

ODBORNÁ PŘÍPRAVA PRACOVNÍKA KRYPTOGRAPHICKÉ OCHRANY



NÚKIB



Úvodní pokyny a informace

Prosíme, věnujte pozornost úvodním pokynům, které budete potřebovat pro úspěšné absolvování on-line kurzu.

[Zákon č. 412/2005 Sb.](#), o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“) stanovuje v [§ 39 zákona](#) podmínky zvláštní odborné způsobilosti pracovníka kryptografické ochrany (dále jen „zvláštní odborná způsobilost“). Zvláštní odborná způsobilost je předpokladem, že pracovník kryptografické ochrany má znalosti z oblasti kryptografické ochrany a je schopen je uplatňovat v praxi. Tyto znalosti a schopnosti ověřuje Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) zkouškou zvláštní odborné způsobilosti (dále jen „odborná zkouška“).

Přihlášku k odborné zkoušce podává písemně dle § 39 odst. 2 zákona odpovědná osoba nebo jí pověřená osoba orgánu státu, právnické nebo podnikající fyzické osoby u NÚKIB nebo u jím pověřeného orgánu státu.

- **Kdy se budu moci přihlásit?**

*Kurz bude účastníkovi k dispozici od obdržení písemného oznámení do doby konání zkoušky, **min. 5 dnů předem**. Kurz je považován za ukončený vyplněním závěrečného testu.*



Obsah kurzu

Je základem odborné způsobilosti pro pracovníky kryptografické ochrany, kteří budou určeni k výkonu kryptografické ochrany.

Je základním seznámením s kryptografickou ochranou pro osoby, kterým seznamování s kryptografickým materiálem vyplývá z popisu pracovního místa, ale neprovádí samotný výkon kryptografické ochrany dle [§ 42a zákona](#).

Obsah

Úvodní pokyny a informace	2
Právní rámec kryptografické ochrany	4
Kryptografická ochrana	5
Manipulace s kryptografickým materiálem	8

Ukončení kurzu

Úspěšné absolvování kurzu je nutnou podmínkou pro všechny pracovníky kryptografické ochrany, kteří budou dále pokračovat ve vzdělávacím procesu a budou určeni k výkonu kryptografické ochrany dle § 38 zákona.

Test

Test má 10 otázek, odpovídá se formou výběru správné odpovědi ze tří možností a, b, c. Každá otázka má vždy 1 správnou odpověď. Maximální počet bodů je 10 minimální 8 bodů. Vyhodnocení testu proběhne automaticky po vyplnění a odeslání testu. **Test bude k dispozici v den konání zkoušky.**



Právní rámec kryptografické ochrany

Přehled právních dokumentů

Manipulace s kryptografickým materiálem podléhá legislativním předpisům, které najdete přehledně vypsány níže, a po rozkliknutí si je lze zobrazit v plném znění.

Právní a prováděcí předpisy v oblasti manipulace s kryptografickým materiálem

- **[Zákon č. 412/2005 Sb.](#)**, o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- **[Vyhláška č. 447/2024 Sb.](#)**, o zajištění kryptografické ochrany utajovaných informací a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti
- **[Vyhláška č. 431/2024 Sb.](#)**, o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti

Základní pojmy z oblasti kryptografické ochrany

Vychází z **[hlavy VIII](#)** zákona č. 412/2005 Sb.

- **kryptografický materiál**
 - **kryptografický prostředek**
 - **materiál k zajištění jeho funkce**
 - klíčový materiál
 - heslový materiál
 - **kryptografický dokument**
- **kryptografické pracoviště**
- **vedení evidencí**

Všechny výše uvedené pojmy pro kryptografickou ochranu budou popsány v další části tohoto kurzu.



Základní pojmy kryptografické ochrany

Přehled základních pojmů

Kryptografický materiál

Kryptografickým materiálem je:

- kryptografický prostředek,
- materiál k zajištění jeho funkce,
- kryptografický dokument.

Kryptografický prostředek

Je kryptografický materiál. Jedná se o hardwarový nebo softwarový produkt určený ke kryptografické ochraně nebo jejich kombinace.

