jednacím protokolu osoby pověřené jeho vedením;
* neprovedení nebo nesprávné provedení autentizace;
* nevyznačení stupně utajení na poznámkovém sešitu a neprovedení autentizace;
* chybné provádění oprav záznamů;
* nesprávně prováděné úkony v administrativních pomůckách, které k tomu nejsou určeny (předání v zápůjční knize, aniž by se jednalo o zápůjčku, potvrzení převzetí UD v nesprávné pomůcce);
* nedoložení provedení příslušných úkonů při personálních změnách (vytvoření předávacího protokolu při změně osoby pověřené vedením jednacího protokolu);
* vedení administrativních pomůcek v elektronické podobě, ačkoli nebyly splněny požadavky stanovené pro tento způsob jejich vedení;
* rozdíl mezi údaji o počtu listů a příloh v administrativních pomůckách při předávání jednoho UD;
* pevné nespojení/nesešití souboru UD po uzavření sběrného archu;
* zničení některých UD zapsaných a zaevidovaných v již uzavřeném sběrném archu;
* nevyhotovení kontrolního listu k UD stupně utajení Důvěrné nebo vyššího;
* neuvedení všech osob, které se s obsahem UD seznámily, do kontrolního listu (tedy i osoba, která dokument vytvořila, a osoba, která ho zaevidovala);
* používání jednoho kontrolního listu k více UD současně;
* absence čísel průkazů totožnosti u osob zapsaných v kontrolních listech, které se seznámily s UD a které nebyly zaměstnanci kontrolované osoby;
* neuložení kontrolního listu u dokumentu, který byl odeslán;
* zničení kontrolního listu před stanovenou lhůtou (např. v rámci skartace UD).

EVIDENCE UTAJOVANÝCH DOKUMENTŮ - JEDNACÍ PROTOKOL A SBĚRNÝ ARCH

* zaevidování utajovaného dokumentu cizí moci společně s „národními“ utajovanými dokumenty;
* neúplné nebo nesprávné záznamy v jednacím protokolu (JP) nebo ve sběrném archu (SA):
	+ chybně provedené nebo vůbec neprovedené záznamy o zrušení stupně utajení (nepřeškrtnutí zkratky ve sloupci č. 1 v JP a ve sloupci „Poř. číslo“ v SA);
	+ nezaevidování iniciačního dokumentu v JP (dokument, kterým se zakládá sběrný arch);
	+ absence informace o založení sběrného archu ve sloupci č. 3 JP;
	+ chybné uvedení data ve sloupci č. 4 JP (namísto data uvedeného na UD uvedeno datum doručení);
	+ ve sloupci č. 6 JP chybně uveden souhrnný počet listů všech výtisků;
	+ ve sloupci č. 8 neuvedení dalších osob, kterým byl UD předán, ani odkazu na administrativní pomůcku, ve které je předání zaznamenáno a potvrzeno;
	+ neuzavření či chybné/neúplné uzavření sběrného archu;
	+ neuzavírání záznamů v JP na konci kalendářního roku, popř. neúplný záznam o tomto úkonu.

**Nedostatky v oblasti REGISTRU utajovaných informací**

OSOBY:

* osoba zařazená v registru utajovaných informací cizí moci byla držitelem osvědčení pro nižší stupeň utajení, než byl stupeň utajení registru utajovaných informací cizí moci;
* osoba zařazená v registru utajovaných informací NATO nebyla držitelem platného osvědčení pro cizí moc;
* seznam osob, kterým lze umožnit přístup k utajovaným informacím cizí moci, neobsahoval všechny povinné údaje;
* byl veden toliko jeden souhrnný seznam osob, kterým lze umožnit přístup k utajovaným informacím cizí moci, nikoli oddělené seznamy zvlášť pro EU, NATO a OSCM;
* s utajovaným dokumentem cizí moci se seznámila osoba, které nebyla držitelem oznámení či osvědčení ani osobou, která má zvláštní přístup k utajované informaci;
* s utajovaným dokumentem NATO stupně utajení Důvěrné se seznámila osoba, která nebyla držitelem osvědčení fyzické osoby pro cizí moc;
* s utajovaným dokumentem cizí moci se seznámila osoba, která nebyla uvedena v přístupovém seznamu.

REGISTR/DOKUMENTY:

* evidenční list registru nebyl aktualizován;
* utajované dokumenty cizí moci byly evidovány v „národních“ jednacích protokolech;
* na utajovaných dokumentech cizí moci, nebyl na první straně vyznačen český ekvivalent stupně utajení včetně příslušné zkratky;
* nebyl vyhotoven kontrolní list utajovaného dokumentu cizí moci;
* utajovaný dokument cizí moci byl odeslán jako příloha „národního“ utajovaného dokumentu;
* na překladu utajovaného dokumentu cizí moci byly vyznačeny stupně utajení, ale bez příslušné zkraty (NATO, EU);
* utajované dokumenty cizí moci byly evidovány ve sběrném archu;
* kontrolní listy nebyly po vyřazení utajovaných dokumentů cizí moci uloženy v registru utajovaných informací (byly zničeny spolu s dokumenty);
* skartování utajovaných dokumentů cizí moci se vznikem větších odpadních částic, než stanoví příslušný předpis (viz fyzická bezpečnost).

VNITŘÍ PŘEDPIS (vlastní administrativní směrnice pro nakládání s utajovanými informacemi):

* obsahoval nadbytečné informace (pasáže ze zákona či vyhlášek) nevztahující se ke konkrétnímu uživateli;
* některá ustanovení vnitřního předpisu upravujícího manipulaci s utajovanými dokumenty neodpovídala platnému znění vyhlášky o administrativní bezpečnosti a o registrech utajovaných informací (platí pro oblast administrativní bezpečnosti a pro oblast registru utajovaných informací).

Doporučení na závěr:

V případě jakýchkoli nejasností či nenadálých situací při práci s utajovanými informacemi neváhejte kontaktovat pracovníky NBÚ, určitě Vám poradí jak danou nejasnost či situaci řešit.

Informační linka NBÚ je 257 283 111, odkud budete přepojeni na kompetentního pracovníka;
e-mailové adresy jednotlivých odborů najdete na odkazu [www.nbu.cz/cs/kontakty/](http://www.nbu.cz/cs/kontakty/).