POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra správního práva a správní vědy

Ochrana utajovaných informací

Diplomová práce

Protection of classified information

Master thesis

VEDOUCÍ PRÁCE
JUDr. Lenka Scheu, Ph.D.

AUTOR PRÁCE
Bc. Josef Fanta

PRAHA
2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

Ve Vlašimi, dne 1. 3. 2023

Bc. Josef Fanta

ANOTACE

Práce se zabývá ochranou utajovaných informací, přičemž hlavní pozornost je věnována zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění. Po historickém přehledu vývoje právních úprav na území České republiky a stručné charakteristice zákona, jsou představeny základní pojmy týkající se problematiky utajovaných informací. Stěžejní část je věnovaná druhům zajištění ochrany utajovaných informací a následné komparaci s připravovanou novelou zákona a se zákonem o ochraně utajovaných skutečností Slovenské republiky. V závěru práce se autor zabývá případovou studií.

KLÍČOVÁ SLOVA

Informace * utajovaná informace * ochrana * bezpečnost * stupeň utajení * osvědčení fyzické osoby * zájem * druhy zajištění ochrany

ANNOTATION

The thesis deals with the protection of classified information, with focus on Act No. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended. After a historical overview of the development of legal regulations in the Czech Republic and a brief description of the law, the basic concepts related to the issue of classified information are presented. The core part is dedicated to the types of ensuring the protection of classified information and the subsequent comparison with the forthcoming amendment to the Act and the Act on the Protection of Classified Information of the Slovak Republic. The author concludes the thesis with a case study.

KEYWORDS

Information * classified information * protection * safety * degree of secrecy * certificate of natural person * interest * types of protection provision

Poděkování

Především děkuji vedoucí práce JUDr. Lence Scheu, Ph.D. za vedení této práce, její cenné rady a připomínky.

Děkuji své rodině a přátelům, zvláště děkuji mé milované ženě Adélce za její velkou podporu a obětavost během celého mého studia, i mým dětem, pro které stojí za to se překonávat.

Ad Maiorem Dei Gloriam.

Seznam zkratek

EU – Evropská unie

OSN – Organizace spojených národů

NBÚ – Národní bezpečnostní úřad

T – Tajné

D – Důvěrné

PT – Přísně tajné

V – Vyhrazené

OFO – Osvědčení fyzické osoby

ČR – Česká republika

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

BOZP – Bezpečnost a ochrana zdraví při práci

KO – Kryptografická ochrana

IT – Informační technologie

NATO – Severoatlantická aliance

EU – Evropská Unie

OBSAH

1 Úvod 8

2 Historický vývoj ochrany utajovaných informací 9

2.1 Rakousko-Uhersko 10

2.2 Období samostatné republiky do roku 1948 11

2.3 Období mezi lety 1948 –1971 12

2.4 Období mezi lety 1971 – 1998 16

2.5 Období mezi lety 1998 – 2005 19

3 Současná právní úprava ochrany utajovaných informací 22

3.1 Prameny právní úpravy 23

4 Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti 24

4.1 Utajovaná informace 24

4.2 Druhy zajištění ochrany utajovaných informací 27

4.3 Personální bezpečnost 28

4.3.1 Přístup fyzické osoby k utajované informaci 28

4.3.2 Prokazování oprávnění k přístupu k utajované informaci 32

4.3.3 Zvláštní přístup k utajované informaci 32

4.4 Průmyslová bezpečnost 33

4.4.1 Prohlášení podnikatele 33

4.4.2 Podmínky pro vydání osvědčení podnikatele 34

4.4.3 Prokazování splnění podmínek 35

4.5 Administrativní bezpečnost 35

4.5.1 Tvorba 36

4.5.2 Evidence 37

4.5.3 Přeprava a přenášení 37

4.5.4 Zánik 38

4.6 Fyzická bezpečnost 38

4.6.1 Ostraha 40

4.6.2 Režimová opatření 40

4.6.3 Technické prostředky 41

4.6.4 Projekt fyzické bezpečnosti 41
4.7 Bezpečnost informačních nebo komunikačních systémů ... 42
4.7.1 Certifikace 44
4.8 Kryptografická ochrana 46
4.8.1 Manipulace s kryptografickým materiálem 47
4.8.2 Přeprava a přenášení 48
4.8.3 Kompromitace 49
5 Komparace 50
5.1 Plánovaná novela zákona 50
5.2 Slovenská republika 51
6 Případová studie 54
6.1 Personální bezpečnost 54
6.1.1 Zaměstnanci 54
6.1.2 Osvědčení fyzické osoby 56
6.2 Průmyslová bezpečnost 58
6.2.1 Utajené objekty 58
6.2.2 Spolupráce veřejné správy a IT firem 59
6.3 Administrativní bezpečnost 60
6.3.1 Označování utajovaných informací a materiálu 60
6.3.2 Přeprava utajovaných informací 61
6.4 Fyzická bezpečnost 62
6.4.1 Ostraha 62
6.4.2 Režimová opatření 63
6.4.3 Technické prostředky 63
6.5 Bezpečnost informačních nebo komunikačních systémů ... 64
6.5.1 Výroba informačních systémů 64
6.5.2 Práce na informačním systému 65
6.6 Kryptografická ochrana 66
6.6.1 Kompromitace kryptografického materiálu 66
7 Závěr 68
8 Seznam použité literatury 71

1 ÚVOD

Ochrana osobních a citlivých údajů je nezbytná nejen pro jednotlivce, ale i pro celé společnosti a národy, s ochranou informací, a zvláště těch citlivých, totiž úzce souvisí jejich bezpečnost.

Specifickou oblastí ochrany informací je pak ochrana utajovaných informací. Vzhledem k jejich významu a rizikům spojených s jejich únikem, je zpracovávání a manipulace s nimi poměrně náročnou disciplínou. Aby byla zajištěna odpovídající a účinná ochrana těchto informací, je nezbytné přijmout a dodržovat celou řadu opatření a pravidel. Základním právním předpisem, věnujícím se této problematice, je zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Díky absolvování bakalářského studijního programu na Policejní akademii České republiky v Praze jsem měl možnost profesního posunu na mém ústředním správním úřadě, kde jsem začal usilovat o nabídku pracovní pozice v oddělení vládního utajeného spojení. Vzhledem k povaze služebního poměru a časové náročnosti výběrového řízení a následné délky bezpečnostního řízení, které bylo potřeba absolvovat pro výkon mé služby, nabízelo se jako vhodné téma diplomové práce zpracování zákona o ochraně utajovaných informací. Zákona, který byl pro mě zcela nový, stejně jako výkon mé práce.

Z povahy státní služby jsem povinen v oboru mé státní služby vykonat i úřednickou zkoušku (ochrana utajovaných informací), pojal jsem tedy diplomovou práci jako zodpovědnou a aktivní přípravu na výkon služby a vykonání státní úřednické zkoušky. Proto je autorem diplomové práce stanoven cíl seznámení se se zákonem a skutečnost, že jsem chtěl zjistit bližší informace o současné právní úpravě zákona o ochraně utajovaných informací a případně je využít k profesnímu růstu v resortu Ministerstva vnitra.

První část práce je věnovaná historii, postupnému vývoji legislativní úpravy až do současnosti k zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Čtenář je seznámen s aplikovanými právními předpisy a strukturou zákona. Ve stěžejní části se autor zaobírá šesti druhy zajištění ochrany utajovaných informací a snaží se je čtenáři ozřejmit. Průběh autorových prvotních školení a seznamování se s praxí na novém působišti a obsáhlé agendě se autor práce snažil zhmotnit v případové studii v závěru diplomové práce.

2 HISTORICKÝ VÝVOJ OCHRANY UTAJOVANÝCH INFORMACÍ

Potřeba výměny a sdělování informací, jazyková komunikace patří k podstatě člověka. V průběhu historie lidé poznali, že tak jako je dobré si vzájemně rozumět (např. s lidmi hovořícími cizím jazykem) a díky rozluštění jiných jazyků a znaků (např. hieroglyfy) se otvírá cesta k porozumění a pochopení jednotlivců či celých národů, může být stejně tak užitečné, když obsahu sdělení nebude třetí osoba rozumět a do obsahu komunikace nebude moci nikdo další nahlédnout.

Každý stát v zájmu své obrany a bezpečnosti dbá o to, aby se věci, které je potřeba utajit, ať už na úseku vojenském, politickém, hospodářském nebo vědecko-technickém, nedostali do nepovolených rukou.[1]

Mnoho různých metod k utajení psaného textu je známo již z dob antiky. Často se jednalo o důmyslné skrývání zpráv (již Cicero v prvním století před naším letopočtem popisuje příběh Řeka Démarata, který svou tajnou zprávou zachránil Řeky před perskou invazí) nebo o různé posuvy abecedy či nahrazení textu.[2] Příkladem může být i šifra Skytalé (Sparťané). Římané používali prokazatelně vojenskou tajnou komunikaci již na začátku našeho letopočtu[3] (Caesarova šifra). Zprávy byly po sepsání srolovány a zapečetěny a pro distribuci byl používán speciální otrok (tzv. γραμματοφόρος, resp. tabellarius), v právních pramenech římského práva je okrajově upravena ochrana soukromých dokumentů.[4] Z moderních dějin nelze nezmínit ENIGMU (jeden z nejslavnějších šifrovacích přístrojů používaný za druhé světové války).[2]

Dříve byly samozřejmě psané zprávy (posílání písemných zpráv, informací) výsadou úzké skupiny osob vzdělaných. A potřeba tajit informace, šifrování a dešifrování tajných zpráv, měly význam zvláště v politice a vojenství a vojenské strategii.

---

[1] BÁTOVSKÝ, Ján. *Ochrana utajovaných skutočností*. Bratislava: Obzor, 1973.
[2] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. Praha: Dokořán, 1.vyd. 2003. Aliter: Dokořán. ISBN 80-865-6918-7.
[3] ZELENKA, Josef. *Ochrana dat: kryptologie*. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4.
[4] SKŘEJPEK, Michal. *Římské soukromé právo: systém a instituce*. 2. upravené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-566-1.

S rostoucí mírou vzdělanosti společnosti, s rostoucí rychlostí dopravy a komunikace a rychlosti, s jakou se zprávy mohou šířit, se způsoby utajování informací stávají neustále složitějšími a potřeba zabezpečit informace neustále roste.

Pro lepší orientaci v problematice autor práce provedl rešerši právních dokumentů, týkající se ochrany utajovaných informací na našem území od druhé poloviny 19. století.

2.1 Rakousko-Uhersko

Významnou právní úpravou vztahující se k ochraně tajných informací v době Rakouska-Uherska byl **Vojenský trestní zákon o zločinech a přečinech z roku 1855** upravující případy porušení služebních předpisů v rámci armády.

Zákon zmiňuje např. tyto případy porušení služebních předpisů: voják či civilní osoba sdělí informace o vojenských informacích, usneseních, instrukcích, rozkazech, disposicích, signálech, bitevních plánech a popisech rozmístění jednotek apod. nepovolané osobě. Dále neopatrné nakládání s nimi, popř. jejich ztráta stejně jako okamžité neoznámení ztráty. Jako vyzrazení chráněných a utajovaných informací je zde chápáno i pokud osoba, která zná příhlas, odhlas nebo zvolání, vyzradí tuto informaci komukoliv, kdo by jí neměl znát. V tomto zákoně lze najít též ochranu hesla či tajného rozkazu při jeho vydání.[5]

Ve **vojenském trestním zákoně z roku 1912** (zákon č. 131/1912 ř. z. o vojenském trestním řádu) je uvedena zmínka týkající se služebního (úředního) tajemství. Dle tohoto zákona obvinění nesmí být dotazování na skutečnosti podléhající služebnímu či úřednímu tajemství, vyjma případu, že kdy byli této povinnosti zproštěni.[6]

---

[5] Zákon č. 19/1855 ř.z. Vojenský trestní zákon o zločinech a přečinech. In: *epravo.cz* [online] a.s. 1999-2023, ISSN 1213-189X. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=342&Section=1&IdPara=1&ParaC=2 [cit. 2023-01-30].

[6] Zákon č. 131/1912 ř.z. o vojenském trestním řádu v úpravě provedené pozdějšími zákony, naposledy zákonem č. 226/1947 Sb., jak byla úprava vyhlášena vyhláškou ministra národní obrany č. 151/1948 Sb. In: *epravo.cz* [online] a.s. 1999-2023, ISSN 1213-189X. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=719&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-03].

O **úřední mlčenlivosti** se hovoří také v tzv. **služební pragmatice** z roku 1914, v zákoně, který upravoval službu státních úředníků, státních sluhů i služební poměr příslušníků tehdejších veřejných ozbrojených sborů.[7,8]

Je zřejmé, že již v době Rakousko-Uherska byla ochrana státních a vojenských tajemství na poměrně vysoké úrovni.

2.2 Období samostatné republiky do roku 1948

Po vzniku samostatné republiky byl s ohledem na ochranu státního zřízení a mezinárodní vztahy v roce 1923 přijat zákon na ochranu republiky č. 50/1923 Sb. Tento zákon se věnuje postihům aktivit, které ohrožují republiku a její bezpečnost např. vojenská zrada, atentát a ohrožení právě tzv. státního tajemství. Zradou státního tajemství se zde rozumí vědomé či nevědomé vyzrazení, vyzvídání skutečností, opatření či věcí, které vláda tají před cizí mocností v důležitém zájmu republiky. [9,10]

O jaké konkrétní skutečnosti, opatření nebo předměty se jedná, ovšem stanoveno nebylo, nebyla také stanovena kritéria pro jejich klasifikaci.

Ministerstvo národní obrany později stanovilo podniky důležité pro obranu státu (**Nařízení vlády č. 197/1936 Sb., o podnicích důležitých pro obranu státu**), pro která platila speciální bezpečnostní pravidla, včetně povinnosti

---

[7] Zákon, daný dne 25. ledna 1914, o služebním poměru státních úředníků a státních sluhů (služební pragmatika). In: *15/1914 ř.z.*. Vídeň 1914, ročník 1914, 8/1914, číslo 15. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=735&Section=1&IdPara=1&ParaC=2 [cit. 2023-01-30].

[8] § 23 služební pragmatiky. *„Úředník o všech záležitostech, o kterých se dověděl za výkonu své služby nebo vzhledem ke svému úřednímu postavení, které vyžadují v zájmu státu nebo stran nebo jinak ze služebních ohledů zachovávání mlčelivosti nebo které mu výslovně byly označeny za důvěrné, zachovávati nejpřísnější mlčelivost naproti každému, jemuž není zavázán o takových záležitostech učiniti úřední sdělení.“*

[9] Zákon č. 50/1923 Sb., na ochranu republiky. In [Systém ASPI]. Wolters Kluwer. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/3259/1/2 [cit. 2023-02-02].

[10] § 5 zákona č. 50/1923 Sb., *„Zrada státního tajemství. Kdo vyzradí přímo nebo nepřímo cizí moci skutečnost, opatření nebo předmět, jež vláda tají v důležitém zájmu republiky nebo jež v takovém zájmu mají zůstati utajeny před cizí mocí, kdo vyzvídá takovou skutečnost, opatření nebo předmět, aby je vyzradil přímo nebo nepřímo cizí moci, trestá se za zločin žalářem od šesti měsíců do pěti let a spáchal-li čin v úmyslu, aby poškodil republiku, těžkým žalářem od pěti do deseti let.“*

zachovávat tajné informace v zájmu obrany státu (zákon č. 131/1936 Sb. o obraně státu).[11]

Dále byl v roce 1924 přijat též **zákon č. 178/1924 Sb. o úplatkářství a proti porušování úředního tajemství**, který se zabýval případy vyzrazení obsahu tajných či důvěrných spisů a jednání soudů či úředních komisí. [12]

Je možné též zmínit např. Dekret presidenta republiky č. 63/1945 Sb. o Hospodářské radě, který ukládá všem zaměstnancům Hospodářské rady povinnost zachovávat přísné tajemství o všech věcech, o kterých se dověděli při své činnosti.[13]

2.3 Období mezi lety 1948 –1971

Zmiňovaný zákon na ochranu republiky byl zrušen v roce 1948 a nahrazen **zákonem č. 231/1948 Sb., na ochranu lidově - demokratické republiky**. Tento zákon přejal pojem **státní tajemství**:

„Státním tajemstvím se rozumí skutečnost, opatření nebo předmět, jež vláda tají v důležitém zájmu republiky, zejména v zájmu politickém, vojenském nebo hospodářském, nebo jež v takovém zájmu mají zůstati utajeny před cizí mocí nebo před cizími činiteli."[14]

Přísaha zachovávat **úřední tajemství** pak byla dle zákona o přísaze soudců povinná pro soudce a soudcovské čekatele při nástupu do služby dle zákona č. 270/1948 Sb. o přísaze soudců.[15]

---

[11] Vládní nařízení č. 197/1936 Sb., o podnicích důležitých pro obranu státu. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/6617/1/2 [cit. 2023-02-02].

[12] Zákon č. 178/1924 Sb., o úplatkářství a proti porušování úředního tajemství. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/3659/1/2/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi [cit. 2023-02-02].

[13] Dekret č. 63/1945 Sb., presidenta republiky o Hospodářské radě. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1945-63 [cit. 2023-02-02].

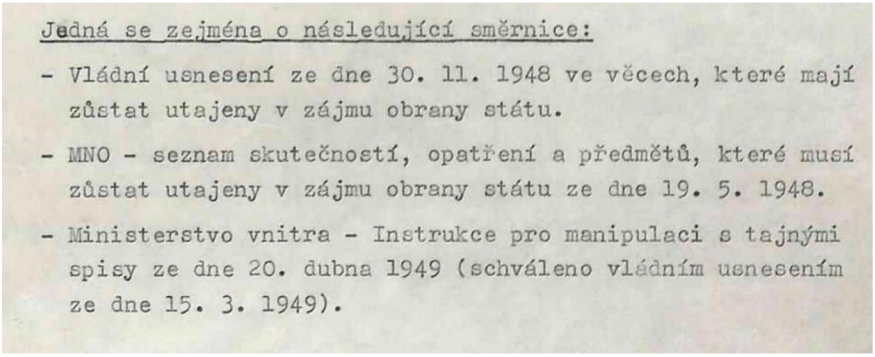
[14] Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/17932/158/2/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky [cit. 2023-02-02].

[15] Zákon č. 270/1948 Sb. Zákon o přísaze soudců In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online]. z: https://www.zakonyprolidi.cz/cs/1948-270 [cit. 2023-02-02].

Příslušníci Sboru národní bezpečnosti skládali přísahu dle Nařízení ministerstva vnitra č. 171/1949 Sb., že budou mimo jiné přísně zachovávat a střežit služební a státní tajemství:

"Já, občan lidově demokratické republiky Československé, přísahám, že budu vždy čestným, statečným, ukázněným a bdělým příslušníkem Sboru národní bezpečnosti, budu přísně zachovávat a střežit služební a státní tajemství a bezpodmínečně plnit uložené mi povinnosti a rozkazy svých velitelů a nadřízených (…)". [16]

Problematika utajovaných informací byla pak podrobněji řešena na nižší (a neveřejné) úrovni v podobě různých směrnic. Například dle obrázku č. 1 z vyšetřovacího spisu s Miladou Horákovou se můžeme dozvědět například o Vládním usnesení ze dne 30.11.1948, o seznamu skutečností či o Instrukcích pro manipulaci.