[*definice na portálu NÚKIB*](#)

Kryptografické prostředky používané pro kryptografickou ochranu utajovaných informací musí být certifikovány Národním úřadem pro kybernetickou a informační bezpečnost.

Materiál k zajištění funkce kryptografického prostředku

Jedná se o klíčový a heslový materiál pro kryptografickou operaci nebo další nezbytný prostředek a materiál pro zajištění funkce a bezpečného provozování kryptografického prostředku.

[*definice na portálu NÚKIB*](#)

Kryptografické pracoviště

Kryptografickým pracovištěm je pracoviště určené k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku, ukládání kryptografického materiálu nebo k distribuci a evidenci kryptografického materiálu nebo k výrobě a testování kryptografických prostředků. Kryptografické pracoviště musí splňovat bezpečnostní standardy a musí být do provozu schváleno odpovědnou osobou nebo bezpečnostním ředitelem.

[*\[§ 37 odst. 3 zákona\]*](#)

Kryptografické pracoviště, které je centrálním distribučním a evidenčním místem

Kryptografické pracoviště určené k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku nebo které je centrálním distribučním a evidenčním místem kryptografického materiálu orgánu státu, právnické osoby nebo podnikající fyzické osoby, musí být před schválením do provozu odpovědnou osobou nebo bezpečnostním ředitelem certifikováno Národním úřadem pro kybernetickou a informační bezpečnost.

[*\[§ 37 odst. 4 zákona\]*](#)



Orgán státu a výkon kryptografické ochrany

Orgán státu, právnická osoba a podnikající fyzická osoba, které vykonávají kryptografickou ochranu, musí vést evidence kryptografického materiálu, pracovníků kryptografické ochrany, provozní obsluhy kryptografických prostředků a kurýrů kryptografického materiálu.

[\[§ 37 odst. 5 zákona\]](#)

Pracovník kryptografické ochrany

Náležitosti, které musí splňovat

Každý pracovník kryptografické ochrany musí splňovat následující podmínky:

- **Držitel platného osvědčení fyzické osoby**

Vydává Národní bezpečnostní úřad.

- **Držitel osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany**

Ověřuje se odbornou zkouškou u Národního úřadu pro kybernetickou a informační bezpečnost nebo pověřeného orgánu státu na základě přihlášky ke zkoušce.

[\[§ 39 zákona\]](#)

- **K výkonu kryptografické ochrany musí být pověřen odpovědnou osobou nebo jí pověřenou osobou**

Odpovědnou osobou je viz [\[§ 2 písm. e\) zákona\]](#)

Administrativní pomůcky kryptografické ochrany

Okruh představuje základní administrativní pomůcky kryptografické ochrany

K čemu slouží a jak se používají

Administrativní pomůcky kryptografické ochrany vycházejí z [§ 17 vyhlášky č. 447/2024 Sb.](#), a slouží k evidování, předávání, přebírání kryptografického materiálu a pro evidování pracovníků kryptografické ochrany, pracovníků provozní obsluhy kryptografického prostředku a kurýrů kryptografického materiálu.

Základními administrativními pomůckami jsou:

- **evidenční karta a rejstřík evidenčních karet;**
- **evidenční kniha;**
- **jednací protokol a pomocný jednací protokol;**
- **manipulační kniha, doručovací kniha, zápůjční kniha.**



Utajovaná administrativní pomůcka musí být na vhodném místě označena **stupněm utajení** a slovem **KRYPTO**.

Neutajovaná administrativní pomůcka musí být na vhodném místě označena slovy **KRYPTOGRAFICKÁ OCHRANA**.

Se souhlasem Národního úřadu pro kybernetickou a informační bezpečnost je možné používat i další administrativní pomůcky.

Kryptografický dokument a jeho náležitosti

Náležitosti kryptografického dokumentu

Vzor úpravy kryptografického dokumentu je uveden v [příloze č. 3 \(přední strana\)](#) a v [příloze č. 4 \(rozdělovník a záznam pro uložení\)](#) dle [vyhlášky č. 447/2024 Sb.](#)

Kryptografický dokument v listinné podobě

- V horní a dolní části na každé straně je vedle stupně utajení slovo **KRYPTO**.
- Zkratkou „**K**“ v čísle jednacím např. **V15/2006/K**.
- Více informací viz. [§13](#) a [§14](#) [vyhlášky č. 447/2024 Sb.](#)

Kryptografický dokument v nelistinné podobě:

- Na popisném štítku nebo přímo na dokumentu ([příloha k č. j. V15/2006/K](#)).
- Vždy se odesílá jako příloha kryptografického dokumentu v listinné podobě.
- Více informací viz. [§15](#) [vyhlášky č. 447/2024 Sb.](#)



! KRYPTOGRAFICKÝ DOKUMENT NEMŮŽE BÝT NEUTAJOVÁN!



Jednací protokol

Kryptografické dokumenty musí být evidovány v samostatném jednacím protokolu. Všechny stupně utajení se mohou evidovat v jednom jednacím protokolu. Administrativní pomůcky kryptografické ochrany lze vést v elektronické podobě na základě schválení Národního úřadu pro kybernetickou a informační bezpečnost.

Poznámka. Při vedení administrativních pomůcek v elektronické podobě je problém dodržet zásadu „**předávání kryptografického materiálu proti podpisu**“.

Manipulace s kryptografickým materiálem

Opis, kopie, překlad, výpis

Pokud provádíme z kryptografického dokumentu opis, kopii, překlad nebo výpis je třeba dodržet následující podmínky:

- **Vyhrazené krypto** - vyžaduje písemný souhlas vedoucího zaměstnance
- **Důvěrné krypto** - vyžaduje písemný souhlas vedoucího zaměstnance
- **Tajné krypto** - vyžaduje písemný souhlas původce dokumentu
- **Přísně tajné krypto** - vyžaduje písemný souhlas původce dokumentu



[§ 23 vyhlášky č. 447/2024 Sb.]

Zapůjčení uloženého kryptografického dokumentu

- **U orgánu státu** – je možné pouze pracovníkovi kryptografické ochrany.
- **Mimo orgán státu** – je opět možné jen pracovníkovi kryptografické ochrany se souhlasem odpovědné osoby.
- **Je nutné učinit záznam v zápůjční knize**



[§ 33 vyhlášky č. 447/2024 Sb.]

Předávání

- **Předává se** oproti podpisu v administrativních pomůckách.



[§ 24 vyhlášky č. 447/2024 Sb.]

Ukládání

- **Ukládá se odděleně** od ostatních utajovaných dokumentů do certifikovaných úschovných objektů u pověřené osoby.



[§ 32 vyhlášky č. 447/2024 Sb.]



Přenášení kryptografického materiálu

Jedná se o dopravení kryptografického materiálu mimo objekt orgánu státu, právnické nebo podnikající fyzické osoby, které provádí pracovník kryptografické ochrany. **Při přenášení nedochází k předání kryptografického materiálu.**

- Kryptografický materiál musí být uložen v zalepené obálce nebo uzavřeném obalu.
 - **Vyhrazené Krypto** – se souhlasem vedoucího zaměstnance.
 - **Důvěrné Krypto** – se souhlasem vedoucího zaměstnance.
 - **Tajné Krypto** – s písemným souhlasem vedoucího zaměstnance
 - **Přísně tajné Krypto** – s písemným souhlasem odpovědné osoby.



[§30 vyhlášky č. 447/2024 Sb.]

- Při přenášení kryptografického materiálu stupně "**Důvěrné**", "**Tajné**" a "**Přísně tajné**" je nutný doprovod nejméně jedné osoby, která je k činnosti pověřena odpovědnou osobou nebo jí pověřenou osobou a byla náležitě poučena pracovníkem kryptografické ochrany.

Přeprava a vývoz

Kryptografický materiál je přepravován k adresátovi kurýrem kryptografického materiálu.

- **Vyhrazené Krypto** – přepravuje kurýr kryptografického materiálu.
- **Důvěrné, Tajné a Přísně tajné Krypto** – převáží kurýr kryptografického materiálu v doprovodu nejméně jedné osoby, která je pověřena odpovědnou osobou nebo jí pověřenou osobou a byla poučena pracovníkem kryptografické ochrany.
- **Kryptografická zásilka** – je kryptografický materiál, který je vybavený k přepravě, a je vyloučena z veřejné dopravy vyjma letecké a lodní.