Jedná se zejména o následující směrnice:

- Vládní usnesení ze dne 30. 11. 1948 ve věcech, které mají zůstat utajeny v zájmu obrany státu.
- MNO - seznam skutečností, opatření a předmětů, které musí zůstat utajeny v zájmu obrany státu ze dne 19. 5. 1948.
- Ministerstvo vnitra - Instrukce pro manipulaci s tajnými spisy ze dne 20. dubna 1949 (schváleno vládním usnesením ze dne 15. 3. 1949).

Obrázek č.1 - Ukázka směrnic z vyšetřovacího spisu s Miladou Horákovou[17]

V **trestním zákoně** z roku 1950 je pak rozlišeno tzv. **státní tajemství, hospodářské tajemství a služební tajemství**. Pod státním tajemstvím se rozumí vše, co *„v důležitém zájmu republiky, zejména v zájmu politickém, vojenském nebo hospodářském, má zůstat utajeno před nepovolanými osobami.“* [18]

Hospodářské tajemství je pak *„vše, co je příznačné nebo významné pro hospodářské podnikání a v obecném zájmu má zůstat utajeno před nepovolanými*

[16] Nařízení č. 171/1949 Sb. Nařízení ministra vnitra, jímž se vydávají předpisy o služební přísaze, o zkušební době, o propuštění v této době a o povolení k uzavírání sňatků příslušníků Sboru národní bezpečnosti In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online]. z: https://www.zakonyprolidi.cz/cs/1949-171 [cit. 2023-02-02].
[17] Svazek vyšetřování a.č. V-6301 MV "Akce STŘED", znalecký posudek a zpráva. Dostupné [online] z: https://www.svazky.cz/archivy/ABS-Praha/FSV/V-6301_MV/V-06301_MV_109.pdf [cit. 2023-02-03].
[18] Zákon č. 86/1950 Sb., trestní zákon. In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1950-86 [cit. 2023-02-02].

osobami.“ A nakonec *„služebním tajemstvím se rozumí důležitá skutečnost, která souvisí s činností národního výboru, soudu nebo jiného úřadu, veřejného orgánu nebo podniku anebo lidového družstva a v obecném zájmu má zůstat utajena před nepovolanými osobami.“* [19]

V zákoně jsou uváděny v souvislosti s trestnými činy proti bezpečnosti republiky – vyzvědačství, ohrožení státního tajemství a ohrožení hospodářského a služebního tajemství. Stejně tak je trestné neohlášení těchto trestných činů.[19]

V roce 1950 bylo zřízeno Ministerstvo národní bezpečnosti[20] a o rok později Ministerstvo státní kontroly[21], jehož orgány měly pravomoc v rámci kontrol zajišťovat veškeré informace i ty podléhající povinnosti mlčenlivosti.[22]

Dále např. Ministerstvo národní bezpečnosti vydalo v roce 1953 vyhlášku č. 115/1953 úředního listu, o skutečnostech tvořících státní tajemství, která stanovovala okruh zájmů státního tajemství resortů vojenského, hospodářského, politického nebo jiného důležitého zájmu.[23]

V tomtéž roce byl ustanoven cenzurní úřad Hlavní správa tiskového dohledu (později nahrazena Ústřední publikační správou)[24], která měla mimo jiné za úkol zajišťovat, aby nebyly zveřejňovány a šířeny údaje a skutečnosti, které

---

[19] Zákon č. 86/1950 Sb., trestní zákon. In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1950-86 [cit. 2023-02-02].

[20] Nařízení vlády č. 48/1950 Sb., vládní nařízení, kterým se zřizuje ministerstvo národní bezpečnosti. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1950-48 [cit. 2023-02-02].

[21] Nařízení vlády č. 73/1951 Sb., vládní nařízení, kterým se zřizuje ministerstvo státní kontroly. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1951-73 [cit. 2023-02-02].

[22] NV č.73/1951 Sb.,: „Osoby, které jsou orgány ministerstva státní kontroly při provádění kontroly vyzvány k předložení plánů, listin, výkazů a jiných dokladů, jakož i k podání zpráv, sdělení a vysvětlení o věcech, spadajících do pravomoci ministerstva státní kontroly, nemohou se vůči nim dovolávat povinnosti mlčenlivosti, uložené v zájmu zachování státního, hospodářského a služebního tajemství.“

[23] Vyhláška č. 115/1953 Ú.l. Ministerstva národní bezpečnosti ze dne 3. dubna 1953 o skutečnostech tvořících státní tajemství. In epravo.cz Dostupné [online] z: https://www.epravo.cz/vyhledavani-aspi/?Id=27250&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-02].

[24] BÁRTA M., Cenzura československého filmu a televize v letech 1953–1968 SECURITAS IMPERII 10 In: Securitas imperii: sborník k problematice bezpečnostních služeb. Praha: Úřad dokumentace a vyšetřování činnosti Státní bezpečnosti ve Vydavatelství a nakladatelství Ministerstva vnitra České republiky, 1994-. ISBN 80-86621-01-4. ISSN 1804-1612. Dostupné [online] z: https://www.policie.cz/soubor/sbornik-securitas-imperii-securitas-imperii-10-pdf.aspx [cit. 2023-02-02].

obsahují státní, hospodářské nebo služební tajemství a zvyšovat ochranu státního tajemství. [25]

V **trestním zákoně z roku 1961** se již v souvislosti s trestnými činy proti bezpečnosti nehovoří o „státním tajemství“ ale o „**utajovaných informacích**“ se kterými jsou spojené trestné činy vyzvědačství a ohrožení utajované informace.

Tento zákon je pak prováděn Vyhláškou ministerstva vnitra č. 181/1964 Sb. o základních skutečnostech tvořících státní tajemství.[26]

Na základě Usnesení vlády č. 498 ze dne 9. září 1964 byla zřízená Stálá komise na ochranu utajovaných skutečností Ministerstva vnitra. Jejím úkolem bylo aktivně se podílet na provádění ochrany utajovaných skutečností a přípravě materiálů pro vládu, týkající se této problematiky.[27]

V roce 1966 vyšel **zákon č. 81/1966 Sb. o periodickém tisku a o ostatních hromadných informačních prostředcích**.[28] Na základě tohoto zákona byla ustanovena Ústřední publikační správa (nahrazující Hlavní správu tiskového dohledu), jejímž úkolem byl dohled nad prostředky hromadného působení (tisk aj.)[29] a které též zajišťovala, aby *„nebyly zveřejňovány informace, které tvoří předmět státního, hospodářského nebo služebního tajemství*“, tento předmět byl dále upřesněn vyhláškou č. 181/1964 Sb., o základních skutečnostech tvořících státní tajemství, a seznamy utajovaných skutečností resortů.[30] Jednalo se také o hlavní cenzurní úřad, jehož úkolem bylo sledovat, zda nejsou v prostředcích hromadného působení zveřejňovány informace, které jsou

---

[25] SECURITAS IMPERII 10 Sborník k problematice vztahů čs. komunistického režimu k „vnitřnímu nepříteli“© Úřad dokumentace a vyšetřování zločinů komunismu, 2003, ISBN 80-86621-01-4. Dostupné [online] z: https://www.policie.cz/soubor/sbornik-securitas-imperii-securitas-imperii-10-pdf.aspx [cit. 2023-02-02].

[26] Vyhláška č. 181/1964 Sb., ministerstva vnitra o základních skutečnostech tvořících státní tajemství. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1964-181 [cit. 2023-02-02].

[27] Inventár, Sekretariát komisie na ochranu štátneho tajomstva, Praha, Značka Archivního fondu A 23 [online]. Dostupné z: https://www.abscr.cz/data/pdf/inventar/inventar-a23.pdf [cit. 2023-02-02].

[28] Zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1966-81 [cit. 2023-02-02].

[29] Nařízení vlády č. 119/1966 Sb., vládní nařízení, kterým se vydává statut Ústřední publikační správy. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1966-119 [cit. 2023-02-02].

[30] Tamtéž.

v rozporu s jinými zájmy společnosti, např. informace zaměřené proti státní politice a ideologii.[31]

Tento zákon byl v důsledku událostí „pražského jara“ zrušen v červnu 1968 a nahrazen zákonem č. 84/1968 Sb., kterým se mění zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích,[32] který cenzuru zrušil.

2.4 Období mezi lety 1971 – 1998

Právní problematika ochrany utajovaných informací nebyla do této doby jednotná a byla upravována mnoha právními předpisy[33] (např. vyhláškami), které byly sjednoceny až v roce 1971 **Zákonem o ochraně státního tajemství č. 102/1971 Sb.** a předpisy Federálního ministerstva vnitra. V rámci tohoto ministerstva pak vznikl samostatný odbor, jehož úkolem bylo prověřování osob a organizací, které měly s utajovanými informacemi pracovat.

Jedná se o první zákon o ochraně utajovaných informací, který byl novelizován až v roce 1990 a platil do roku 1998. Tento zákon definoval pojem **státní tajemství,** upravil jeho ochranu a vymezil způsob jeho určení i ochrany před vyzrazením a zneužitím proti ústavnímu zřízení České a Slovenské Federativní Republiky a jejím zájmům.[34]

Na základě tohoto zákona vydávalo Federální ministerstvo vnitra metodické pokyny či směrnice k zajištění jednotného provádění ochrany státního tajemství a kontrolu jejich dodržování.

---

[31] Nařízení vlády č. 119/1966 Sb., vládní nařízení, kterým se vydává statut Ústřední publikační správy. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1966-119 [cit. 2023-02-02].

[32] Zákon č. 84/1968 Sb., zákon, kterým se mění zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1968-84 [cit. 2023-02-02].

[33] KALAMÁR, Štěpán, Markéta BRUNOVÁ, Josef VESELÝ, Drahomír SÝKORA, Karel ŠIMAN a Petr VLK. *Vnitřní bezpečnost - vybraná témata ochrany utajovaných informací*. Praha: Vysoká škola finanční a správní, 2020. Educopress. ISBN 978-80-7408-202-3.

[34] Zákon č. 102/1971 Sb., o ochraně státního tajemství. In [Systém ASPI]. Wolters Kluwer.. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/31976/1/2/zakon-c-102-1971-sb-o-ochrane-statniho-tajemstvi [cit. 2023-02-02].

Zákon stanovil podmínky, za jakých se může stát osoba pověřenou k přístupu ke státnímu tajemství. Jedná se o obdobu bezpečnostního řízení, které je uvedeno v zákoně č. 412/2005 Sb.

„Určenou osobou může být občan České a Slovenské Federativní Republiky, který svými charakterovými a osobními vlastnostmi poskytuje záruku, že státní tajemství nebude ohroženo. Zjistí-li organizace, že určená osoba již stanoveným předpokladům nevyhovuje, je povinna učinit ihned potřebná opatření.“[35]

Se státním tajemstvím se mohl seznámit i cizinec a osoba bez státní příslušnosti, pokud je to v souvislosti s přípravou, uzavíráním a plněním mezinárodních smluv a dohod, v ostatních případech jen se souhlasem federálního ministerstva vnitra.[36]

Za ochranu státního tajemství v orgánech a organizacích zodpovídali dle zákona jejich vedoucí, jejichž povinností bylo především vytvářet vhodné podmínky pro zabezpečení ochrany státního tajemství, dbát na dodržování souvisejících předpisů a při jejich porušení vyvozovat příslušné závěry a opatření. Také bylo jejich povinností provádět kontrolu osob určených k přístupu ke státnímu a hospodářského tajemství a kontrolu nakládání s těmito informacemi.

Osoba, která byla určená ke styku s utajovanými informacemi, byla povinna učinit vše, aby se státní tajemství nestalo známým nepovolané osobě. Zejména byla povinna: *„zachovávat mlčenlivost o státním tajemství, s nímž přichází do styku při výkonu funkce (práce), a to i po skončení pracovního (služebního) poměru a dbát, aby nedocházelo k vyzrazení státního tajemství technickými prostředky (telefon, telegraf, dálnopis apod.).“*[35]

Povinnost mlčenlivosti též platila pro osobu, která se seznámila se státním tajemstvím, ačkoliv k tomu nebyla určena. Např. pokud by nalezla dokument obsahující státní tajemství, bylo její povinností jej předat bez odkladu nejbližšímu

---

[35] Zákon č. 102/1971 Sb., o ochraně státního tajemství. In [Systém ASPI]. Wolters Kluwer.. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/31976/1/2/zakon-c-102-1971-sb-o-ochrane-statniho-tajemstvi [cit. 2023-02-02].

[36] BREJCHA, Aleš. *Právo na informace a povinnost mlčenlivosti v českém právním řádu*. Praha: Codex Bohemia, 1998. ISBN 80-85963-47-7.

útvaru, popřípadě příslušníku Sboru národní bezpečnosti nebo jinému státnímu orgánu.

Mlčenlivosti mohly být osoby seznámené se státním tajemstvím zproštěny v případech, kdy byly dotazovány v řízení před státním orgánem, a tento orgán o zproštění mlčenlivosti požádal. O zproštění mlčenlivosti a jeho rozsahu rozhodoval vedoucí organizace, v níž byla tato osoba ke styku se státním tajemstvím určena. Pokud se jednalo o věc, kterou projednávaly orgány zákonodárných sborů, mohlo o zproštění mlčenlivosti rozhodnout předsednictvo tohoto sboru.[37] Ovšem tyto orgány mohly zproštění mlčenlivosti odepřít v případě, že by jejím zproštěním mohla být způsobena státu vážná škoda, dopady na bezpečnost, obranu, ekonomiku či životy a zdraví občanů.

Zajímavé je, že na rozdíl od současné právní úpravy bylo zákonem zakázáno fotografovat, filmovat, zakreslovat nebo jinak zaznamenávat objekty, prostory a zařízení označené tabulkou ZÁKAZ FOTOGRAFOVÁNÍ (v kompetenci Ministerstva obrany a Ministerstva vnitra).

Dále zákon zavedl tzv. šifrovou službu, spadající do kompetence Ministerstva vnitra. Tuto službu řídilo a provozovalo Federální ministerstvo vnitra a za její činnost odpovídal vedoucí organizace.

Na rozdíl od současné právní úpravy zákon o ochraně státního tajemství upravoval také ochranu tzv. *hospodářského tajemství*, čímž se rozumělo vše, co bylo důležité pro hospodářskou činnost a mělo zůstat utajeno před nepovolanou osobou. *Služebním tajemstvím* byla pak důležitá skutečnost, která souvisí s činností národního výboru, soudu, ozbrojených sil nebo ozbrojeného sboru nebo jiného státního orgánu, státní, hospodářské, družstevní nebo společenské organizace a v obecném zájmu má zůstat utajena před nepovolanou osobou.

Významným prováděcím předpisem tohoto zákona byla Směrnice federálního ministerstva vnitra č. 9/1972 Ú. V. pro manipulaci a dopravu písemných a jiných materiálů obsahujících skutečnosti tvořící předmět státního,

[37] Zákon č. 102/1971 Sb., o ochraně státního tajemství. In [Systém ASPI]. Wolters Kluwer.. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/31976/1/2/zakon-c-102-1971-sb-o-ochrane-statniho-tajemstvi [cit. 2023-02-02].

hospodářského a služebního tajemství.[38] Tato směrnice stanovila základní pravidla pro tvorbu, příjem, evidenci, manipulaci, přepravu, ukládání a skartaci písemných i jiných materiálů, které obsahují skutečnosti tvořící předmět státního, hospodářského a služebního tajemství.

Na základě této směrnice se utajované dokumenty dělily dle závažnosti obsahu na přísně tajné zvláštní důležitosti, které obsahovaly skutečnosti tvořící předmět státního tajemství zvláště důležitého; přísně tajné, obsahující skutečnosti tvořící předmět státního tajemství a tajné, obsahující skutečnosti tvořící předmět hospodářského a služebního tajemství.

Rozhodující pro stanovení stupně utajení pak byly seznamy utajovaných skutečností.

2.5 Období mezi lety 1998 – 2005

V roce 1998 byl přijat zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, vymezující skutečnosti nutné v zájmu České republiky utajovat, způsob jejich ochrany a povinnosti fyzických a právnických osob atd.[39] Tato oblast utajovaných informací se dává do gesce Národního bezpečnostního úřadu.

Jedním z důvodů, proč byl připraven nový zákon, bylo, že v zákoně o ochraně státního tajemství[40] nebyly dostatečně řešeny podmínky, které musí osoba splnit, aby jí byl umožněn přístup k utajované skutečnosti, a nebyly zde nijak upraveny přístupy k utajované skutečnosti ze strany právnických osob.[41]

---

[38] Směrnice 9/1972 Ú.v. federálního ministerstva vnitra ze dne 23. prosince 1971 pro manipulaci a dopravu písemných a jiných materiálů obsahujících skutečnosti tvořící předmět státního, hospodářského a služebního tajemství. In epravo.cz. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=32074&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-02].

[39] MIKULE, Vladimír. *Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů: Zákon č. 123/1998 Sb., o právu na informace o životním prostředí : [s vysvětlivkami]*. Praha: Codex Bohemia, 1998. AZPP. ISBN 80-85963-72-8.

[40] Zákon č. 102/1971 Sb., o ochraně státního tajemství. In [Systém ASPI]. Wolters Kluwer.. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/31976/1/2/zakon-c-102-1971-sb-o-ochrane-statniho-tajemstvi [cit. 2023-02-02].

[41] KALAMÁR, Štěpán, Markéta BRUNOVÁ, Josef VESELÝ, Drahomír SÝKORA, Karel ŠIMAN a Petr VLK. *Vnitřní bezpečnost - vybraná témata ochrany utajovaných informací.* Praha: Vysoká škola finanční a správní, 2020. Educopress. ISBN 978-80-7408-202-3.

Zákon definoval **utajovanou skutečnost** jako takovou skutečnost, se kterou by neoprávněné nakládání mohlo způsobit újmu zájmům České republiky nebo zájmům, k jejichž ochraně se Česká republika zavázala, nebo by mohlo být pro tyto zájmy nevýhodné, a která je uvedena v seznamu utajovaných skutečností. Zpracování seznamu utajovaných skutečností bylo v kompetenci **Národního bezpečnostního úřadu** na návrh ústředních úřadů a tyto seznamy vydávala vláda.

Národní bezpečnostní úřad byl zřízen jakožto ústřední správní úřad pro oblast ochrany utajovaných skutečností.[42] Tento úřad zajišťuje jednotné provádění ochrany utajovaných skutečností v České republice, vykonává státní dozor a metodickou činnost. Dále např. zajišťoval a koordinoval kryptologický výzkum a vývoj, řídil kryptografickou ochranu utajovaných skutečností a zajišťoval kryptoanalytické služby, informační systémy pro nakládání s utajovanými informacemi, a vydával bezpečnostní prověrky a další.

Dále byl definován **zájem České republiky** na zachování ústavnosti, svrchovanosti, územní celistvosti, zajištění obrany státu, veřejné bezpečnosti, ochrana důležitých ekonomických a politických zájmů, práv a svobod fyzických a právnických osob a ochrana života nebo zdraví fyzických osob. Dále byla stanovena **újma zájmu České republiky**, čímž se rozumělo takové poškození nebo ohrožení zájmu České republiky nebo zájmu, k jehož ochraně se Česká republika zavázala, jehož následky nelze odstranit nebo je lze zmírnit pouze následnými opatřeními. Podle významu zájmu a závažnosti způsobené újmy, se újma dělí na mimořádně vážnou újmu, vážnou újmu a prostou újmu.

Nově také byly zavedeny čtyři druhy **stupňů utajení**. Vyhrazené (V), Důvěrné (D), Tajné (T) a Přísně tajné (PT). A také byly stanoveny podmínky bezpečnostní prověrky, náležitosti dotazníku, rozdělení bezpečnostního řízení podle jednotlivých stupňů prověrky. Do prověřování osob byly zahrnuty zpravodajské služby.

[42]Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1998-148 [cit. 2023-02-03].

Zákon vymezil, kdo je statutárním orgánem u orgánu státu, obce a u organizace a též vymezil jeho povinnosti. Úkolem statutárního orgánu bylo též zajistit ochranu utajovaných skutečností a provádět opatření bezpečnostní prověrky I. stupně. Tomuto orgánu byl přímo podřízen bezpečnostní ředitel, což byla nově zřízená funkce a byly též určeny povinnosti.

Jako **určenou osobu** vymezil zákon takovou fyzickou osobu, která byla určena ke styku s utajovanými skutečnostmi pro vymezenou oblast činnosti a pro stupeň utajení, na který bylo vydáno osvědčení, nebo pro stupeň utajení nižší.

V případě, že osobě, která žádá o vydání osvědčení, nebylo osvědčení vydáno, měla právo podat stížnost a bylo možno podat opravný prostředek proti rozhodnutí o zamítnutí stížnosti, o kterém rozhodovalo Kolegium státních zástupců.

Nově byl zřízen Ústřední registr utajovaných skutečností a Registry utajovaných skutečností (spadající pod Národní bezpečnostní úřad), kde jsou povinně evidovány všechny utajované skutečnosti poskytnuté v rámci mezinárodní spolupráce, kromě utajovaných skutečností evidovaných v rámci spolupráce bezpečnostních sborů, zpravodajských služeb a armády. Též byl stanoven výkon státního dozoru a sankce.

3 SOUČASNÁ PRÁVNÍ ÚPRAVA OCHRANY UTAJOVANÝCH INFORMACÍ

Dne 21. 9. 2005 byl přijat v současnosti platný a účinný zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Vznikl jako novela předchozího zákona reagující na jeho vyhodnocení a také další vývoj potřeb ochrany utajovaných informací v rámci mezinárodních vztahů.

Hlavním cílem bylo odstranění nedostatků předchozí právní úpravy v oblasti ochrany utajovaných skutečností a úprava některých institutů, které se dotýkají členství České republiky v Evropské unii a v Organizaci Severoatlantické smlouvy a též zvýšení právní jistoty adresátů těchto norem.[43] Zákon je v souladu s mezinárodními právními předpisy, s bezpečnostními standardy NATO[44] a s právem EU.[45]

Důvodová zpráva k návrhu tohoto zákona hovořila o nedostatcích předchozího zákona a problémech při jeho aplikaci, zejména z důvodu jeho složitosti, nepřehledné a nejasné struktury a nejednoznačné terminologie. Poukázala na absenci některých základních institutů zajišťujících právní jistotu zúčastněných subjektů. Nedostatky procesní úpravy konstatoval také Ústavní soud, jehož nálezy vedly k novelizaci. Velmi závažným nedostatkem bylo přetěžování NBÚ v oblasti personální bezpečnosti, způsobené především velkým počtem žádostí statutárních orgánů o vydání osvědčení bez vyjasněné personální koncepce v oblasti ochrany utajovaných skutečností. Důsledkem čehož bylo navrhování osob na neodpovídající stupně utajení, které se v průběhu již započaté bezpečnostní prověrky často měnily.

---

[43] Důvodová zpráva k zákonu 412/2005 Sb. in Vládní návrh na vydání zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, tisk 880/0, Parlament České republiky, Poslanecká sněmovna 2005. Dostupné [online] z: https://www.psp.cz/sqw/text/tiskt.sqw?o=4&ct=880&ct1=0 [cit. 2023-02-04].

[44] Jedná se o bezpečnostní směrnici C-M (2002)49 - Bezpečnost v rámci NATO z dubna 2002

[45] Konkrétně např. s rozhodnutím Rady Evropské unie 2001/264/EC, jímž se přijímají bezpečnostní směrnice Rady, rozhodnutím Komise Evropských společenství 2001/844/EC, jímž se přijímají bezpečnostní směrnice Komise a rovněž s nařízením Rady č. 1958/3, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii. Návrh je též slučitelný s Evropskou Úmluvou o ochraně lidských práv a základních svobod z roku 1950, protože na rozdíl od stávající právní úpravy zavádí možnost soudního přezkumu správního rozhodnutí Úřadu (viz Důvodová zpráva)

3.1 Prameny právní úpravy

Problematika ochrany utajovaných informací je v právním řádu ČR upravena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací. Protože praxe nám ukazuje, že není dosažitelné, aby zákony byly formulovány s dostatečnou přesností a absolutní předvídatelností, proto i zákon o ochraně utajovaných informací, jeho výklad a aplikace, se konkretizují pomocí prováděcích předpisů. Jedná se o vyhlášku č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, vyhlášku č. 405/2011 Sb., o průmyslové bezpečnosti, ve znění vyhlášky č. 416/2013 Sb., vyhlášku č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, vyhlášku č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, vyhlášku č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb., vyhlášku č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb., vyhlášku č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.

Pro stanovení utajené informace má velký význam nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

Pramenem právní úpravy ochrany utajovaných informací je také zákon č. 40/2009 Sb., trestní zákoník upravující skutkové podstaty trestných činů přímo spojených s ochranou utajovaných informací.[46] V Hlavě IX Díl 2 hovoří o vyzvědačství, ohrožení utajované informace a ohrožení utajované informace z nedbalosti.

Ve vztahu k procesním předpisům, můžeme za pramen vztahující se k ochraně utajovaných informací považovat zákon č. 99/1963 Sb., občanský soudní řád, zákon č. 141/1961 Sb., trestní řád, zákon č. 500/2004 Sb., správní řád a zákon č. 150/2002 Sb., soudní řád správní.[46]

[46] PAVELKA I.: Základní instituty ochrany utajovaných informací v ČR. Správní právo číslo 5/2017 In: Správní právo: odborný časopis pro oblast státní správy a správního práva. Praha: Ministerstvo vnitra, 1968-. ISSN 0139-6005. Dostupné [online] z: https://www.mvcr.cz/clanek/spravni-pravo-cislo-5-2017.aspx [cit. 2023-02-23].

4 ZÁKON Č. 412/2005 SB. O OCHRANĚ UTAJOVANÝCH INFORMACÍ A O BEZPEČNOSTNÍ ZPŮSOBILOSTI

Zákon o ochraně utajovaných informací je stěžejním dokumentem problematiky ochrany utajovaných informací. Říká nám, co to vůbec je utajovaná informace a jak ji chápat a určuje, za jakých podmínek a kdo může s takovými informacemi nakládat, stanovuje podmínky a pravidla pro veškerou manipulaci s nimi.

Bezpečnostní opatření jsou zaměřená jednak na osoby či firmy, které s utajovanými informacemi pracují, ale také na technickou a materiální stránku zabezpečení těchto informací, ať již se jedná o jejich administraci či zabezpečení počítačů či celých budov.

Důvěrné informace a tajemství jsou obvykle chráněny především povinností mlčenlivosti, u ochrany informací státního charakteru je navíc zřejmý poměrně silný důraz na opatření technického rázu, přičemž míra těchto opatření je úměrná stupni jejich utajení.

4.1 Utajovaná informace

Pojem informace jako takový je velmi obecný a současné vědy a jejich pojmosloví jej nedokáží jednoznačně definovat, stejně jako tomu je např. s pojmy vědomí, pohyb, čas či poznání… Informace obsahuje výslednici poznávání lidské činnosti. Podle toho, v kterém oboru se pojem informace definuje, tak i podle toho se různě vykládá. Informaci je možno chápat jako popis čehosi, sdělení a přenos onoho sdělení.[47]

Zákon o ochraně utajovaných informací vymezuje pojem *utajovaná informace,* a to poměrně ze široka jako: *„informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných*

[47] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

informací".[48] Konkrétně si lze představit informaci nejčastěji jako písemnou, ale i jako ústní, fotografickou, v podobě map a plánů, či dokonce ve hmotné podobě nějaké stavby nebo technologického zařízení.

Pokud informace splňuje kritéria daná zákonem, je považována za utajovanou. Jedná se o splnění tzv. formálního a materiálního znaku utajované informace. Formální znaky splňuje informace, která je zaznamenána, označená v souladu se zákonem o ochraně utajovaných informací a je uvedena v seznamu utajovaných informací. Při absenci kteréhokoliv z těchto znaků se o utajovanou informaci nejedná.[49]

Materiální znak utajované informace je vymezen negativně. Nechceme, aby byla utajovaná informace vyzrazena nebo zneužita, a proto zde mluvíme o možnosti újmy či nevýhodnosti pro zájmy České republiky. **Zájmem** České republiky je *„zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob".*[50] **Újmou** zájmu České republiky je pak poškození nebo ohrožení zájmu České republiky.[51]

Podle poškození a míry jeho závažnosti nebo dle ohrožení zájmu České republiky se újma dělí na mimořádně vážnou újmu, vážnou újmu a prostou újmu. Pro celistvost zde uvádíme i čtvrtý faktor, kterým je nevýhodnost pro zájmy České republiky.

Za **mimořádně vážnou újmu** pro zájem České republiky, který vznikne vyzrazením nebo zneužitím utajované informace neoprávněné osobě, může mít například za následek: bezprostřední ohrožení svrchovanosti a územní celistvosti České republiky, rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení

[48] §2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[49] DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.
[50] §2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[51] §3 Tamtéž.

zdraví obyvatel či značné narušení vnitřního pořádku a bezpečnosti České republiky.[52]

Pokud bychom vyzradili neoprávněné osobě či zneužili utajovanou informaci, která by měla za následek např.: značnou škodu České republiky ve finanční, měnové nebo hospodářské oblasti, vážné zvýšení mezinárodního napětí či vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb, vznikla by **vážná újma** zájmu České republiky.[53]

O **prosté újmě** lze hovořit, kdyby vyzrazení neoprávněné osobě či zneužití utajované informace mělo v budoucnu za následek např. zhoršení vztahů České republiky s cizí mocí či ohrožení bezpečnosti jednotlivce.[54]

U **nevýhodnosti** pro zájem České republiky například uvádíme: narušení důležitých obchodních nebo politických jednání České republiky s cizí mocí nebo narušení bezpečnostních operací nebo činnosti zpravodajských služeb,[55] což by bylo následkem zneužití nebo vyzrazení utajované informace neoprávněné osobě.

Na základě výše zmíněných aspektů stanovuje zákon o ochraně utajovaných informací **čtyři stupně utajení**: Vyhrazené, Důvěrné, Tajné a Přísně tajné. Vztah mezi újmou a stupněm utajení zobrazuje Tabulka č.1:

Přísně tajné	→	mimořádně vážná újma
Tajné	→	vážná újma
Důvěrné	→	prostá újma
Vyhrazené	→	může být pro zájem ČR nevýhodné

Tabulka č. 1 - Stupeň utajení

Pro úplnost výkladu definice utajované informace, která je zakončena konstatováním, že musí být i uvedena v seznamu utajovaných informací, by zde autor ještě zmínil Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací a vzhledem k charakteru studia na Policejní Akademii

[52] §3 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[53] §3 odst. 3 Tamtéž.
[54] §3 odst. 4 Tamtéž.
[55] §3 odst. 5 Tamtéž.

České republiky v Praze, který je veden s akcentem na bezpečnost, uvádí příklady některých informací uvedených v seznamu utajovaných informací.

Jedná se o informace z oblasti krizového řízení, civilního nouzového plánování a plánování obrany státu. V seznamu je uveden i způsob zajištění bezpečnosti objektů orgánu státu a dalších objektů, včetně projektové dokumentace a analýzy rizik. Dále Nařízení zmiňuje seznamy a související dokumentace dopravních staveb (objektů) a zařízení pro řízení dopravního provozu, které jsou kritickou infrastrukturou podle krizového zákona. Nebo bezpečnostní opatření směřující k ochraně vnitřního pořádku a bezpečnosti České republiky.[56]

4.2 Druhy zajištění ochrany utajovaných informací

Od vzniku utajované informace až po její zánik musí být zajištěna její ochrana, aby nedošlo k jejímu vyzrazení či zneužití. Z definice pojmu utajované informace víme, že je pro zajištění její ochrany vybudován velmi silný a rozsáhlý aparát její ochrany.

Při ochraně utajovaných informací je třeba pamatovat zejména na osoby, které přicházejí či budou přicházet do styku s utajovanými informacemi, myslet na veškerou manipulaci s utajovanou informací, zabezpečení objektu, kde se zpracovává, či ochranu informačních systémů nebo komunikačních systému a způsob šifrování dat obsahující utajovanou informaci.

Pro tyto potřeby zákon formuluje následující oblasti ochrany utajovaných informací: personální bezpečnost, průmyslovou bezpečnost, administrativní bezpečnost, fyzickou bezpečnost, bezpečnost informačních a komunikačních systémů a kryptografickou bezpečnost.

Tento výčet oblastí nemá žádnou vnitřní hierarchii, můžeme na ně nahlížet jako na sobě rovnocenné a vzájemně podpůrné oblasti. Jejich smyslem a úkolem je předejití porušení povinností při ochraně utajované informace.

[56] Příloha č. 1 – 20, Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

4.3 Personální bezpečnost

Personální bezpečnost je tvořena souborem opatření, která zajišťují, aby se k utajovaným informacím dostaly pouze vhodné (důvěryhodné) fyzické osoby. Zákon stanovuje kritéria pro výběr osob způsobilých pro práci s utajovanými informacemi a způsob jejich ověření. Součástí personální bezpečnosti je též výchova těchto osob a jejich ochrana.

Jiné osoby než ty, které splňují zákonné podmínky pro práci s utajovanými informacemi, s takovými informacemi pracovat ani se s nimi seznamovat nesmí.

Personální bezpečnosti se věnuje hlava II. zákona o ochraně utajovaných informací a blíže ji specifikuje vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

4.3.1 Přístup fyzické osoby k utajované informaci

Podmínky přístupu k utajované informaci lze též dělit na formální a materiální. Materiálním znakem je skutečnost, že tyto informace osoba **nezbytně potřebuje** k výkonu své pracovní nebo jiné činnosti, formálním znakem pak je, že osoba **je držitelem osvědčení fyzické osoby**[57] na příslušný stupeň utajení (PT, T nebo D, pro stupeň **Vyhrazené být alespoň držitelem oznámení** o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené nebo **dokladu)** a je řádně **poučena**.[58] Pro přehlednost autor práce uvádí v Tabulce č. 2 dokumenty pro jednotlivé stupně utajení.

Stupeň Vyhrazené	→	OZNÁMENÍ fyzické osoby		
Stupeň Důvěrné	→	OSVĚDČENÍ fyzické osoby	→	platnost 9 let,
Stupeň Tajné	→	OSVĚDČENÍ fyzické osoby	→	platnost 7 let,
Stupeň Přísně tajné	→	OSVĚDČENÍ fyzické osoby	→	platnost 5 let.

Tabulka č. 2 Dokumenty pro jednotlivé stupně utajení

[57] Příloha č. 7 k vyhlášce č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti ve znění pozdějších předpisů.
[58] BÁNYAIOVÁ, Alena, Josef BENDA, Daniela KOVÁŘOVÁ, Pavel MATES, Stanislav PŘIBYL, František PÚRY a Pavel UHEREK, TULÁČEK, Jan, ed. *Tajemství v českém právním řádu*. Praha: Leges, 2019. Extra (Leges). ISBN 978-80-7502-347-6.

Oznámení o splnění podmínek pro přístup k utajované informaci se vydá pouze fyzické osobě, která je svéprávná, dosáhla alespoň 18 let věku a je bezúhonná.[59] Pro získání **osvědčení fyzické osoby** se musí také jednat o občana České republiky nebo státního příslušníkem členského státu EU nebo OSN, který je navíc osobnostně způsobilý a je bezpečnostně spolehlivý.[60] Tyto podmínky musí fyzická osoba splňovat po celou dobu platnosti těchto dokumentů. Přehled způsobu a rozsahu ověřování podmínek je uveden souhrnně v Tabulce č. 3.

PODMÍNKY	VYHRAZENÉ (oznámení)	DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ (osvědčení)
Svéprávnost	ANO	ANO
Věk minimálně 18 let	ANO	ANO
Bezúhonnost	ANO	ANO
Státní občanství ČR, země EU, NATO	NE	ANO
Osobnostní způsobilost	NE	ANO
Bezpečnostní spolehlivost	NE	ANO

Tabulka č.3 - Přehled způsobu a rozsahu ověřování podmínek[61]

Pravidla pro přístup k utajované informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné jsou samozřejmě přísnější a prověřování osoby je podrobnější. Splnění podmínek pro získání osvědčení fyzické osoby je ověřováno v **bezpečnostním řízení** NBÚ, v Tabulce č. 4 je uvedena statistika žádostí na Osvědčení fyzické osoby (osvědčení FO).

	Osvědčení FO přijaté žádosti	Osvědčení FO vydáno	Osvědčení FO nevydáno	Osvědčení FO zrušení platnosti
2015	6236	6161	16	40
2016	5739	5487	16	18
2017	5445	5297	13	19
2018	5175	4970	10	26
2019	6692	5776	14	23
2020	5806	5981	18	12

Tabulka č. 4 - Statistika provádění bezpečnostního řízení NBÚ[62]

[59] § 6 odst.2 a § 12 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[60] § 12 Tamtéž.
[61] Obecně k personální bezpečnosti. In: Věstník Národního bezpečnostního úřadu. č.2/2022 Praha: Národní bezpečnostní úřad, 1999-. ISSN 1212-7086. Dostupné [online] z: https://www.nbu.cz/cs/o-nas/985-vestnik/ [cit. 2023-02-02].
[62] NBÚ, Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, Dostupné [on-line] z: https://odok.cz/portal/veklep/material/KORNCGRBY646/ [cit. 2023-02-10].

Svéprávnost osoba dokládá písemným prohlášením fyzické osoby o svéprávnosti dle předepsaného vzoru,[63] věk občanským průkazem nebo cestovním dokladem.

Bezúhonnost se prokazuje výpisem z evidence Rejstříku trestů ne starším než tři měsíce. Pokud se jedná o cizince, musí předložit obdobný doklad státu, jehož je státním příslušníkem, a rovněž státu, v němž nepřetržitě pobýval více než šest měsíců. Jako bezúhonná se považuje osoba, která není pravomocně odsouzena za spáchání trestného činu vztahujícího se k ochraně utajovaných informací.[64]

Osobnostně způsobilá je fyzická osoba, která netrpí poruchou či obtížemi ovlivňujícími její spolehlivost či schopnost utajovat informace. K ověření slouží prohlášení k osobní způsobilosti nebo v případě pochybnosti ověřovatele znalecký posudek o osobnostní způsobilosti. Zpravodajská služba dále ověřuje osobní způsobilost psychologickým vyšetřením, psychologickým pracovištěm zpravodajské služby nebo Ministerstva vnitra.[65]

Bezpečnostní spolehlivost splňuje fyzická osoba, u níž není zjištěno bezpečnostní riziko. Bezpečnostním rizikem je především závažná nebo opakovaná činnost proti zájmům České republiky, majetkové poměry zjevně nepřiměřené řádně přiznaným příjmům fyzické osoby nebo činnost spočívající v potlačování základních práv a svobod.[66] Dále se může jednat např. o zařazení do složky bývalé Státní bezpečnosti, užívání jiné identity, styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmu České republiky, uvedení nepravdivé informace nebo zamlčení informace v bezpečnostním řízení. V těchto i ostatních případech, které stanovuje zákon, se posuzuje, zda je daná skutečnost bezpečnostním rizikem. Bezpečnostní rizika se zjišťují i za několik let zpětně v závislosti na tom o jaký stupeň utajení se žádá.

---

[63] Příloha č. 1 k vyhlášce č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti ve znění pozdějších předpisů.
[64] §8 odst.1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[65] § 13 Tamtéž.
[66] § 14 Tamtéž.

Poučení[67] osoby před prvním přístupem k utajované informaci zajistí odpovědná osoba. Obě strany podepíší i listinné poučení a každá si nechá jeden výtisk. V případě vyšších stupňů utajení se vyhotovuje a podepisuje ještě další výtisk a odpovědná osoba jej musí zaslat NBÚ.

Pokud dojde k zániku platnosti osvědčení fyzické osoby, ve kterém byl fyzické osobě umožněn přístup k utajované informaci, se má za to, že fyzická osoba není poučena,[68] stejně jako v případě, kdy dojde k zániku platnosti oznámení.

Platnost osvědčení i oznámení zaniká např. uplynutím doby jeho platnosti, úmrtím držitele, odcizením či ztrátou nebo změnou údajů či jeho nečitelností. Oznámení zaniká například též ukončením služebního poměru.[69]

V případě, že fyzická osoba přestane například splňovat podmínky vydání oznámení pro práci s utajovanými informacemi a je jí doručeno písemné vyrozumění o této skutečnosti (v případě stupně Vyhrazené) nebo osoba s osvědčením fyzické osoby obdrží zrušení platnosti osvědčení (pro daný vyšší stupeň utajení), dojde k zániku platnosti příslušného dokumentu. Povinností fyzické osoby je pak do patnácti dnů odevzdat oznámení (osvědčení) tomu, kdo oznámení (osvědčení) vydal.

Pokud dojde k zániku platnosti z důvodu odcizení, poškození, ztráty či změny údajů, držitel oznámení (osvědčení) může do patnácti dnů (ode dne zániku) písemně požádat o vydání nového oznámení (osvědčení). V tom případě může fyzická osoba dále k utajované informaci přistupovat a musí jí být do pěti dnů od doručení žádosti vydáno oznámení nové, které nahrazuje původní.

V případě, že dojde k zániku platnosti oznámení **či osvědčení** fyzické osoby, je povinností vydavatele zajistit, aby tato osoba k utajovaným informacím již neměla přístup.

---

[67] Vzor POUČENÍ Podle § 9 odst. 1 /§ 11 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nalezneme v Příloze č. 4 k vyhlášce č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti ve znění pozdějších předpisů.

[68] § 11 odst. 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

[69] § 9 odst. 3 Tamtéž.

Povinností fyzické osoby je hlásit písemně veškeré změny týkající se svéprávnosti a bezúhonnosti. Dále pak má za povinnost hlásit odcizení, ztrátu nebo poškození oznámení, ale i skutečnosti, které by měly za následek zánik platnosti (např. jeho nečitelnost), nebo den doručení osvědčení fyzické osoby či dokladu. Veškeré skutečnosti je fyzická osoba povinna hlásit ve lhůtě patnácti dnů ode dne, kdy tomu nastalo.

4.3.2 Prokazování oprávnění k přístupu k utajované informaci

Při prověřování oprávnění fyzické osoby k přístupu k utajovaným informacím se musí fyzická osoba prokázat **poučením** a jedním z následujících dokumentů (podle stupně utajení dané informace): **oznámením** o splnění podmínek k přístupu k utajované informaci stupně utajení Vyhrazené, **osvědčením fyzické osoby** nebo **dokladem** (oprávnění k výkonu citlivé činnosti).

4.3.3 Zvláštní přístup k utajované informaci

Zákon určuje výjimky z těchto pravidel pro konkrétní osoby, které tak mají k utajovaným informacím všech stupňů utajení přístup z titulu své funkce (platí pouze po dobu výkonu jejich funkce a pouze v nezbytném rozsahu pro její výkon), aniž by musely být držiteli osvědčení fyzické osoby a poučení. Jedná se o prezidenta republiky, členy vlády nebo Parlamentu ČR, Veřejného ochránce práv a zástupce Veřejného ochránce práv, soudce, prezidenta, viceprezidenta a členy Nejvyššího kontrolního úřadu. Tento zvláštní přístup se ale dle zákona nevztahuje na přístup k utajované informaci cizí moci, s výjimkou prezidenta republiky, předsedy Senátu Parlamentu, předsedy Poslanecké sněmovny Parlamentu, předsedy vlády a ministra zahraničních věcí.[70]

Zvláštním právním předpisem může být stanoveno také kdo a za jakých podmínek má přístup k utajované informaci bez platného osvědčení fyzické osoby v trestním nebo občanském soudním řízení, ve správním řízení a v soudním řízení

[70] § 58 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

správním, a to v rozsahu nezbytném pro uplatnění jejich práv a plnění povinností v těchto řízeních.

Zákon také upravuje tzv. **jednorázový přístup k utajované informaci** stupně utajení Tajné osobě, která má osvědčení na stupeň utajení Důvěrné ve výjimečných a odůvodněných případech na základě písemné žádosti zaslané odpovědnou osobou Národnímu bezpečnostnímu úřadu.

4.4 Průmyslová bezpečnost

Průmyslovou bezpečnost *„tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele,“*[71] kterou provádí dle dikce zákona o ochraně utajovaných informací. Průmyslovou bezpečnost nalezneme v III. hlavě zákona o ochraně utajovaných informací, a podrobněji se ji věnuje vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, ve znění vyhlášky č. 416/2013 Sb.

Zákon stanovuje, za jakých podmínek lze podnikateli, který k výkonu své činnosti nezbytně potřebuje přístup k utajované informaci, tento přístup umožnit. Podmínky musí splňovat i ti podnikatelé, u kterých utajované informace vznikají.

V případě, že se jedná o stupně utajení Vyhrazené, musí buď doložit písemným prohlášením svou schopnost zabezpečit ochranu utajovaných informací (prohlášení podnikatele), nebo být držitelem platného osvědčení podnikatele.[72]

Pro stupně utajení Důvěrné a vyšší musí být podnikatel držitelem platného osvědčení podnikatele příslušného stupně utajení.[73]

4.4.1 Prohlášení podnikatele

Prohlášení podnikatele může učinit podnikatel, který potřebuje přístup k informacím stupně utajení Vyhrazené a má vytvořeny podmínky odpovídající

[71] §5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[72] § 54 Tamtéž.
[73] § 58 až 62 Tamtéž.

formě přístupu k této informaci a příslušnému druhu zajištění její ochrany a zároveň pokud je odpovědná osoba držitelem oznámení, osvědčení fyzické osoby nebo dokladu.[74] Vzor prohlášení podnikatele a veškeré jeho náležitosti stanoví prováděcí právní předpis, ve kterém v jeho příloze nalezneme onen vzor.[75]

4.4.2 Podmínky pro vydání osvědčení podnikatele

Osvědčení podnikatele může podle zákona podnikatel od NBÚ obdržet pouze pokud je ekonomicky stabilní, bezpečnostně spolehlivý, schopný zabezpečit ochranu utajovaných informací, odpovědná osoba musí být držitelem platného osvědčení fyzické osoby pro odpovídající stupeň utajení nebo vyšší. Všechny tyto podmínky musí podnikatel splňovat po celou dobu platnosti osvědčení podnikatele. Splnění těchto podmínek ověřuje NBÚ v bezpečnostním řízení.[76]

Ekonomicky stabilní je podnikatel, který nepodléhá soudnímu moratoriu, není v insolvenci (úpadku) a u kterého nebyla zavedena nucená správa či dočasná správa (v posledních třech letech) apod. a plní své finanční závazky ať již vůči státu (zdravotní či sociální pojištění, daně) či vůči fyzickým nebo právnickým osobám a nebyla na něj uvalena exekuce.

Bezpečnostní spolehlivost splňuje podnikatel, u kterého nebylo zjištěno bezpečnostní riziko. Bezpečnostním rizikem je např. činnost statutárního orgánu nebo jeho člena nebo člena kontrolního orgánu či prokuristy proti zájmům České republiky nebo spočívající v potlačování základních práv a svobod, popř. podpora takové činnosti. Za bezpečnostní riziko se považuje např. také uvedení nepravdivých informací nebo zamlčení informací rozhodných pro ověření podmínek pro vydání osvědčení podnikatele. Dále např. také vazby na osoby či cizí moci, jejichž činnost je proti zájmům ČR či trestná činnost nebo činnost proti zájmům ČR.

---

[74] § 15 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[75] Příloha č. 7 k vyhlášce č. 405/2011 Sb., o průmyslové bezpečnosti
[76] § 16 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

Způsobilost zabezpečit ochranu utajovaných informací[77] splňuje podnikatel, který je schopen zajistit a dodržovat jednotlivé druhy zajištění ochrany utajovaných informací podle zákona v závislosti na příslušném stupni utajení a formě přístupu k utajované informaci.

4.4.3 Prokazování splnění podmínek

Podnikatel má přístup k utajované informaci, která u něj vzniká, nebo mu byla řádně poskytnuta. V případě poskytnutí utajované informace musí ale podnikatel zabezpečit adekvátní ochranu utajovaných informací.

Před prvním přístupem k utajované informaci se musí podnikatel prokázat poskytovateli informace prohlášením či osvědčením podnikatele, případně může poskytovatel požadovat také předložení bezpečnostní dokumentace podnikatele.

Povinností podnikatele je neprodleně písemně oznámit zánik platnosti prohlášení podnikatele tomu, komu jej předal nebo zaslal. Platnost prohlášení podnikatele zaniká dle zákona například uplynutím pěti let, oznámením podnikatele o ukončení přístupu k utajované informaci, zánikem podnikatele nebo když podnikatel přestane splňovat zákonné podmínky pro přístup k utajované informaci.[78]

4.5 Administrativní bezpečnost

Administrativní bezpečnost zahrnuje ucelený soubor opatření a pracovních postupů s cílem zajistit ochranu utajovaných informací po celý jejich životní cyklus – od jejich vzniku až po jejich vyřazení (zánik).[79]

Administrativní bezpečnost *„tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,“*[80] podrobně

---

[77] § 19 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[78] § 15 Tamtéž.
[79] FÍK, Petr. *Metodika správy utajovaných dokumentů*. Praha: Institut pro správu dokumentů, 2020. ISBN 978-80-907792-0-4.
[80] §5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

upravuje hlava IV. zákona o ochraně utajovaných informací a vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, v aktuálním znění.

4.5.1 Tvorba

Utajovaná informace vzniká u původce. Původcem dle zákona o ochraně utajovaných informací je orgán státu, právnická osoba nebo podnikající fyzická osoba, nebo Úřad průmyslového vlastnictví. Při vzniku utajené informace dbá původce na správné stanovení stupně utajení (naplnění formálního a materiálního znaku).

Vyhláška podrobně stanovuje praktické náležitosti, kterými musí být opatřena administrativní pomůcka a jak musí vypadat (např. že se její listy průběžně očíslují a prošijí, na vnitřní straně desek se přelepí konce prošití, otiskne razítko atd.), jak se provádí zápis a opravy údajů, dále se zabývá specifiky některých administrativních pomůcek (např. kdo vyhotovuje kontrolní list, jak se do něj provádí zápis) a jaké náležitosti jsou nutné pro vedení administrativních podmínek v elektronické podobě.

Vyhláška stanovuje povinné údaje, kterými musí být každá administrativní pomůcka označena a určuje podrobnější pravidla (např. popisuje náležitosti jednacího čísla či označování stupně utajení).

Na utajovaném dokumentu v listinné podobě musí být uveden název původce, číslo jednací, den vzniku a stupeň utajení, číslo a počet výtisků, popř. počet utajovaných a neutajovaných příloh.[81]

Stupeň, který původce označil na utajované informaci, zůstává po celou dobu existence této informace a jeho změny je oprávněn provádět pouze původce utajované informace. Charakter utajované informace může vyžadovat od původce vyznačení doby, po kterou má být informace utajována, po uplynutí této doby stupeň utajení zaniká. Pokud pomine důvod pro utajení informace nebo důvody pro utajení neodpovídají stanovenému stupni utajení, je povinností původce

[81] §14 vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

stupeň utajení neprodleně zrušit nebo změnit a uvést to na informaci. Prověřování důvodů utajení je povinností původce nejméně po pěti letech od doby jejího vzniku. Všichni adresáti utajované informace musí být o těchto skutečnostech (zánik, změny utajení) informováni.

4.5.2 Evidence

Utajovaná informace se eviduje v administrativních pomůckách určených vyhláškou č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Jednací protokol slouží pro evidování utajovaného dokumentu. Na rozdíl od předešlé vyhlášky, která hovoří o knize nebo sešitu, aktuální verze již formu nezmiňuje, uvádí ale jeho přesný předepsaný vzor. Pohyb utajovaného dokumentu se zaznamenává do pomocného jednacího protokolu pod číslem jednacím z jednacího protokolu. Veškeré manipulace s utajovanými dokumenty se zaznamenávají do manipulační knihy pro zaznamenávání utajovaného dokumentu při jeho vytváření, převzetí a předávání. Pro potřeby jeho předání slouží doručovací kniha, zápůjčky se zaznamenávají do zápůjční knihy, všechny osoby seznámené s obsahem utajovaného dokumentu se evidují v kontrolním listu. V případě, že je potřeba evidovat větší počet dokumentů k jedné věci, použije se sběrný arch.[82]

Výjimka může nastat v případě stupně utajení Vyhrazené, kdy může odpovědná osoba stanovit, že se neevidují. Avšak i samotné administrativní pomůcky podléhají evidenci.

4.5.3 Přeprava a přenášení

S utajovanými informacemi nelze libovolně manipulovat, pokud je nutné je někam dopravit, je možné je přepravovat nebo přenášet pouze v přenosných schránkách (např. v aktovce či v kufru) nebo v uzavřeném obalu dle jejího stupně utajení a na jejím nosiči. Přepravu smí zajišťovat pouze kurýrní služba nebo držitel poštovní licence. Příjemce je povinen písemně potvrdit převzetí utajované informace.

[82] § 3 vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

Přepravou zásilky se rozumí její dopravení mimo objekt orgánu státu (popř. právnické osoby nebo podnikající fyzické osoby) za účelem jejího doručení adresátovi.

Přenášení utajovaného dokumentu v listinné nebo nelistinné podobě znamená jeho dopravení mimo objekt orgánu státu (popř. právnické osoby nebo podnikající fyzické osoby), jehož účelem není doručení.

4.5.4 Zánik

Pokud je třeba utajovaný dokument zničit, musí to být provedeno tak, aby nebylo možné jej rekonstruovat a identifikovat tak utajované informace, které obsahoval.

Toto zničení musí provést alespoň dvě pověřené osoby a musí o něm být proveden písemný zápis a záznam v příslušné administrativní pomůcce. Osoby, které zničení provedly, musí zápis podepsat a zápis musí být uložen na evidenčním místě. Zničeny mohou být ty utajované informace, které jsou již nepotřebné a nebyly vybrány jako archiválie.

4.6 Fyzická bezpečnost

Fyzickou bezpečnost *„tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat“.*[83] zákon o ochraně utajovaných informací o ní hovoří ve své V. hlavě, bližší upravení nalezneme ve vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Aby byla ochrana utajovaných informací v rámci fyzické bezpečnosti dostatečně zabezpečena, určují se objekty, zabezpečené oblasti a jednací oblasti. Toto dělení umožňuje zamezit nepovolané osobě se seznámit s utajovanou informací, či jí v maximální možné míře ztížit přístup k ní, a vlastně i podepřít administrativní bezpečnost ve formě zabezpečení správné manipulace s utajovanou informací v rámci objektu.

[83] § 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

Objektem rozumíme jakýkoliv ohraničení prostor, zpravidla budovu, ve které se dále nacházejí zabezpečené oblasti, které jsou určené opět jasně stanoveným ohraničeným prostorem a jednacími oblastmi, které slouží k pravidelnému projednávání utajované informace ve stupni utajení Přísně tajné a Tajné.

Utajované informace lze zpracovávat pouze v zabezpečené oblasti odpovídajícího stupně utajení nebo vyšším či v objektu odpovídajícího stupně utajení nebo vyšším, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba. Utajovaná informace se ukládá v zabezpečené oblasti příslušné kategorie nebo vyšší a v ní v trezoru, uzamykatelné skříni nebo jiné schránce.

Za určitých podmínek lze zpracovávat utajované informace v objektu jiné kategorie, než je stupeň utajení zpracovávané utajované informace, nebo mimo objekt, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba. Podle nejvyššího stupně utajení utajované informace, která se ukládá v zabezpečené oblasti se zařazují oblasti do kategorií Přísně tajné, Tajné, Důvěrné a Vyhrazené.

Zabezpečené oblasti v objektu se dále dělí do dvou tříd: třída I a třída II. Rozdíl mezi třídou I a třídou II spočívá v možnosti přístupu k utajované informaci. U třídy II vstupem neoprávněné osoby nedochází k seznámení s utajovanou informací, tato osoba ale musí být v doprovodu osoby oprávněné do této zabezpečené oblasti vstupovat.

Oproti tomu zabezpečené oblasti třídy I zcela zapovídají vstupu neoprávněné osobě. Existují ale odůvodněné případy, kdy neoprávněná osoba i přesto potřebuje vstoupit do této oblasti třídy I. Na tuto možnost zákon pamatuje, a proto v odůvodněných případech a s vědomím odpovědné osoby, která poskytne písemný souhlas, opravňující dočasně změnit třídu I na třídu II tímto vstup umožní. Do třídy II je totiž vstup neoprávněné osobě v doprovodu s oprávněnou osobou a za podmínky, že se zamezí neoprávněné osobě seznamovat s utajovanými informacemi povolen.

Objekty, zabezpečené oblasti a jednací oblasti jsou po fyzické bezpečnosti zabezpečovány ostrahou, režimovými opatřeními a technickými prostředky.

4.6.1 Ostraha

Minimální počet osob zajišťujících nepřetržitou ostrahu se liší podle stupně utajení objektu. V objektu kategorie Přísně tajné to jsou minimálně dvě osoby sloužící přímo v objektu. V případě kategorie Tajné též minimálně dvě osoby, ale z toho jen jedna osoba je osoba přímo přítomna v objektu, a druhá osoba, které poplachové hlášení technických prostředků umožní rychlý zásah (dojezd). U objektu kategorie Důvěrné nejméně jednou osobou, u které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno.

V případě objektu kategorie Vyhrazené a u objektu bez zabezpečené oblasti nebo jednací oblasti se ostraha zajišťuje v rozsahu stanoveném odpovědnou osobou.

Ostraha je zpravidla prováděna zaměstnanci orgánu státu, příslušníky ozbrojených sil nebo ozbrojených bezpečnostních sborů anebo zaměstnanci bezpečnostní ochranné služby.[84]

4.6.2 Režimová opatření

Režimovými opatřeními jsou stanoveny cíle spočívající v kontrole oprávněnosti vstupu či vjezdu do objektu a výstupu a výjezdu z objektu všech osob a vozidel. Díky režimovým opatřením se též kontroluje a eviduje pohyb osob v zabezpečené oblasti a jednacích oblastí. Dále jsou jimi stanoveny i prostředky a způsoby kontroly osob oprávněných vstupovat do objektu, zabezpečených a jednacích oblastí a dále například způsoby nakládání s klíči a identifikačními prostředky sloužícími pro vstupy a jejich řádné používání.[85]

[84] § 28 odst. 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[85] § 29 Tamtéž.

V rámci režimových opatření, na které naráží osoba vstupující do objektu (prvotní kontrola) se setkáváme i s následnými režimovými opatřeními uvnitř objektu (další opatření). Každá zabezpečená oblast má stanovena svá konkrétní opatření zabraňující vstupu neoprávněné osobě a následného seznamování s utajovanou informací, například další ostrahou přímo před zabezpečenou oblastí.

4.6.3 Technické prostředky

Za technické prostředky fyzické bezpečnosti pokládáme například mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, tísňové systémy, zařízení elektrické zabezpečovací či požární signalizace, aj.[86]

V závislosti na vyhodnocení rizik se určuje míra zabezpečení jednací oblasti a zabezpečené oblasti opatřeními fyzické bezpečnosti dle jejich bodového ohodnocení. Bodové ohodnocení se přiřazuje certifikovaným technickým prostředkům a odpovědnou osobou schváleným necertifikovaným technickým prostředkům.

Opatření fyzické bezpečnosti nebo jejich kombinace musí vždy odpovídat alespoň nejnižší míře zabezpečení jednací oblasti nebo zabezpečené oblasti a jsou stanoveny v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací, které jsou v jednací oblasti pravidelně projednávány, nebo na kategorii zabezpečené oblasti.

Pokud se jedná o objekt bez zabezpečené oblasti nebo jednací oblasti, opatření fyzické bezpečnosti se schvalují v projektu fyzické bezpečnosti.

4.6.4 Projekt fyzické bezpečnosti

Pro objekty, ve kterých se nacházejí zabezpečené oblasti kategorie PT, T nebo D (nebo jednací oblasti), musí vzniknout projekt fyzické bezpečnosti, který popisuje určení objektu a zabezpečených oblastí (nebo jednacích oblastí), včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí, dále pak vyhodnocení

[86] § 30 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

rizik, způsoby použití opatření fyzické bezpečnosti, provozní řád objektu a plán zabezpečení objektu a zabezpečených oblastí (nebo jednací oblasti) v krizových situacích.[87] V případě, že tyto objekty nemají zabezpečené oblasti či jednací oblasti, se projekt fyzické bezpečnosti zužuje jen na vytyčení hranic objektu, provozní řád a plán zabezpečení a opatření fyzické bezpečnosti.

V případě objektu kategorie Vyhrazené bez zabezpečené oblasti obsahuje projekt pouze určení objektu a jeho hranic. Pokud se však v objektu nachází zabezpečená oblast, projekt se o ní rozšíří, určí se její hranice, odpovídající kategorie, třídy a způsob opatření fyzické bezpečnosti.[88]

Projekt fyzické bezpečnosti se dle zákona ukládá u odpovědné osoby nebo bezpečnostního ředitele.

Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků blíže specifikuje způsob ukládání utajovaných informací, organizační požadavky na ostrahu a zabezpečení jednacích oblastí, režimová opatření, požadavky na technické prostředky a zabezpečení objektů, jednacích oblastí apod., vždy v závislosti na stupni utajení dané informace, kategorii zabezpečené oblasti a objektu. Dále přiřazuje bodové ohodnocení pro jednotlivá opatření fyzické bezpečnosti, stanovuje nejnižší míru zabezpečení jednací oblasti nebo zabezpečené oblasti, způsoby hodnocení rizik, ověřování a obsah provozního řádu objektu a plánu zabezpečení objektů, zabezpečených oblastí a jednacích oblastí v krizových situacích.

4.7 Bezpečnost informačních nebo komunikačních systémů

Vzhledem k významu výpočetní techniky a obrovskému nárůstu využití informačních a komunikačních technologií v moderní společnosti, která je na ní v mnoha odvětvích závislá, jsou kybernetické hrozby a informační kriminalita zásadními bezpečnostními hrozbami současného světa. Proto je nezbytné

[87] § 32 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.
[88] § 32 Tamtéž.

neustále zlepšovat bezpečí dat a informací a stále pracovat na zlepšování ochrany v této oblasti, tím spíše pokud se jedná o informace utajované a zvláště citlivé.[89]

Bezpečnost informačních nebo komunikačních systémů *„tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému,“* [90] upravuje ji hlava VI. zákona o ochraně utajovaných informací a vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů.

Hlavním úřadem zajišťujícím ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany a který zajišťuje bezpečnost systémů kritické infrastruktury je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který vznikl 1. srpna 2017.

Všechny **informačními systémy** nakládající s utajovanými informacemi musí být schválené a certifikované Národním úřadem pro kybernetickou a informační bezpečnost. Informačními systémy jsou počítače, počítačové sítě a jejich programové vybavení a veškerá připojená zařízení, včetně jejich správy. Těmito systémy je tedy myšlený nejen hardware, ale i software, a také osoby, které je obsluhují.

Přenos utajovaných informací zajišťují tzv. **komunikační systémy.** Tyto systémy zahrnují koncová komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy. Provozovatel každého takového komunikačního systému musí mít Národním úřadem pro kybernetickou a informační bezpečnost schválený tzv. projekt bezpečnosti komunikačního systému.

Projekt bezpečnosti komunikačního systému musí obsahovat bezpečnostní politiku komunikačního systému, organizační a provozní postupy provozování

---

[89] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-868-9838-5.
[90] § 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

komunikačního systému, provozní směrnice pro bezpečnostní správu komunikačního systému a také pro uživatele komunikačního systému.[91]

NÚKIB má tedy na starosti certifikaci informačních systémů, schvalování projektů bezpečnosti komunikačních systémů, včetně jejich evidence a kontrolní činnosti. Zároveň také provádí akreditaci informačních systémů nakládajících s utajovanými informacemi, např. pro NATO, EU.

4.7.1 Certifikace

Proces schvalování a certifikace provádí NÚKIB na základě podané žádosti o certifikaci informačního systému a doložené bezpečnostní dokumentace informačního systému.

Bezpečnostní dokumentace informačního systému se skládá z projektové bezpečnostní dokumentace, obsahující bezpečnostní politiku informačního systému, výsledky analýzy rizik, návrh bezpečnosti informačního systému (včetně konkrétních realizovatelných opatření) zajišťující splnění bezpečnostní politiky tohoto systému a také dokumentaci k testům bezpečnosti.[92] Druhou částí je provozní bezpečnostní dokumentace informačního systému, která obsahuje bezpečnostní směrnice předepisující činnost bezpečnostních správců a uživatelů.

Pro zajištění bezpečnosti informačního sytému musí být splněn souhrn opatření zahrnujících počítačovou a komunikační bezpečnost, kryptografickou ochranu, ochranu proti úniku kompromitujícího vyzařování, administrativní, personální a fyzickou bezpečnost informačního systému.[93]

Pokud NÚKIB shledá, že je daný informační systém způsobilý k ochraně utajované informace, získá žadatel certifikát s certifikační zprávou pro informační systém. Tento certifikát je veřejnou listinou deklarující tuto způsobilost a je vydávaný na omezenou dobu v závislosti na potřebném stupni utajení informace (Vyhrazené – max. pět let, Důvěrné – tři roky, Tajné a Přísně tajné – dva roky).

---

[91] Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor - znění od 1. 1. 2012. In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-523#f2972230 [cit. 2023-02-22].
[92] Tamtéž.
[93] Tamtéž.

Dle kompetenčního zákona je svěřeno provozování informačního a komunikačního systému nakládajícího s utajovanými informacemi pro potřeby orgánů veřejné moci Ministerstvu vnitra, a to prostřednictvím oddělení vládního utajeného spojení, které provozuje informační systémy pro nakládání s utajovanými informacemi.

Pro hlasovou komunikaci na mezirezortní úrovni do stupně utajení Tajné, popřípadě Důvěrné slouží dle výroční zprávy NÚKIBu dva informační systémy: Vega-T a Vega-D. Rozvoj těchto systémů je pod dohledem NÚKIBu a jsou úřadem i dle zákona certifikovány.[94]

[94] NÚKIB, *Výroční zpráva o činnosti za rok 2017*, Dostupné [online] z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-cinnosti-nukib-2017.pdf [cit. 2023-02-22].

4.8 Kryptografická ochrana

Kryptografie je spolu s kryptoanalýzou jedním z oborů vědecké disciplíny zvané kryptologie, která se zjednodušeně řečeno zabývá tvorbou, používáním a luštění šifer. Kryptografie se věnuje převáděním informací do takové podoby, aby byla pro neodpovědnou osobu nečitelná, nerozluštitelná (zašifrovaná)[95] a vlastně bezcenná. Studuje např. šifrovací algoritmy, kryptografické nástroje, protokoly apod. Do oblasti utajování informací se někdy řadí také steganografie, jejímž cílem je utajení existence zprávy jako takové, na rozdíl od kryptografie, jejímž cílem je utajit obsah zprávy (informace) nikoliv její existenci samotnou.[96] Cílem kryptoanalýzy je naopak získávání zašifrovaných informací, prolamování šifer a získávání utajovaných dat.[97]

Kryptografickou ochranu (KO) tvoří dle zákona *„systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací,“*[98] upravuje ji hlava VIII. zákona o ochraně utajovaných informací a vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. Jak již bylo řečeno, kryptografickou ochranu zabezpečuje Národní úřad pro kybernetickou a informační bezpečnost.

Kryptografickým materiálem se rozumí kryptografický prostředek, materiál k zajištění jeho funkce nebo kryptografický dokument. Veškeré kryptografické prostředky (hardware či software) zajišťující ochranu utajovaných informací musí být certifikovány Národním úřadem pro kybernetickou a informační bezpečnost.

Materiál k zajištění funkce kryptografického prostředku je buď klíčový materiál nezbytný k jednoznačnému zašifrování (např. čipová karta, USB disk), či heslový materiál neboli znakový řetězec, ze kterého se např. odvozuje

---

[95] ZELENKA, Josef. *Ochrana dat: kryptologie*. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4.
[96] KALAMÁR, Štěpán, Markéta BRUNOVÁ, Josef VESELÝ, Drahomír SÝKORA, Karel ŠIMAN a Petr VLK. *Vnitřní bezpečnost - vybraná témata ochrany utajovaných informací*. Praha: Vysoká škola finanční a správní, 2020. Educopress. ISBN 978-80-7408-202-3.
[97] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-868-9838-5.
[98] § 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v aktuálním znění.

kryptografický klíč a další materiály nezbytné pro zajištění správného a bezpečného fungování kryptografického prostředku. Kryptografický dokument je nosič informací ať již v listinné či nelistinné podobě obsahující utajované informace kryptografické ochrany. Jedná se o zvláštní druh utajovaného dokumentu podléhající specifickým pravidlům pro jeho tvorbu, označování, evidenci a manipulaci. Na rozdíl od běžných utajovaných informací musí být např. označen slovem „KRYPTO“.

Výkon kryptografické ochrany (výrobu kryptografických prostředků či materiálů sloužících k zajištění jejich funkce, jejich obsluhu, bezpečnostní správu, evidenci a servis) mohou provádět pouze **pracovníci kryptografické ochrany**, kteří jsou speciálně proškoleni a jsou držiteli platného osvědčení fyzické osoby, držiteli osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany a mají pověření odpovědné osoby. Kryptografická ochrana je zajišťována speciálními **kryptografickými pracovišti** rozdělenými do kategorií podle stupně utajení zpracovávaných informací a certifikovanými Národním úřadem pro kybernetickou a informační bezpečnost.

Bezpečnostní správu kryptografické ochrany vykonává bezpečnostní správce kryptografické ochrany, správce kryptografického materiálu a nadřízený pracovníka kryptografické ochrany, tato správa je zajišťována plněním bezpečnostních opatření jednotlivých druhů ochrany utajovaných informací (bezpečnosti informačních a komunikačních technologií, administrativní, personální a fyzické bezpečnosti).[99]

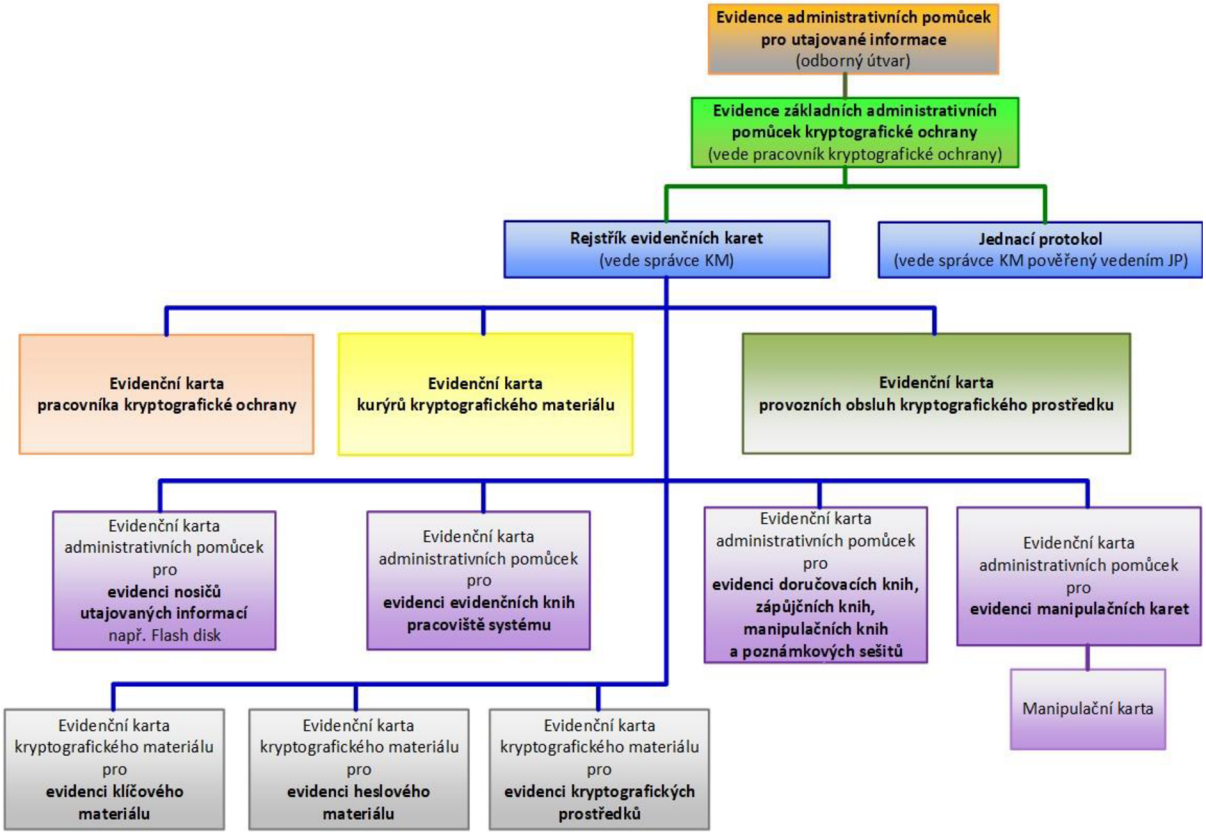
4.8.1 Manipulace s kryptografickým materiálem

Veškerý kryptografický materiál i pracovníci kryptografické ochrany či provozní obsluhy kryptografické ochrany a kurýři kryptografického materiálu musí být evidováni v evidenčních pomůckách kryptografické ochrany v listinné nebo elektronické podobě. Veškeré administrativní pomůcky jsou označeny slovy „KRYPTOGRAFICKÁ OCHRANA“ a musí být zaevidovány a autentizovány (podpis bezpečnostního ředitele nebo osoby pověřené). Grafické znázornění

[99] KALAMÁR, Štěpán, Markéta BRUNOVÁ, Josef VESELÝ, Drahomír SÝKORA, Karel ŠIMAN a Petr VLK. *Vnitřní bezpečnost - vybraná témata ochrany utajovaných informací*. Praha: Vysoká škola finanční a správní, 2020. Educopress. ISBN 978-80-7408-202-3.

veškerých evidenčních pomůcek zobrazuje obrázek č. 2 - Systém evidence krypto. S pomůckami se může seznamovat jen pracovník kryptografické ochrany, pracovník provozní obsluhy kryptografického prostředku nebo kurýr kryptografického materiálu.

Kryptografický materiál může být předáván pouze oproti podpisu v příslušné administrativní pomůcce.



Obrázek č. 2 - Systém evidence krypto

4.8.2 Přeprava a přenášení

Přenášením se rozumí přepravování kryptografického materiálu mimo objekt, jehož cílem není jeho doručení. Přeprava je zde chápána shodně s administrativní bezpečností jako dopravení kryptografického materiálu mimo objekt za účelem jeho doručení adresátovi. Kryptografický materiál tedy přechází do evidence adresáta. K přenášení kryptografického materiálu musí být pracovník kryptografické ochrany zaškolen. Přepravu provádí kurýr kryptografického materiálu služebním vozidlem a je opatřen i mobilním telefonem pro případ např. poruchy vozidla a následného spojení s odesílatelem. Při přenášení je

zapovězeno použití veřejného dopravního prostředku (s výjimkou přepravy letecké a námořní) a podmínkou je souhlas vedoucího zaměstnance nebo odpovědné osoby (záleží na stupni). Oproti administrativní bezpečnosti se přenášení a přeprava u kryptografické ochrany liší též v počtu osob, kdy již nepostačuje jedna osoba, ale je zapotřebí minimálně ještě jeden doprovod.

4.8.3 Kompromitace

Za kompromitaci kryptografického materiálu považujeme takové nakládání s kryptografickým materiálem, které způsobilo nebo by mohlo způsobit porušení ochrany utajované informace. Mezi příklady kompromitace můžeme zařadit například případ neoprávněné manipulace s kryptografickým materiálem či dokonce ztrátu kryptografického materiálu nebo seznámení neoprávněné osoby s kryptografickým materiálem. V případně kryptografického prostředku například odstranění bezpečnostních ochranných prvků (hologramů) či neoprávněná změna nastavení a konfigurace prostředku. Jakýkoliv případ kompromitace se neprodleně oznamuje Národnímu úřadu pro kybernetickou a informační bezpečnost.

5 KOMPARACE

5.1 Plánovaná novela zákona

V roce 2022 dostal NBÚ za úkol připravit a předložit vládě novelu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, která by měla nabýt účinnosti 1. července 2023.

Navrhované změny v zákoně vychází z praktických zkušeností při aplikaci zákona a z některých obtíží, které v praxi vznikají, a reflektují změny a nové poznatky, které od poslední novelizace v roce 2011 vyvstaly. Zároveň uvedou zákon do souladu s právními předpisy EU (např. nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a nařízení Evropského parlamentu a Rady 2016/679/EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.[100]

Jedním z úkolů NBÚ byla revize bezpečnostního řízení a vztah ke správnímu řádu, protože některá ustanovení zákona se shodují se správním řádem a byla zvažována varianta aplikace správního řádu jako celku. Ovšem nebylo shledáno odůvodněným provádět zásadní změny v procesní úpravě.

Mezi plánované změny současného znění zákona patří např. zpřesnění samotné definice utajované informace, která momentálně nezahrnuje všechny reálně možné podoby utajované informace (např. není zahrnuta ústní, obrazová ani zvuková podoba, které nemusí být nutně zachyceny na nějakém nosiči).

Nově by měl být zaveden také pojem utajovaný dokument (protože v praxi se s tímto pojmem pracuje běžně) – kterým je myšlen záznam jakékoliv utajované informace bez ohledu na její podobu. Utajované informace se dále nebudou uvádět v „seznamu“, ale v „katalogu oblastí“ utajovaných informací.

[100] NBÚ, Důvodová zpráva k *návrhu zákona, kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů*, Dostupné [online] z: https://odok.cz/portal/veklep/material/KORNCGRBY646/ [cit. 2023-02-10].

Lze zmínit též nově uvedenou povinnost fyzické osoby, která již nezbytně nepotřebuje přístup k utajovaným informacím (např. přestane být zařazena na daném služebním místě), písemně potvrdit mlčenlivost o utajovaných informacích, ke kterým měla přístup, a neumožnit k nim přístup neoprávněné osobě.

Přístup k utajované informaci stupně Vyhrazené bez platného oznámení budou moci mít např. všichni státní zaměstnanci, příslušníci bezpečnostních sborů či vojáci po dobu výkonu služebního nebo pracovního poměru, pokud jej samozřejmě nezbytně potřebují a jsou poučeni.

Pro vydání osvědčení fyzické osoby již zákon nebude obsahovat podmínku „osobnostní způsobilosti“, ale nahradí ji „bezúhonnost pro účely vydání osvědčení fyzické osoby“ a upraví se i podmínky pro „bezpečnostní spolehlivost“ osoby.

Zároveň je cílem nové úpravy zákona zlepšit a zjednodušit administrativu osob pracujících s utajovanými informacemi (např. NBÚ bude v případě změn údajů v osvědčeních vydávat nová osvědčení, aniž by bylo nutné podávat žádost o novou). Vydání osvědčení pro podnikatele bude nově podmíněno bezúhonností podnikatele. Také by se měla prodloužit platnost osvědčení fyzické osoby a osvědčení podnikatele v režimu tajné a důvěrné na deset let (momentálně se jedná o sedm let a devět let), což bude též v souladu s právní úpravou NATO.

5.2 Slovenská republika

Na rozdíl od České republiky byl na Slovensku původní a několikrát novelizovaný zákon č. 102/1971 Sb., o ochraně státního tajemství již v roce 1996 nahrazen zákonem novým, a to zákonem č. 100/1996 Z. z., o ochrane štátneho tajomstva, služobného tajomstva, o šifrovej ochrane informácií a o zmene a doplnení Trestného zákona v znení neskorších predpisov. Tento zákon byl především reakcí na nové prvky v ochraně utajovaných skutečností (utajované informace jsou zde spolu s utajovanými věcmi zahrnuty pod pojem „utajované skutočnosti“) a nové společensko-politické poměry v zemi dané novým státním uspořádáním. Další dva právní předpisy upravovaly ochranu utajovaných skutečností kvalitativně jiným způsobem (Zákon č. 241/2001 Z. z. a zákon

č. 215/2004 Z. z.) a reagovaly především na mezinárodní vlivy a probíhající proces začlenění Slovenska do NATO a EÚ.[101]

V současné době platí ve Slovenské republice Zákon č. 215/2004 Z. z. Zákon o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.[102]

Některé odlišnosti oproti naší právní úpravě této oblasti stojí za zmínku. Jak již bylo naznačeno klíčovým pojmem ve slovenské právní úpravě je tzv. **utajovaná skutečnost**, pod kterou se rozumí informace nebo věc určená původcem utajované skutečnosti a kterou je potřeba, vzhledem k zájmu Slovenské republiky, chránit před neoprávněnou manipulací a která může vznikat jen ve stanovených oblastech. Slovenský zákon tak přesněji a šířeji určuje, co je předmět utajení (utajovaná skutečnost), informací pak rozumí nejen obsah písemnosti (či nákresu, výkresu, mapy, fotografie, grafu nebo jiného záznamu), ale i obsah ústního vyjádření a obsah elektrického, elektromagnetického, elektronického nebo jiného fyzikálního transportního média. Věcí je pak hmotný nosič se záznamem informací, výrobek, zařízení, či nemovitost. Stejně jako v naší právní úpravě se vymezuje zájem republiky a jeho případná újma a rozdělují se dle významu a závažnosti a utajované skutečnosti se dělí do stejných kategorií (PT, T, D, V).[103]

Zajímavé je, že slovenský zákon určuje oblasti, které nesmí být utajovány. Jedná se např. o informace o nezákonném nebo nesprávném postupu nebo nezákonném rozhodnutí nebo trestné činnosti veřejných činitelů, informace o nehospodárném, neefektivním a neúčelném nakládaní s veřejnými prostředky, o závažném ohrožení nebo poškození životního prostředí, života a zdraví, a též o platových náležitostech, hmotném zabezpečení a hmotných výhodách veřejných činitelů.

---

[101] BRVNIŠŤAN, M., POLÁK, P.: *Vývoj ochrany utajovaných skutočností na území SR*. Právny obzor, 92, 2009, č. 3, s. 262 - 288., Právny obzor: teoretický časopis pre otázky štátu a práva. Bratislava: Slovak Academic Press, [1918]-. ISSN 0032-6984, in Legalis. Dostupné [online] z: https://www.legalis.sk/sk/casopis/pravny-obzor/vyvoj-ochrany-utajovanych-skutocnosti-na-uzemi-sr.m-1060.html [cit. 2023-02-22].

[102] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností - znenie účinné od 01.01.2021 Dostupné [online] z: https://www.zakonypreludi.sk/zz/2004-215 [cit. 2023-02-10].

[103] Tamtéž.

Přístup k utajovaným informacím má pouze oprávněná osoba, která prošla tzv. bezpečnostní prověrkou. Zákon rozlišuje bezpečnostní prověrku I., II., III., IV. stupně (podle stupně utajení). Podmínky oprávnění jsou konkrétnější a obdobné podmínkám pro získání našeho osvědčení fyzické osoby. Musí se jednat o k tomu určeného občana Slovenské republiky, plně právně způsobilého, bezúhonného, který dovršil minimálně 18 let věku (v případě stupně utajení PT dokonce minimálně 21 let), souhlasí s bezpečnostní prověrkou, svým chováním zaručuje, že zabezpečí ochranu utajovaných skutečností, je bezpečnostně spolehlivý a podepíše prohlášení o mlčenlivosti. V případě vyšších stupňů utajení, než je Vyhrazené, musí mít ještě oprávněná osoba tzv. osvědčení úřadu a bezúhonnost nedokládá pouze výpisem z Rejstříku trestů, ale opisem z něho. Platnost osvědčení pro stupeň utajení Přísně tajné je pět let, pro Tajné je sedm let a pro Důvěrné deset let.

Je zde také na rozdíl od naší právní úpravy uveden zákaz fotografovat, filmovat nebo jinak zaznamenávat budovy, prostory nebo zařízení označené zákazem fotografování.

Členění zákona je na první pohled podobné, ovšem po bližším prozkoumání působí logičtěji a přehledněji, ačkoliv jsou druhy (oblasti) ochrany utajovaných informací (resp. skutečností) stejné jako u nás (personální bezpečnost, administrativní, průmyslová atd.). V českém zákoně jsou např. bezpečnostní způsobilost a bezpečnostní řízení samostatnými částmi zákona, kdežto ve slovenském jsou zahrnuty v části ochrana utajovaných skutečností.

6 PŘÍPADOVÁ STUDIE

Práce s utajovanými informacemi na různé úrovni je zahrnuta v agendě většiny organizací státní správy a je proto nezbytné, aby tyto organizace byly řádně poučeny a byly schopny se v této problematice bez problému pohybovat a daná pravidla aplikovat v praxi. Různé oblasti bezpečnosti utajovaných informací mají svá specifická pravidla a též rizika. Společným cílem je zajistit, aby se utajované informace nedostaly do nepovolaných rukou a nemohly tak být jakýmkoliv způsobem zneužity.

6.1 Personální bezpečnost

6.1.1 Zaměstnanci

Zaměstnavatel je povinen zajistit bezpečnost a ochranu zdraví svých zaměstnanců při práci (BOZP)[104] a činí tak. Jak ale ochránit zaměstnavatele před zaměstnancem nám již žádný právní předpis neukládá, a přesto nám škody zaměstnanců ohrožují bezpečí zaměstnavatele i celé organizace. Člověk je považován za nejslabší a nejrizikovější článek pracovních systémů a hrozba selhání lidského faktoru je tak jedním z největších bezpečnostních rizik.[105] Je dobré se tedy zamyslet nad konkrétními riziky a preventivními opatřeními.

Případ 1: Zaměstnanec, který zpracovává utajovanou informaci, nebo má-li ji rozpracovanou, si ji uchovává v listinné nebo elektronické podobě například na nějakém nosiči dat.

Řešení: Zaměstnavatel dohlíží na zaměstnance a vyžaduje po zpracovateli, aby veškeré utajované informace či podkladový materiál uchovával na místech tomu určených, jedná-li se o materiál na nějakém médiu (např. Flash disku), dbá o to, aby byl disk služební a řádně evidovaný.

---

[104] Zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2006-309 [cit. 2023-02-22].

[105] PALEČEK, Miloš; MALÝ, Stanislav; GIECI, Adam. *Spolehlivost lidského činitele*. 1. vyd Praha: Výzkumný ústav bezpečnosti práce, 2008. 140 s. ISBN 978-80-86973-28-9.

Případ 2: Státní zaměstnanec, na jehož služebním místě je nutné mít způsobilost přístupu k utajovaným informacím se může cítit neadekvátně ohodnocen, hrozí zde riziko úmyslného a cíleného poskytnutí utajované informace třetí osobě a způsobení tak újmu zájmu České republiky.

Řešení: Zaměstnavatel by měl zaměstnance finančně adekvátně ohodnotit, aby nebyl motivován řešit svou finanční situaci vyzrazením utajované informace. Motivačním prostředkem ze strany zaměstnavatele může být i řada nabízených služebních benefitů. Negativním vymezením může být například i zákaz konkurence[106] a hrozba vysoké pokuty v případě vyzrazení utajované informace.

Případ 3: Zaměstnanec může způsobit újmu zájmu České republiky i neúmyslně. Například z důvodu přetížení a velkého pracovního nasazení (mnoho úkolů, málo času a kapacit, stresující atmosféra) apod.

Řešení: Zaměstnavatel dbá na rovnoměrné pracovní zatížení zaměstnanců, se zvyšující se agendou pracoviště úměrně navyšuje počet služebních míst. Řádným plánováním předchází práci ve stresu či časové tísni. Zaměstnavatel pravidelně proškoluje zaměstnance v řešení konfliktních a problémových situací.[107]

Případ 4: Ostatní zaměstnanci, kteří nemají přístup k utajovaným informacím, se při výkonu svého zaměstnání nacházejí v bezprostřední blízkosti zaměstnanců zpracovávající utajovanou informaci. Příkladem může být správce objektu, technický pracovník, malíř, uklízečka.

Řešení: Při jakékoliv pracovní činnosti kolegů, kteří nemají přístup k utajovaným informacím, ale nacházejí se v bezprostřední blízkosti zpracovatele (např. uklízečka umývá okna, údržbář kontroluje vzduchotechniku, technický pracovník mění tonery v tiskárně a jiné), zajistí zaměstnavatel dohled (doprovod), aby se zamezilo jakémukoliv úniku utajované informace.

---

[106] Dle §17 odst. 1 bod e) zákona č. 234/2014 Sb., o státní službě. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2014-234/ [cit. 2023-02-22].
[107] Prostřednictvím např. Oddělením personálního rozvoje a psychologických služeb, Dostupné [online] z: https://www.mvcr.cz/clanek/odbor-personalni-4130.aspx [cit. 2023-02-22].

6.1.2 Osvědčení fyzické osoby

Osvědčení fyzické osoby je veřejná listina, vydávaná Národním bezpečnostním úřadem, stvrzující, že držitel splnil podmínky přístupu k utajované informaci v daném stupni utajení.

Případ 1: Podáním první žádosti o vydání osvědčení fyzické osoby dle zákona o ochraně utajovaných informací se žadatel stává účastníkem bezpečnostního řízení. Bezpečnostní řízení zpravidla trvá tři měsíce u osvědčení fyzické osoby pro stupeň utajení Důvěrné, sedm měsíců u osvědčení fyzické osoby pro stupeň utajení Tajné a deset měsíců u osvědčení fyzické osoby pro stupeň utajení Přísně tajné.

Řešení: Z důvodů efektivity a hospodárného nakládání s veřejnými finančními prostředky[108] by se nemělo o osvědčení fyzické osoby žádat nadbytečně, ale dle zásady: „čím méně osob má přístup k utajované informaci, tím menší je riziko úniku utajených informací."

Na druhé straně, pokud žadatel osvědčení fyzické osoby bezpodmínečně potřebuje k výkonu své pracovní činnosti, je třeba dbát o co nejrychlejší vyhotovení (nejkratší možnou dobu bezpečnostního řízení), aby bylo veřejnými finančními prostředky nakládáno účelně a hospodárně a zaměstnanec se mohl co nejrychleji zapojit do plnohodnotného pracovního procesu.

Případ 2: Na počátku bezpečnostního řízení o vydání osvědčení fyzické osoby má žadatel povinnost předložit podkladové materiály. V průběhu bezpečnostního řízení a na základně stupně podané žádosti na osvědčení fyzické osoby si může Národní bezpečnostní úřad povolat svědka.[109] Problém je spatřován v tom, je-li například jako svědek povolán soused, popř. člen bytového družstva domu, který nemusel do této doby být obeznámen s pracovní pozicí souseda.

Řešení: Je-li zapotřebí ze strany Národního bezpečnostního úřadu povolat pro potřeby bezpečnostního řízení svědka, například pro zjištění osobní cti a důstojnosti, preferujme úzké či vzdálené rodinné příslušníky,

[108] OCHRANA, František a Milan PŮČEK. *Dosahování úspor a omezování plýtvání ve veřejném sektoru.* Praha: Wolters Kluwer Česká republika, 2012. ISBN 978-80-7357-909-8.
[109] §104, zákona 412/2005 Sb. o ochraně utajovaných informací, v aktuálním znění.

popř. spolupracovníky, u kterých se můžeme domnívat, že mají jakýsi nástin vhledu pracovní pozice účastníka bezpečnostního řízení. Povoláním svědka z okolí bydliště účastníka bezpečnostního řízení se může NBÚ nevědomky dopustit zvýšeného zájmu o tuto osobu z řad jeho spoluobčanů.

Druhým negativním jevem by mohla být i interpersonální percepce, kdy žadatele sousedi znají z relativně ustálených a opakujících se (zpravidla zdvořilostních) situací, u kterých vzniká relativně bezrozporný obraz a odhad žadatele.[110]

Případ 3: Za předpokladu kladného posouzení žádosti o vydání osvědčení fyzické osoby se po skončení bezpečnostního řízení zašle osvědčení fyzické osoby v písemnosti do vlastních rukou žadatele. Jestliže se žadatel v době doručování písemnosti nevyskytuje v místě bydliště a s uložením zásilky není obeznámen (chybou doručovatelky, nebo odcizením oznámení o uložení zásilky), osvědčení fyzické osoby se následně vrací zpět k odesílateli.

Řešení: Vzhledem k povinnosti žadatele v rámci bezpečnostního řízení, který poskytl Národnímu bezpečnostnímu úřadu osobní údaje (telefon, e-mail), se jeví jako vhodné, současně s odesláním písemnosti obsahující osvědčení fyzické osoby pro příslušný stupeň utajení, též odeslat účastníku bezpečnostního řízení informaci (formou textové zprávy, či e-mailem) o vypravené písemnosti. Díky této povinnosti by nedocházelo k nezaviněnému průtahu při předání osvědčení fyzické osoby.

Případ 4: U držitelů osvědčení fyzické osoby je při vstupu do různých objektů v rámci své pracovní činnosti vyžadována kontrola, stejně tak jako u osob, které nejsou držiteli osvědčení fyzické osoby.

Řešení: Zaměstnanci v rámci své pracovní činnosti umožnit vstup do objektů bez nutnosti kontroly, a to na základně předložení veřejné listiny stvrzující, že její držitel splnil podmínky pro přístup k danému stupni utajované informace (osvědčení fyzické osoby).

[110] ČÍRTKOVÁ, Ludmila. *Policejní psychologie*. 2., rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 9788073805814.

6.2 Průmyslová bezpečnost

Průmyslová bezpečnost se netýká fyzických osob, ale týká se soukromé sféry za předpokladu, že se chtějí seznamovat s utajovanými informacemi. Pokud podnikatel (právnická osoba) nezbytně nutně k výkonu své činnosti potřebuje přístup k utajované informaci a splní veškeré podmínky, Národní bezpečnostní úřad vydá podnikateli osvědčení (certifikát) podnikatele a uvede jej v seznamu.[111]

6.2.1 Utajené objekty

Ze zcela zřejmých důvodů týkajících se bezpečnosti, nemá obyvatelstvo vědomí o existenci jakéhokoliv utajeného objektu. K seznámení dochází zpravidla v době odtajnění objektu a jeho následného jiného využití. Z poslední doby možno například jmenovat velmi medializovaný bezpečnostní projekt v podobě ložiska pitné vody na levém břehu Vltavy nedaleko smíchovského pivovaru v Praze.[112]

Případ 1: Na výše zmíněném příkladu vodního díla, které není z povahy věci ani zavedeno v katastru nemovitostí, se vraťme v čase na dobu objevu a nutnosti výstavby velmi složitého a důmyslného systému přivaděčů, potrubí, šachet, studní a vrtů, díky kterým lze vodu čerpat až na zemský povrch. Tuto stavbu musí zhotovit a projektovat firma, která má certifikaci / osvědčení podnikatele. Někteří zaměstnanci či externí firmy pracující na zakázce, ale žádným osvědčením fyzické osoby nedisponují.

Řešení: Z dostupných materiálů již víme, že projektové dokumentace se zhostila firma Metroprojekt, a právě ta zpracovala technickou dokumentaci k vodnímu dílu – konkrétně ke gravitačnímu přivaděči, který vodu dopraví do technického centra.[113] Měla tedy přístup k utajované dokumentaci. Na elementárním příkladu, např. betonářské firmy dodávající na staveniště

---

[111] NBÚ, *Seznam platných osvědčení podnikatele*. Dostupné [on-line] z: https://www.nbu.cz/cs/informacni-centrum/seznamy/936-seznam-podnikatelu-s-vydanym-potvrzenimosvedcenim-podnikatele/ [cit. 2023-02-10].

[112] KOUTNÍK Ondřej in Lidovky.cz, *Praha svádí boj o utajený zdroj vody. Firma s neprůhledným vlastníkem nad ním chystá miliardový projekt*. Dostupné [on-line] z: https://www.lidovky.cz/domov/praha-svadi-boj-o-utajeny-zdroj-vody-firma-s-nepruhlednym-vlastnikem-nad-nim-miliardovy-projekt.A181204_220318_ln_noviny_vlh [cit. 2023-02-10].

[113] KOUTNÍK Ondřej in Lidovky.cz, *Tajemná firma chce stavět na cenném zdroji vody na Smíchově. Zpochybňuje znalecký posudek*. Dostupné [on-line] z: https://www.lidovky.cz/domov/firma-chce-stavet-na-tajnem-zdroji-vody-na-smichove-zpochybnila-znalecky-posudek.A181215_200300_ln_domov_ele [cit. 2023-02-10].

beton, již tato povinnost není – neseznamují se s utajovanými informacemi. Betonáři vědí, že dodávají beton zhotoviteli stavby, který disponuje certifikátem / osvědčením podnikatele, ale již neví, za jakým účelem. Bylo by dobré, aby v zájmu utajení stavby, měli veškeří subdodavatelé též certifikát / osvědčení podnikatele.

6.2.2 Spolupráce veřejné správy a IT firem

V současné době nabývá na významu tzv. public-private partnership, tedy spolupráce veřejného a soukromého sektoru. Tento fenomén se v mnoha odvětvích osvědčil[114] (např. rozvoj a provoz dopravní infrastruktury), protože přináší výhody pro obě smluvní strany, které sdílí rizika a díky kterému dochází ke zvyšování kvality a efektivity veřejných služeb a také alokaci finančních prostředků.[115] Této problematice se podrobněji věnují např. autoři Hyánek a Řežuchová.

Případ 1: Veřejnou institucí zajišťující kybernetickou bezpečnost a ochranu utajovaných informací v IT je NÚKIB, jeví se jako přínosné neoddělovat striktně veřejný a soukromý sektor v této oblasti, ale naopak co nejúžeji spolupracovat s firmami, které vyvíjí systémy v podobném segmentu a vzájemně se obohatit.

Řešení: Jednou z nejdominantnějších firem na poli IT technologií a síťových prvků a jeho vývoje je bezesporu firma CISCO. Vzhledem k stále častějším a sofistikovanějším hrozbám dnešní doby, které se v kyberprostoru objevují a se kterými je NÚKIB detailně seznámen a vzhledem k intenzivnímu rozvoji firmy Cisco ve stejné oblasti, vznikla vzájemná spolupráce obou subjektů. Ta spočívá ve výměně informací a aktuálního bezpečnostního směřování, výzkumu kybernetických hrozeb, postupů „best practice“ a společných školení. Dochází k výměně informací, dovedností a trendů mezi akademickou, veřejnou

[114] Pravidla (návody) pro úspěšná partnerství veřejného a soukromého sektoru (orig. Guidelines for Successful Public – Private Partnerships). 4. Version 1. EUROPEAN COMMISSION. DIRECTORATE-GENERAL. REGIONAL POLICY. Brussels, February 2003 Pravidla (návody) pro úspěšná partnerství veřejného a soukromého sektoru Dostupné [on-line] z: https://www.mfcr.cz/assets/cs/media/2004-03_Guidelines-for-successful-Public-Private--Partnership-ceska-verze.pdf [cit. 2023-02-10].

[115] HYÁNEK, Vladimír a Markéta ŘEŽUCHOVÁ. *Role soukromého sektoru v poskytování veřejných služeb*. Brno: Masarykova univerzita, 2009. ISBN 978-80-210-4888-1.

a soukromou sférou, díky které firma CISCO i státní organizace mohou zajistit co nejlepší ochranu a minimalizovat riziko narušení kyberprostoru a mohou zefektivnit procesy svého vývoje, směřování a fungování. [116]

6.3 Administrativní bezpečnost

Jedná se o zvláštní režim práce a zacházení s dokumenty, který vyžaduje i specifický přístup, protože dokumenty obsahují utajované informace. Jakákoliv manipulace vyžaduje přístup, ve kterém nemůže dojít k úniku informací, a jejich maximální ochranu.

6.3.1 Označování utajovaných informací a materiálu

Utajovaný dokument, ale i materiál, musí být prokazatelným způsobem zaevidován. Evidenci provádí vždy pověřená osoba, která eviduje utajovanou informaci v souladu se zákonem o ochraně utajovaných informací a vyhláškou o administrativní bezpečnosti a o registrech utajovaných informací.

Případ 1: Řádně evidovaný utajovaný dokument je vložen do neoznačené obálky. V případě nálezu neoznačené obálky třetí osobou může dojít k jejímu otevření a seznámení se s utajovanou informací.

Řešení: Je-li potřebné vkládat utajované dokumenty v listinné podobě do obálky, měla se následně tato obálka opatřit též stupněm utajení a větou: „NEOTEVÍREJTE“. Popř. je vhodné opatřit obálku jmény osob a identifikačních údajů k osobě / osobám (např. služební osobní evidenční číslo zaměstnance), které mohou obálku otevřít.

Případ 2: V případě starého počítačového disku, na kterém se zpracovávaly utajované informace a který již neslouží svému účelu, a je uložen v úschovném objektu, hrozí jeho zneužití osobou, která by k němu měla přístup.

Řešení: Pokud se starý disk ukládá do úschovného objektu, kam mají přístup i jiné osoby, ukládá se odděleně, popřípadě v ochranném obalu opatřeném

[116] CISCO, *Případová studie*, Dostupné [on-line] z: https://www.cisco.com/c/cs_cz/about/case-studies/nukib.html [cit. 2023-02-20].

např. bezpečnostní pečetí a nápisem zakazujícím otevření neoprávněnou osobou. V případě archivace pro následnou skartaci je vhodné disk svépomocí znehodnotit například úderem kladiva či navrtáním disku.

Případ 3: Velmi malé předměty, které je potřeba označit dle zákona, a je zcela zřejmé, že veškeré zákonné náležitosti se na předmět nevejdou, a proto se předmět neoznačí.

Řešení: U velmi malých předmětů (příkladem může být mini paměťový flash disk), neopatřujeme zákonné náležitosti přímo na předmět (na předmětu je jen výrobní číslo), ale na štítek pevně spojený s předmětem, který obsahuje zákonné náležitosti a případně navíc i výrobní číslo disku pro průkaznou identifikaci.

6.3.2 Přeprava utajovaných informací

Ačkoliv nejbezpečnější cestu přenosu a přepravy utajované informace nám v dnešní době nabízí informační systém zabezpečený kryptografickou ochranou, potřeba převážet utajovanou informaci v přenosné schránce kurýrem k tomuto pověřeným nebo držitelem poštovní licence, který se nesmí s přepravovanými informacemi seznámit, je stále potřebná a běžná.

Případ 1: Pro tyto případy je nutné zabezpečit zásilku proti neoprávněnému zneužití informací v ní obsažené. K tomuto účelu nám slouží bezpečnostní pečeť.

Řešení: Správným postupem při přepravě zásilky je opatření zásilky pečetí a její následný zápis do předávacího protokolu nebo doručovací knihy a vzájemná kontrola neporušenosti adresátem a odesílatelem. Nutné je ovšem také zajistit pravidelnou a častou výměnu pečetící hmoty, aby nedocházelo ke tvrdnutí a snadnému neporušenému odtržení pečetě a seznámení se s utajovanou informací.

Případ 2: V případě, že se jedná o utajované informace zvláštního významu a hrozí možnost, že třetí osoba o držení informace ví a měla by zájem se s ní seznámit jakýmkoliv způsobem (za jakoukoliv cenu), vzniká riziko odcizení celé zásilky.

Řešení: Pokud existuje důvodné podezření o riziku odcizení, je voleno několik transportních tras s různými kurýry s tím, že utajovanou informaci veze jen jeden a ostatní vytvářejí jen krytí. Popřípadě je vhodné kurýra doplnit o další osobu, popř. další doprovodné vozidlo/vozidla.

6.4 Fyzická bezpečnost

Jedná se o systém opatření, která zabraňují neoprávněné osobě přístupu k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat.

6.4.1 Ostraha

Ostraha objektu nebo zabezpečených oblastí vykonává činnosti za účelem ochrany vůči vniknutí neoprávněných osob, ale i za účelem monitorování prostor elektronickým zabezpečovacím systémem či elektronickým požárním systémem.

Případ 1: Na velíně disponuje ostraha klíči od všech dveří v objektu a má povolení do nich také vstoupit. Nejčastější způsob uchovávání klíčů zabraňující zneužití je v plastové krabičce opatřené pečetí. Tento způsob ale není nepřekonatelný (opatrné vyloupnutí pečetě).

Řešení: Jednotlivé zapečetěné klíče se vkládají do elektronické zásuvkové skříně. Denním reportem otevření zásuvek se dá zjistit, kdo z ostrahy a za jakým účelem klíč vyjmul.

Případ 2: Ostraha může nepozorovaně sama vstoupit do zabezpečené oblasti nebo může umožnit třetí osobně vstupu do zabezpečených oblastí.

Řešení: Oblasti, do kterých je nežádoucí vstup neoprávněné osoby, jsou navíc zabezpečeny i technickými prostředky bez znalosti ostrahy jejich přístupových kódů. Vstupy, resp. výstupy, z těchto oblastí je žádoucí též monitorovat kamerovým záznamovým systémem.

Případ 3: Přílišné spoléhání pracovníka ostrahy k elektronickým zabezpečujícím systémům a nevěnování se řádnému monitorování objektu (například v nočních hodinách), přičemž v nočních hodinách může docházet k nežádoucím jevům.

Řešení: Velín ostrahy by měl disponovat „aktivizující“ službou (např.: á 30 minut zmáčkni tlačítko), být řádně proškolen, či být namátkově kontrolován.

6.4.2 Režimová opatření

Opatření opravňující vstup osob, popř. vjezd aut do objektu nebo jen do některých částí objektu.

Případ 1: Při vstupu je osoba jen identifikována a není fyzicky kontrolována. Kontrola vozů a zavazadlového prostoru je malá či jen namátková.

Řešení: Ostraha pečlivě kontroluje každou osobu (rám, rentgen) a vozidlo včetně zavazadlového i motorového prostoru.

Případ 2: Do místností určených pro zpracovávání utajované informace mohou volně vstupovat i osoby, které nemají oprávnění.

Řešení: Zamezení přístupu neoprávněných osob pomocí dveřních koulí, popř. vstupem na čip či jakýkoliv jiný identifikující přístup.

Případ 3: Lidský faktor osoby, která dohlíží na režimy vstupů, a umožní přístup třetí osobě.

Řešení: Dbát na velmi dobrý a kvalitní výběr zaměstnanců, motivovat zaměstnance po finanční či po stránce benefitů. Nastavit ostrahu duálně (jeden kontroluje druhého).

6.4.3 Technické prostředky

Technické prostředky slouží především jako podpora ostrahy a režimových opatření. Monitorují objekt či zabezpečenou oblast a informují o sebemenší změně vstupních okolností.[117]

Případ 1: Elektronické zabezpečovací zařízení jen otevírá zámek dveří.

Řešení: Elektronické zabezpečovací zařízení nejenže umožní vstup, ale i zaznamenává, kdy a kým byl použit.

---

[117] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2000. ISBN 80-7251-046-0.

Případ 2: Stacionární kamerové systémy nedisponují funkcí detekce pohybu.

Řešení: Modernizovat kamerové systémy, aby nemusela ostraha objektu neustále sledovat záznamy, ale aby měly kamery funkci detekce pohybu.

Případ 3: Provozuschopnost a funkčnost elektronického zabezpečovacího systému či elektronického požárního systému.

Řešení: Sestavit kontrolní listy a v pravidelných intervalech kontrolovat funkčnost elektronického zabezpečovacího systému či elektronického požárního systému.

Případ 4: Vzhledem k elektronickému systému technických prostředků je klíčová stálá dodávka elektrické energie.

Řešení: Pro případ výpadku elektrické energie disponovat náhradním zdrojem elektrické energie, na který objekt automaticky přejde a nedojde k přerušení provozu a funkčnosti systémů.

6.5 Bezpečnost informačních nebo komunikačních systémů

6.5.1 Výroba informačních systémů

Výběr společností, který mají ve svém portfóliu výrobu a vývoj hardwaru a softwaru pro informační systémy, je klíčový. Při realizaci informačního systému je záhodné vybírat firmu, která disponuje bezpečnostní prověrkou národního bezpečnostního úřadu.

Případ 1: Již při výrobě hardwaru, popřípadě až při samotné realizaci informačního systému, do něj výrobce může přidat odposlouchávací nebo monitorovací zařízení.[118]

Řešení: Při přebírce komponent či celého informačního systému dochází k demontáži hardwaru a jeho důkladné kontrole specializovaným pracovníkem.

[118] DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada, 1998. ISBN 8071694797.

Případ 2: Výrobce či zhotovitel zakázky softwarově uzpůsobí systém ke vzdálenému přístupu či změní nějakou funkcionalitu systému.

Řešení: Zneužití informačního systému neoprávněnou osobou lze předejít vlastní instalací, popřípadě reinstalací systému správcem.

6.5.2 Práce na informačním systému

Jakákoliv činnost či zpracování utajované informace na certifikovaném a do provozu schváleném informačním systému nakládajícím s utajovanými informacemi podléhá nejprve poučením a zaškolením uživatele systému.

Případ 1: Uživatel informačního systému není řádně zaškolen a poučen.

Řešení: Administrátor znemožní funkcionalitou systému uživateli práci na systému do doby řádného zaškolení a poučení.

Případ 2: Uživatel si své přihlašovací údaje zapisuje na lepící papírek a následně lepí na monitor, či vnáší s sebou nepovolené informační a komunikační zařízení (mobil, chytré hodinky, a.j.).

Řešení: Provádět pravidelná např. roční školení a apelovat na dodržování. Přihlašovací údaje si nejlépe pamatovat, popřípadě uschovávat v trezoru. Před vstupem do místnosti s informačním systémem odložit veškeré informační a komunikační zařízení.

Případ 3: Uživatel nedodržuje při práci na informačním systému směrnici (např.: neznemožní přístup třetí osobě zanecháním otevřených dveří či nezatažením okenních záclon).

Řešení: Stanovit uživateli povinnost před započetím činnosti zatemnit okna a uzavřít dveře. Technickými prostředky znemožnit seznámení s utajovanými informacemi třetí osobě (např.: při otevření dveří třetí osobou se vypne displej monitoru).

Případ 4: Uživatel zpracovává utajované informace na hardwarově či softwarově pozměněném informačním systému.

Řešení: Každá komponenta by měla být opatřena bezpečnostním prvkem, např.: hologramem, znemožňující třetí osobě nepřípustné změny systému. Při odstraněném nebo porušeném hologramu uživatel ani nezapočne zpracovávat utajené informace.

6.6 Kryptografická ochrana

6.6.1 Kompromitace kryptografického materiálu

Kompromitací kryptografického materiálu je neoprávněné nakládání s kryptografickým materiálem způsobující porušení ochrany utajované informace nebo jen možnost způsobení této neoprávněné manipulace. Například porušení ochranných prvků, nakládání neoprávněnou osobou s kryptografickým materiálem či seznámení s konfigurací kryptografického prostředku.

Případ 1: Při přenášení či přepravě kryptografického prostředku, jeho montáži či demontáži, může dojít k porušení ochranných prvků.

Řešení: Speciální obsluha disponuje dostatečným počtem náhradních ochranných prvků, které v případě potřeby nahradí a provede o tomto zápis.

Případ 2: V rámci kryptografické ochrany se setkáváme s dvojím typem značení „KRYPTO“ a „KRYPTOGRAFICKÁ OCHRANA“. První kategorie je utajovaná druhá neutajovaná. Obě dvě jsou potřebné ke správnému a funkčnímu provozu kryptografického prostředku. S druhou zmiňovanou kategorií se může seznámit jen a pouze pracovník kryptografické ochrany; pracovník provozní obsluhy kryptografického prostředku nebo kurýr kryptografického materiálu za určitých okolností.

Řešení: Ke správné funkčnosti kryptografického prostředku je potřeba seznámení se s oběma typy / kategoriemi. Čili kryptografický pracovník de facto přistupuje k těmto dvěma kategoriím jakoby rovnocenným a stejně utajovaným. Bylo by tedy namístě tyto kategorie sjednotit.

Případ 3: Nastane-li kompromitace, nastalou situaci řeší příslušný orgán (nejvyšším orgánem je Národní úřad pro kybernetickou a informační bezpečnost, ale může jím být i místní oddělení informační bezpečnosti)

Řešení: Domnívá-li se pracovník speciální obsluhy kryptografického prostředku, že došlo ke kompromitaci, neprodleně tuto informaci zaznamená a nahlásí svému bezprostředně nadřízenému, ten spraví místní oddělení informační bezpečnosti v organizaci, která po vyhodnocení spravuje Národní úřad pro kybernetickou a informační bezpečnost.

7 ZÁVĚR

Jedním ze základních pilířů bezpečnosti, ať již se jedná o jedince či celá společenství (státy či mezinárodní společenství), je ochrana informací. Pravdou je, že činnost demokratického státu by měla být transparentní, ovšem v zájmu vnější i vnitřní bezpečnosti a ochrany svých občanů musí i demokratický stát některé informace utajit (např. před zločinci, teroristy apod.). Vzhledem k stále narůstajícím bezpečnostním hrozbám v této oblasti a významu ochrany utajovaných informací jsem se této problematice věnoval v rámci své diplomové práce. Snažil jsem se předložit ucelený a přehledný pohled na ochranu utajovaných informací. Mou motivací bylo prostudovat podrobněji problematiku ochrany utajovaných informací a hlouběji se seznámit se zákony a vyhláškami, které se k tomuto tématu vztahují. Je třeba říci, že se jedná o velmi rozsáhlou a složitou oblast. Snažil jsem se vymezit, objasnit a představit nejdůležitější části ochrany utajovaných informací co nejjednodušeji a nejpřehledněji.

Během zpracování diplomové práce jsem primárně vycházel ze zákona o ochraně utajovaných informací. Ačkoliv se nejedná se o příliš rozsáhlý zákon a není mnoho literatury, která by se jím zabývala, po obeznámení se se všemi jeho prováděcími předpisy a různými aspekty a pohledy, jsem chvílemi váhal, jestli se nejedná naopak o téma příliš obsáhlé. Při psaní práce mi pomáhala praxe a realita práce s utajovanými informacemi na mém novém působišti, a zároveň praktické využití nabitých vědomostí při přípravě na vykonání úřednické zkoušky z oboru služby ochrana utajovaných informací.

Nejprve jsem se věnoval obecnému vymezení pojmu utajované informace a jejich klasifikací a také újmou, která by mohla být způsobena České republice při nedostatečné ochraně těchto informací. Zabýval jsem se pravidly a podmínkami, které musí fyzické osoby i podnikatelé splnit, pokud potřebují mít přístup k utajovaným informacím a přehledně popsal potřebné dokumenty pro jeho získání např. Osvědčení fyzické osoby a Osvědčení podnikatele. V rámci tzv. administrativní bezpečnosti jsem se zabýval vznikem utajované informace u původce, způsoby jejího vedení a náležitostmi jednotlivých evidencí, dále rozdílností přepravy a přenášení tkvící v doručení či nedoručení adresátovi, a nakonec zánikem samotné utajované informace a jejímu adekvátnímu zničení.

Věnoval jsem se též fyzickým opatřením, která znemožňují neoprávněné osobě se seznamovat s utajovanou informací a která jsou důležitou součástí ochrany utajovaných informací. Tato oblast zahrnuje projekt fyzické bezpečnosti, podmínky ostrahy objektu, režimová opatření a technické prostředky sloužící k zamezení či minimálně k ztížení přístupu k utajované informaci či alespoň tento neoprávněný pokus o přístup zaznamenat.

Oblast ochrany informačních a komunikačních technologií zajišťuje Národní úřad pro kybernetickou a informační bezpečnost, který např. upravuje požadavky na informační systémy nakládající s utajovanou informací v elektronické podobě, schvaluje projekt bezpečnosti zařízení a provádí jeho certifikaci. Dále má na starosti také oblast kryptografické ochrany, která se zabývá použitím kryptografických metod pro šifrování utajované informace, způsoby manipulace s kryptografickým materiálem, kryptografickými pracovišti a pracovníky kryptografické ochrany.

V kapitole komparace jsem nejprve porovnal stávající znění zákona s připravovanou novelou. Novela se dotkne samotného pojmu utajované informace, která bude přesněji definována a nově se v zákoně objeví pojem utajovaný dokument, v praxi již využívaný. Cílem novely je napravení jistých nedostatků, které odhalila především praxe, zjednodušení administrativy, a potřeba sladit zákon s právními předpisy EU a NATO. Rovněž jsem porovnal klíčové oblasti našeho zákona s odpovídajícím zákonem Slovenské republiky (slovenský zákon např. definuje jako klíčový pojem utajovaná skutečnost a hovoří o ní jako o utajované informaci či věci).

V případové studii jsem se snažil využít teoretické vědomosti a poznatky z mnoha odborných školení a specializovaných kurzů, které jsem po nástupu na oddělení vládního utajeného spojení musel absolvovat před výkonem mé služby, a pak z mé následné praxe, a navrhnout možná řešení konkrétních modelových situací týkajících se jednotlivých oblastí práce s utajovanými informacemi v návaznosti na zákon.

Na ochranu utajovaných informací dohlíží Národní bezpečnostní úřad, má na starosti personální bezpečnost (oprávněnost přístupu osob k utajovaným informacím), administrativní bezpečnost (zdali jsou dodržována pravidla tvorby,

evidence, přepravy a přenášení), fyzikou bezpečnost (řádné a způsobilé zabezpečení objektů) a informační bezpečnost (přístupová práva, certifikace). Jeho úkolem je provádět osvětu a vzdělávací aktivity, ale i aktualizovat a přizpůsobovat potřebám doby a vývoje v oblasti IT zákon o ochraně utajovaných informací i všechny jeho prováděcí předpisy. Veškeré prováděné změny musí řádně zdůvodnit a vysvětlit v připomínkovém řízení, protože z hlediska právní jistoty je vhodné co nejjednoznačnější vymezení.

K zajištění ochrany utajovaných informací je třeba dodržovat pravidla daná všemi výše zmíněnými druhy ochrany utajovaných informací, protože jedině tak lze zajistit, že utajované informace budou v bezpečí od svého vzniku až po svůj konec. Důležité je především se zaměřovat na personální bezpečnost a nepodceňovat ji, protože tato oblast s sebou nese největší míru rizika. Také je třeba veškeré povinnosti řádně kontrolovat. Možností je také provádět jejich cvičné testování a analyzovat tak jejich funkčnost. Např. pomocí různých cvičení, podobně jako se dělá cvičné nahlášení bomby, požáru ve škole a nácvik evakuace. Výstupy z těchto cvičení by mohly sloužit jako podklady k novelizacím.

8 SEZNAM POUŽITÉ LITERATURY

Monografie

[1].BÁNYAIOVÁ, Alena, Josef BENDA, Daniela KOVÁŘOVÁ, Pavel MATES, Stanislav PŘIBYL, František PÚRY a Pavel UHEREK, TULÁČEK, Jan, ed. *Tajemství v českém právním řádu.* Praha: Leges, 2019. Extra (Leges). ISBN 978-80-7502-347-6.

[2].BÁTOVSKÝ, Ján. *Ochrana utajovaných skutočností*. Bratislava: Obzor, 1973.

[3].BREJCHA, Aleš. P*ráv*o *na informace a povinnost mlčenlivosti v českém právním řádu.* Praha: Codex Bohemia, 1998. ISBN 80-85963-47-7.

[4].ČÍRTKOVÁ, Ludmila. *Policejní psychologie.* 2., rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 9788073805814.

[5].DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.

[6].DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář.* Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.

[7].FÍK, Petr. *Metodika správy utajovaných dokumentů*. Praha: Institut pro správu dokumentů, 2020. ISBN 978-80-907792-0-4.

[8].HYÁNEK, Vladimír a Markéta ŘEŽUCHOVÁ. *Role soukromého sektoru v poskytování veřejných služeb*. Brno: Masarykova univerzita, 2009. ISBN 978-80-210-4888-1.

[9].KALAMÁR, Štěpán, Markéta BRUNOVÁ, Josef VESELÝ, Drahomír SÝKORA, Karel ŠIMAN a Petr VLK. *Vnitřní bezpečnost – vybraná témata ochrany utajovaných informací.* Praha: Vysoká škola finanční a správní, 2020. Educopress. ISBN 978-80-7408-202-3.

[10].MIKULE, Vladimír. *Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů: Zákon č. 123/1998 Sb., o právu na informace o životním prostředí: [s vysvětlivkami].* Praha: Codex Bohemia, 1998. AZPP. ISBN 80-85963-72-8.

[11].MUSIL, Rudolf. *Ochrana utajovaných skutečností*. Praha: Eurounion, 2001. ISBN 80-85858-93-2.

[12].OCHRANA, František a Milan PŮČEK. *Dosahování úspor a omezování plýtvání ve veřejném sektoru.* Praha: Wolters Kluwer Česká republika, 2012. ISBN 978-80-7357-909-8.

[13].PALEČEK, Miloš; MALÝ, Stanislav; GIECI, Adam. *Spolehlivost lidského činitele.* 1. vyd. Praha: Výzkumný ústav bezpečnosti práce, 2008. 140 s. ISBN 978-80-86973-28-9.

[14].POŽÁR, Josef. *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[15].POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-868-9838-5.

[16].SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha: Dokořán, 1.vyd. 2003. Aliter: Dokořán. ISBN 80-865-6918-7.

[17].SKŘEJPEK, Michal. *Římské soukromé právo: systém a instituce*. 2. upravené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-566-1.
[18].UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2000. ISBN 80-7251-046-0.
[19].ZELENKA, Josef. *Ochrana dat: kryptologie*. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4.

Časopisecké články

[20].BÁRTA M., *Cenzura československého filmu a televize v letech 1953–1968* SECURITAS IMPERII 10 In: Securitas imperii: sborník k problematice bezpečnostních služeb. Praha: Úřad dokumentace a vyšetřování činnosti Státní bezpečnosti ve Vydavatelství a nakladatelství Ministerstva vnitra České republiky, 1994-. ISBN 80-86621-01-4. ISSN 1804-1612. Dostupné [online] z: https://www.policie.cz/soubor/sbornik-securitas-imperii-securitas-imperii-10-pdf.aspx [cit. 2023-02-02].
[21].BRVNIŠŤAN, M., POLÁK, P.: Vývoj ochrany utajovaných skutočností na území SR. Právny obzor, 92, 2009, č. 3, s. 262–288., Právny obzor: teoretický časopis pre otázky štátu a práva. Bratislava: Slovak Academic Press, [1918] -. ISSN 0032-6984, in Legalis. Dostupné [online] z: https://www.legalis.sk/sk/casopis/pravny-obzor/vyvoj-ochrany-utajovanych-skutocnosti-na-uzemi-sr.m-1060.html [cit. 2023-02-22].
[22].NULÍČEK, P.: *Obecně k personální bezpečnosti.* In: Věstník Národního bezpečnostního úřadu. č.2/2022 Praha: Národní bezpečnostní úřad, 1999-. ISSN 1212-7086. Dostupné [online] z: https://www.nbu.cz/cs/o-nas/985-vestnik/ [cit. 2023-02-02].
[23].PAVELKA, I.: *Základní instituty ochrany utajovaných informací v ČR.* Správní právo číslo 5/2017 In: Správní právo: odborný časopis pro oblast státní správy a správního práva. Praha: Ministerstvo vnitra, 1968-. ISSN 0139-6005. Dostupné [online] z: https://www.mvcr.cz/clanek/spravni-pravo-cislo-5-2017.aspx [cit. 2023-02-22].

Zákonná úprava

[24].Zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-412 [cit. 2023-02-20].
[25].Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-522 [cit. 2023-02-20].
[26].Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti ve znění pozdějších předpisů In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2011-363 [cit. 2023-02-20].

[27].Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, ve znění vyhlášky č. 416/2013 Sb., In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2011-405 [cit. 2023-02-20].

[28].Vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2022-275 [cit. 2023-02-20].

[29].Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-528 [cit. 2023-02-20].

[30].Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb., In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-523 [cit. 2023-02-20].

[31].Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb., In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2011-432 [cit. 2023-02-20].

[32].Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb., In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2005-525 [cit. 2023-02-20].

[33].Sdělení č. 440/2009 Sb., Národního bezpečnostního úřadu o vyhlášení převodních tabulek stupňů utajení podle mezinárodních smluv, kterými je Česká republika vázána. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2009-440 [cit. 2023-02-20].

[34].Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností – znenie účinné od 01.01.2021 Dostupné [online] z: https://www.zakonypreludi.sk/zz/2004-215 [cit. 2023-02-20].

[35].Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1998-148 [cit. 2023-02-20].

[36].Směrnice č. 9/1972 Ú.v. federálního ministerstva vnitra ze dne 23. prosince 1971 pro manipulaci a dopravu písemných a jiných materiálů obsahujících skutečnosti tvořící předmět státního, hospodářského a služebního tajemství. In epravo.cz Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=32074&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-02].

[37].Zákon č. 102/1971 Sb., o ochraně státního tajemství. In [Systém ASPI]. Wolters Kluwer. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/31976/1/2/zakon-c-102-1971-sb-o-ochrane-statniho-tajemstvi [cit. 2023-02-02].

[38].Zákon č. 84/1968 Sb., zákon, kterým se mění zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1968-84 [cit. 2023-02-02].

[39].Nařízení vlády č. 119/1966 Sb., vládní nařízení, kterým se vydává statut Ústřední publikační správy. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1966-119 [cit. 2023-02-02].

[40].Zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1966-81 [cit. 2023-02-02].

[41].Vyhláška č. 181/1964 Sb., ministerstva vnitra o základních skutečnostech tvořících státní tajemství. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1964-181 [cit. 2023-02-02].

[42].Vyhláška č. 115/1953 Ú.l. Ministerstva národní bezpečnosti ze dne 3. dubna 1953 o skutečnostech tvořících státní tajemství. In epravo.cz Dostupné [online] z: https://www.epravo.cz/vyhledavani-aspi/?Id=27250&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-02]

[43].Nařízení vlády č. 73/1951 Sb., vládní nařízení, kterým se zřizuje ministerstvo státní kontroly. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1951-73 [cit. 2023-02-02].

[44].Nařízení vlády č. 48/1950 Sb., vládní nařízení, kterým se zřizuje ministerstvo národní bezpečnosti. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1950-48 [cit. 2023-02-02].

[45].Zákon č. 86/1950 Sb., trestní zákon. In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1950-86 [cit. 2023-02-02].

[46].Nařízení č. 171/1949 Sb. Nařízení ministra vnitra, jímž se vydávají předpisy o služební přísaze, o zkušební době, o propuštění v této době a o povolení k uzavírání sňatků příslušníků Sboru národní bezpečnosti In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online]. z: https://www.zakonyprolidi.cz/cs/1949-171 [cit. 2023-02-02].

[47].Zákon č. 19/1855 ř.z. Vojenský trestní zákon o zločinech a přečinech. In: *epravo.cz* [online] a.s. 1999-2023, ISSN 1213-189X. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=342&Section=1&IdPara=1&ParaC=2 [cit. 2023-01-30].

[48].Zákon č. 270/1948 Sb. Zákon o přísaze soudců In: Zákony pro lidi.cz © AION CS 2010-2023 Dostupné [online]. z: https://www.zakonyprolidi.cz/cs/1948-270 [cit. 2023-02-02].

[49].Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/17932/158/2/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky [cit. 2023-02-02].

[50].Zákon č. 131/1912 ř.z. o vojenském trestním řádu v úpravě provedené pozdějšími zákony, naposledy zákonem č. 226/1947 Sb., jak byla úprava vyhlášena vyhláškou ministra národní obrany č. 151/1948 Sb. In: *epravo.cz* [online] a.s. 1999-2023, ISSN 1213-189X. Dostupné [on-line] z:https://www.epravo.cz/vyhledavani-aspi/?Id=719&Section=1&IdPara=1&ParaC=2 [cit. 2023-02-03].

[51].Zákon, daný dne 25. ledna 1914, o služebním poměru státních úředníků a státních sluhů (služební pragmatika). In: *15/1914 ř.z.*. Vídeň 1914, ročník 1914, 8/1914, číslo 15. Dostupné [on-line] z: https://www.epravo.cz/vyhledavani-aspi/?Id=735&Section=1&IdPara=1&ParaC=2 [cit. 2023-01-30].

[52].Zákon č. 50/1923 Sb., na ochranu republiky. In [Systém ASPI]. Wolters Kluwer. ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/3259/1/2 [cit. 2023-02-02].

[53].Vládní nařízení č. 197/1936 Sb., o podnicích důležitých pro obranu státu. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/6617/1/2 [cit. 2023-02-02].

[54].Zákon č. 178/1924 Sb., o úplatkářství a proti porušování úředního tajemství. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/3659/1/2/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi [cit. 2023-02-02].

[55].Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/17932/158/2/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky/zakon-c-231-1948-sb-na-ochranu-lidove-demokraticke-republiky [cit. 2023-02-02].

[56].Zákon č. 178/1924 Sb., o úplatkářství a proti porušování úředního tajemství. In [Systém ASPI]. Wolters Kluwer ISSN 2336-517X. Dostupné [on-line] z: https://www.aspi.cz/products/lawText/1/3659/1/2/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi/zakon-c-178-1924-sb-o-uplatkarstvi-a-proti-porusovani-uredniho-tajemstvi [cit. 2023-02-02].

[57].Dekret č. 63/1945 Sb., presidenta republiky o Hospodářské radě. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/1945-63 [cit. 2023-02-02].

[58].Zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2006-309 [cit. 2023-02-22].

[59].Zákona č. 234/2014 Sb., o státní službě. In: Zákony pro lidi.cz © AION CS 2010-2023. Dostupné [online] z: https://www.zakonyprolidi.cz/cs/2014-234/ [cit. 2023-02-22].

Internetové zdroje

[60].Pravidla (návody) pro úspěšná partnerství veřejného a soukromého sektoru (orig. Guidelines for Successful Public – Private Partnerships). 4. Version 1. EUROPEAN COMMISSION. DIRECTORATE-GENERAL. REGIONAL POLICY. Brussels, February 2003 Pravidla (návody) pro úspěšná partnerství veřejného a soukromého sektoru Dostupné [on-line] z: https://www.mfcr.cz/assets/cs/media/2004-03_Guidelines-for-successful-Public-Private--Partnership-ceska-verze.pdf [cit. 2023-02-10].

[61].Důvodová zpráva k zákonu 412/2005 Sb. in Vládní návrh na vydání zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, tisk 880/0, Parlament České republiky, Poslanecká sněmovna 2005. Dostupné [online] z: https://www.psp.cz/sqw/text/tiskt.sqw?o=4&ct=880&ct1=0 [cit. 2023-02-04].

[62].Inventár, Sekretariát komisie na ochranu štátneho tajomstva, Praha, Značka Archivního fondu A 23 [online]. Dostupné z: https://www.abscr.cz/data/pdf/inventar/inventar-a23.pdf [cit. 2023-02-02].

[63].Svazek vyšetřování a.č. V-6301 MV "Akce STŘED", znalecký posudek a zpráva. Dostupné [online] z: https://www.svazky.cz/archivy/ABS-Praha/FSV/V-6301_MV/V-06301_MV_109.pdf [cit. 2023-02-03].

[64].NBÚ, *Seznam platných osvědčení podnikatele*. Dostupné [on-line] z: https://www.nbu.cz/cs/informacni-centrum/seznamy/936-seznam-podnikatelu-s-vydanym-potvrzenimosvedcenim-podnikatele/ [cit. 2023-02-10].

[65].NBÚ, Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, Dostupné [on-line] z: https://odok.cz/portal/veklep/material/KORNCGRBY646/ [cit. 2023-02-10].

[66].KOUTNÍK Ondřej in Lidovky.cz, *Praha svádí boj o utajený zdroj vody. Firma s neprůhledným vlastníkem nad ním chystá miliardový projekt*. Dostupné [on-line] z: https://www.lidovky.cz/domov/praha-svadi-boj-o-utajeny-zdroj-vody-firma-s-nepruhlednym-vlastnikem-nad-nim-miliardovy-projekt.A181204_220318_ln_noviny_vlh [cit. 2023-02-10].

[67].KOUTNÍK Ondřej in Lidovky.cz, *Tajemná firma chce stavět na cenném zdroji vody na Smíchově. Zpochybňuje znalecký posudek.* Dostupné [on-line] z: https://www.lidovky.cz/domov/firma-chce-stavet-na-tajnem-zdroji-vody-na-smichove-zpochybnila-znalecky-posudek.A181215_200300_ln_domov_ele [cit. 2023-02-10].

[68].Prostřednictvím např. Oddělením personálního rozvoje a psychologických služeb, Dostupné [online] z: https://www.mvcr.cz/clanek/odbor-personalni-4130.aspx [cit. 2023-02-22].

[69].CISCO, *Případová studie*, Dostupné [on-line] z: https://www.cisco.com/c/cs_cz/about/case-studies/nukib.html [cit. 2023-02-20].