[§ 28, § 29 vyhlášky č. 447/2024

- Pro přepravu kryptografické zásilky, vyjma kryptografického dokumentu, je nezbytné vyhotovit **průvodní list kryptografické zásilky**.



[příloha č.6 vyhlášky č. 447/2024 Sb.]

- Certifikovaný kryptografický prostředek lze vyvézt mimo území ČR pouze na základě povolení od Národního úřadu pro kybernetickou a informační bezpečnost. Za vývoz se nepovažuje použití takového prostředku orgánem státu.



[§ 42 odst. 2 - 4 zákona č. 412/2005 Sb.]



Odesílání a balení kryptografického materiálu

Přepravu provádí kurýr kryptografického materiálu v samostatné přenosné schránce.

- **Materiál k zajištění funkce kryptografického prostředku** - balí se do 2 obalů, kdy vnitřní obsahuje veškeré informace – odesílatele, číslo zásilky, stupeň utajení, označení slovem **KRYPTO**, adresáta a nápis "**OTEVŘE POUZE PROVĚŘENÝ PRACOVNÍK KRYPTOGRAFICKÉ OCHRANY**". Vnější obalem je přenosná schránka.
- **Kryptografický prostředek** - 1 pevný přepravní obal, evidenční označení a nápis "**OTEVŘE POUZE PROVĚŘENÝ PRACOVNÍK KRYPTOGRAFICKÉ OCHRANY**".
- **Kryptografický dokument** - je balen do 2 obálek, kdy vnitřní obálka obsahuje veškeré informace – odesílatele, číslo zásilky, stupeň utajení, označení slovem **KRYPTO**, adresáta a nápis "**OTEVŘE POUZE PROVĚŘENÝ PRACOVNÍK KRYPTOGRAFICKÉ OCHRANY**". Vnější obálkou je přenosná schránka.



[§ 25 vyhlášky č. 447/2024 Sb.]

Označení přenosné schránky

Na přenosné schránce je uveden následující nápis:

**!!!V PŘÍPADĚ NÁLEZU NEOTEVÍREJTE A PŘEDEJTE NEPRODLENĚ POLICII ČESKÉ REPUBLIKY
NEBO NÁRODNÍMU ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST!!!**



Kurýr kryptografického materiálu

- Musí být držitelem platného osvědčení fyzické osoby min. pro stupeň utajení přepravovaného kryptografického materiálu.
- Je k přepravě zaškolen – vlastní písemné potvrzení o odborném zaškolení kurýra kryptografické ochrany.
- Je pracovník, který je pověřen k přepravě odpovědnou osobou nebo jí pověřenou osobou.
- Nemusí být pracovníkem kryptografické ochrany.



[§ 42 odst. 1 zákona č. 412/2005 Sb.]

Příjem kryptografické zásilky

Zásilku přijímá pověřený pracovník po předchozí dohodě.

- V případě poškození zásilky je nutné vyhotovit záznam o poškození kryptografické zásilky a neprodleně o tom informovat odesílatele.
- Příjem zásilky je nutné potvrdit a odeslat odesílateli potvrzený výtisk průvodního listu kryptografické zásilky.
- Elektronický přenos kryptografického dokumentu je možné uskutečnit v informačním systému, který je certifikován Národním úřadem pro kybernetickou a informační bezpečnost a je pro takový přenos určen.



[§ 28 vyhlášky č. 447/2024 Sb.]

Kompromitace kryptografického materiálu

Je takové nakládání s kryptografickým materiálem, které způsobilo nebo by mohlo způsobit porušení ochrany utajované informace.

Kompromitace kryptografického materiálu musí být neprodleně oznámena Národnímu úřadu pro kybernetickou a informační bezpečnost.



[§ 43 zákona č. 412/2005 Sb.]



Licence, autorství, kontakt

Obsahovým garantem je národní distribuční středisko (NDS) NÚKIB.

Obsah je publikován s licencí CC:

