Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Veřejná správa a regionální rozvoj

Diplomová práce

Ochrana utajovaných informací ve zvolené organizaci

Bc. Bohumil Jošt

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Bohumil Jošt

Veřejná správa a regionální rozvoj – c.v. Klatovy

Název práce

Ochrana utajovaných informací ve zvolené organizaci

Název anglicky

Protection of classified information in the chosen organization

---

Cíle práce

Hlavním cílem je analýza současného stavu ochrany utajovaných informací a návrh projektu fyzické bezpečnosti ve zvolené organizaci.

Dílčí cíle práce jsou:
- vytvoření přehledu současné legislativy, nástrojů a metod ochrany utajovaných informací,
- provedení analýzy současného stavu ochrany utajovaných informací a analýzy rizik ve zvolené organizaci,
- vypracování a zhodnocení návrhu projektu fyzické bezpečnosti,
- návrh doporučení a formulace závěru.

Metodika

V teoretické části bude provedena deskripce a analýza a srovnání současné platné legislativy ochrany utajovaných informací v ČR, EU a NATO (zejména dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečností způsobilosti a v doprovodných vyhláškách Národního bezpečnostního úřadu).

V praktické části bude vypracována analýza současného stavu ochrany utajovaných informací, analýza hrozeb a rizik informačních systémů určených pro zpracování utajovaných informací. Následně bude vypracován návrh projektu fyzické bezpečnosti modelové organizace veřejné správy se zaměřením na možnosti fyzické ochrany.

Na základě syntézy poznatků teoretické části a vyhodnocení projektu fyzické bezpečnosti budou zhodnoceny výsledky a následně pomocí indukce budou stanovena obecná doporučení a opatření pro zefektivnění ochrany utajovaných informací.

Doporučený rozsah práce

80 stran

Klíčová slova

Ochrana utajovaných informací, analýza rizik, informační systém, fyzická bezpečnost, veřejná správa.

Doporučené zdroje informací

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.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6

LAWRENCE, Fennelly. Effective Physical Security. Fitfh edition. Amsterdam: Butterworth-Heinemann, 2016. ISBN 978-0-12-804462-9.

MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

SZCZEPANIUK, Edyta Karolina, et al. Information security assessment in public administration. Computers & Security, 2020, 90: 101709.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Miloš Ulman, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 20. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Analýza ochrany utajovaných informací ve zvolené organizaci" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Miloši Ulmanovi, Ph.D. za odborné vedení, cenné rady a vstřícnost, s jakou se mi věnoval.

Ochrana utajovaných informací ve zvolené organizaci

Abstrakt

Diplomová práce je vypracována na téma analýza ochrany utajovaných informací na základě zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Zaměřuje se na fyzickou bezpečnost a bezpečnost informačních a komunikačních systémů. Předkládá základní informace o nutnosti a způsobu ochrany informací.

Ochrana utajovaných informací je zásadní pro instituce, které v případě seznamování, zpracování a ukládání utajovaných informací musí splňovat velmi přísná kritéria.

Teoretická část se zabývá nejen základními pojmy, které se týkají této problematiky, ale je hlavně zaměřena na analýzu a rozbor zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Zároveň jsou podrobně analyzovány doprovodné vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků a č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. V rámci zaměření diplomové práce je pozornost věnována zvláště ochraně informačních a komunikačních systémů a fyzické bezpečnosti při ochraně utajovaných informací.

V praktické části je vypracován návrh projektu fyzické bezpečnosti pro fiktivní státní organizaci, která zpracovává, projednává a ukládá utajované informace do stupně utajení Tajné a Přísně tajné. Návrh projektu se podrobně věnuje zabezpečení oblastí na ukládání utajovaných informací v informačním systému, na zabezpečení projednávání utajovaných informací a na zabezpečení ukládání utajovaných informací v listinné podobě. Poukazuje na možnosti a důležité aspekty při tvorbě projektu fyzické bezpečnosti. Způsoby zabezpečení v různých podmínkách jsou podrobeny komparaci a rozdílný způsob zabezpečení technickými prostředky je popsán a zdůvodněn.

Klíčová slova: utajovaná informace, bezpečnost, fyzická bezpečnost, informační bezpečnost, riziko, zabezpečená oblast, ochrana, analýza rizik, technické prostředky, zabezpečení, režimová opatření, projekt.

Protection of classified information in the chosen organization

Abstract

The thesis is based on the analysis of the protection of classified information on the basis of Act No. 412/2005 Coll., on the protection of classified information and security clearance, as amended. It focuses on physical security and security of information and communication systems. It presents basic information on the need for and method of information protection.

The protection of classified information is essential for institutions, which have to meet very strict criteria in the case of the listing, processing and storage of classified information.

The theoretical part deals not only with the basic concepts related to this issue, but is mainly focused on the analysis and analysis of Act No. 412/2005 Coll., on the protection of classified information and security eligibility. At the same time, the accompanying Decree No. 528/2005 Coll., on physical security and certification of technical devices and No. 523/2005 Coll., on security of information and communication systems and other electronic devices handling classified information and on certification of shielding chambers are analysed in detail. Within the focus of the thesis, attention is paid in particular to the protection of information and communication systems and physical security in the protection of classified information. The criteria related to physical protection and protection of information and communication systems are discussed and explained in detail.

In the practical part, a physical security project design is developed for a fictitious state organization that processes, handles and stores classified information classified Secret and Top Secret. The design of the project covers in detail the security of the areas of storage of classified information in the information system, security of the handling of classified information and security of the storage of classified information in paper form. It highlights the options and important considerations in developing a physical security design. The methods of security under different conditions are compared and the different methods of security by technical means are described and justified.

Keywords: classified information, security, physical security, information security, risk, secure area, protection, risk analysis, technical means, security, security measures, project.

Obsah

1 Úvod

Předkládaná diplomová práce se věnuje informacím a jejich ochraně. Je zaměřena na informace utajované a jejich možnou ochranu dle zákona v České republice (ČR). Zvolené téma lze, s ohledem na celosvětovou bezpečnostní situaci, považovat za více než aktuální, ale také se jedná o téma velmi zajímavé a obsáhlé s možností zpracování ve více rovinách. Dalším důležitým aspektem, při výběru téma, je pracovní zařazení. Bohaté pracovní zkušenosti autora, umožňují problematiku zpracovat s větším důrazem na praktické zkušenosti.

Zpracování bezpečnostních dokumentací a zajištění uceleného a komplexního řešení ochrany utajovaných informací představuje záruku ochrany utajovaných informací nejen ve státním sektoru, ale také v podnikatelském sektoru.

Slovo "informace" slyšíme, používáme, čteme, vnímáme a užíváme každý den, například pro popis vědomostí nebo určitých znalostí, které jsou předávány mezi lidmi, pracovišti, společností či národy, a které jsou prospěšné či využitelné pro nějaký účel.[1]

Informace může nabývat různých forem, včetně verbální, vizuální nebo psané podoby, a je přenášena prostřednictvím rozmanitých médií, jako jsou knihy, tisk, televizní vysílání nebo internet. Lidstvo se aktivně věnuje shromažďování, zpracovávání a analýze obrovských datových souborů, s cílem získat, co nejvíce užitečných informací. Tento proces umožňuje hlubší porozumění světu a vytváření informačního kontextu pro širokou veřejnost. Následně jsou informace využity v běžném životě, v zaměstnání a lze díky nim usnadnit práci, případně efektivněji řídit vlastní firmu, korporaci a v neposlední řadě efektivněji řídit stát nebo zajišťovat bezpečnost státu.

Je velmi důležité, aby toto shromažďování, předávání, šíření a využívání informací bylo vždy v našem státě vykonáváno v souladu s platnými předpisy. Česká republika, stejně tak jako i jiné samostatné státy, musí chránit takové informace, které by v případě vyzrazení, mohly způsobit státu újmu či ohrozit samotný chod státu nebo jeho bezpečnost. Jedná se kategorii utajovaných informací.

[1] BAWDEN, David a Lyn ROBINSON. *Úvod do informační vědy*. Doubravník: Flow, 2017. ISBN 978-80-88123-10-1.

2 Cíl práce a metodika

Cílem diplomové práce je předložit ucelený obraz o možnostech ochrany utajovaných informací (UI). Na základě tohoto obrazu následně vypracovat popis zajištění ochrany utajovaných informací v Projektu fyzické bezpečnosti (PFB), který je vypracován pro smyšlenou státní instituci, která pracuje s utajovanými informacemi.

Dílčí cíle práce jsou:

1) zpracování přehledu legislativy v oblasti ochrany utajovaných informací,
2) deskripce metod a nástrojů ochrany utajovaných informací - vysvětlit základní a specifické požadavky na zajištění ochrany utajovaných informací,
3) vytvoření přehledu současného stavu poznání v oblasti řízení informační bezpečnosti a ochrany utajovaných informací ve veřejné správě a legislativy v souvislosti s novými bezpečnostními hrozbami v tuzemsku a zahraničí.
4) vypracování analýzy rizik v popsané fiktivní organizaci,
5) vypracování a zhodnocení návrhu projektu fyzické bezpečnosti,
6) navržení postupů vedoucích ke zkvalitnění ochrany utajovaných informací s důrazem na zkvalitnění ochrany fyzické a ochrany informačních a komunikačních systémů.

Teoretická část je zaměřena na deskripci jednotlivých druhů zabezpečení utajovaných informací a analýzu zákona o ochraně utajovaných informací. Součástí legislativní analýzy je i porovnání legislativy ČR a legislativy, vztahující se k ochraně utajovaných informací, Evropské unie (EU) a Severoatlantické aliance (NATO) Pozornost je také zaměřena na výkon státní správy v této oblasti, tak jak je definována v zákoně č. 412/2005 Sb., na ochranu utajovaných informací a o bezpečnostní způsobilosti.[2]

V praktické části je vypracován PFB. Součástí projektu je vypracování analýzy rizik informačního systému. Pro svou práci autor zvolil smyšlenou organizaci, která nakládá s utajovanými informacemi kategorie Tajné a Přísně tajné. V PFB jsou vybudovány varianty zabezpečených oblastí určených pro zpracování utajovaných informací v informačním systému, pro ukládání a pro projednávání utajovaných informací v kategorii Tajné a Přísně tajné a dále varianta zabezpečené oblasti datového centra. Práce je zaměřena na vhodné technické zabezpečení z pohledu fyzické bezpečnosti. Na základě zjištěných poznatků je navržen adekvátní způsob zajištění ochrany utajovaných informací.

[2] Dále Zákon č. 412/2005 Sb., na ochranu utajovaných informací a o bezpečnostní způsobilosti či ZOUI.

3 Současný stav poznání řešené problematiky

Počáteční část kapitoly je věnována definicím základních pojmů v oblasti ochrany utajovaných informací. Následně je popsáno zdůvodnění důležitosti zachování utajovaných informací a způsoby, jakými jsou tyto informace chráněny v ČR. Pro plné pochopení tématu je provedena stručná analýza stávající legislativy, této problematiky, v ČR a porovnání se základní legislativou v EU a NATO. Součástí této analýzy bude i vymezení různých forem ochrany utajovaných informací, s důrazem na bezpečnost informačních a komunikačních systémů a se zaměřením na fyzickou bezpečnosti.

3.1 Vymezení základních pojmů

Bezpečnost –pojem bezpečnost se ve své podstatě vztahuje k vlastnosti**.** Bezpečností se rozumí ochránit či samotná ochrana před různými hrozbami a riziky. V souvislosti se zadáním této práce je možné mluvit o specifické bezpečnosti, a to kybernetické nebo o bezpečnosti informační. Bezpečnost informačních technologií pojímá ochranu důvěrnosti, integrity a dosažitelnosti při manipulaci s informacemi či daty. Manipulací je míněno zpracování, ukládání, šíření nebo při prezentaci informací. Pojem, **kybernetická bezpečnost**, je neoddělitelně spojen s pojmem **kybernetický prostor**. Tím je míněno digitální prostředí, které dává prostor pro vznik, zpracování a také výměnu informací, které jsou tvořeny elektronicky, tedy pomocí informačních technologií.[3] Velmi zjednodušeně lze říci, že v případě kybernetické bezpečnosti se jedná o celý soubor různých opatření, která směřují na zabezpečení informačních systémů před neoprávněným přístupem. Definici ke kybernetické bezpečnosti je možné vyhledat v materiálech agentury EU pro kybernetickou bezpečnost ENISA, která se podílí na kybernetické politice EU. Ke kybernetické bezpečnosti uvádí „*Kyberbezpečnost se vztahuje na bezpečnost kyberprostoru, kde samotný kybernetický prostor odkazuje na soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a na samotnou sadu objektů, jejichž rozhraní umožňující jejich dálkové ovládání, vzdálený přístup k datům, anebo jejich zapojení do řídících akcí v rámci kyberprostoru“.*[4]

[3] JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf
[4] ENISA. Definition of Cybersecurity [online]. [cit. 03. 09.23]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Ve výkladovém slovníku kybernetické bezpečnosti je pod pojmem Kybernetická bezpečnost uvedeno, „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“*[5]

Utajovaná informace[6] – jedná se o informaci, která je z nějakého důvodu chráněna a nemá být veřejně dostupná. Chránit a tajit nějakou informaci nemusí pouze stát. Informaci může chránit i například organizace nebo výrobní podnik. Utajování bývá spojeno s různými důvody, například s konkurenční výhodou nebo citlivostí. Informace jsou v těchto případech zabezpečeny například pomocí smlouvy nebo pomocí doložky o mlčenlivosti. Státy chrání informace pomocí legislativy. V České republice se jedná o zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon definuje utajovanou informaci 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 informací*“.[7]

Zákon upravuje podmínky pro stanovení utajované informace, podmínky pro přístup k těmto informacím a celý soubor opatření na jejich ochranu.

Bezpečnostní klasifikace - určení, jaký specifický stupeň ochrany před přístupem data nebo informace vyžadují, spolu s vyznačením tohoto stupně ochrany.[8] Zjednodušeně se jedná o stupně utajení informace. Ty jsou přidělovány původcem informace a jejich rozsah je dám výší újmy, která by nastala v případě vyzrazení či znehodnocení informace. Klasifikace informací je podrobněji vysvětlena v kapitole 1.2.1.

Bezpečnostní politika - je základním dokumentem, který představuje ucelený soubor pravidel pro ochranu informací a vymezuje strukturu bezpečnostního rizika a výši či úroveň ochrany těchto informací. Jedná se o základní dokument, ze kterého čerpají další bezpečnostní dokumentace, jakými jsou například bezpečnostní směrnice. Ve své podstatě bezpečnostní politika definuje pravidla, normy a postupy, jakými je zajišťována bezpečnost, důvěrnost, integrita, dostupnost služeb celého systému. Dále také určuje odpovědnost uživatelů, správců a bezpečnostních správců za jejich činnost v systému.

---

[5] JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 03. 01.24] Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

[6] Utajovaná informace dále UI či utajovaná informace

[7] 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. [cit. 10. 09.23].

[8] JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 03. 01.24] Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

Informační systém je definován v § 34 ZOUI jako jeden nebo více počítačů, včetně jejich programového vybavení, periferních zařízení, procesů nebo prostředků schopných provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací. Ve slovníku kybernetické bezpečnosti je informační systém definován jako „ *funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat*.[9] Informační systém zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky. K informačnímu systému se vztahuje také jeho správa, procesy nebo prostředky schopné vytvářet, zpracovávat, ukládat, zobrazovat nebo přenášet utajované informace.[10]

Identifikace – jedná se o proces, kdy na základě identifikátoru je možné rozeznat entitu. V případě Identifikace ID se jedná o pomyslný vzorec používaným systémem k identifikaci uživatele.[11]

[9] JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 03. 01.24] Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

[10] Blíže viz. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. [online]. Dostupné z: https://www.zakonyprolidi.cz

[11] JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 03. 01.24] Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

3.2 Legislativní vymezení

Pro ochranu UI je vytvořen v ČR, EU a NATO ucelený legislativní rámec. Zákony, vyhlášky, normy a jiné předpisy v této problematice jsou obsáhlé a určují postupy, standardy a povinnosti týkající se ochrany UI.

Cílem této diplomové práce je poskytnout přehled, vybraných zákonů a předpisů, které mají úzký vztah k tématu této práce. Tyto právní předpisy jsou významné pro pochopení kontextu a rámcových podmínek, které ovlivňují bezpečnostní politiku týkající se UI.

3.2.1 Legislativa k ochraně utajovaných informací ČR

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Zákon nahradil zákon č. 102/1971 Sb., o ochraně státního tajemství. Účinnost tohoto zákona se datuje od 01. 11. 1998. Jde o první zákon, který definuje utajovanou skutečnost, místo do té doby používaného státního tajemství, a který definoval režim nakládání s utajovanou skutečností. Dále, byly stanoveny nové kategorie pro utajení. Nová klasifikace stanovila čtyři stupně utajení - VYHRAZENÉ, DŮVĚRNÉ, TAJNÉ a PŘÍSNĚ TAJNÉ. Tato kategorizace UI byla implementována v souladu s legislativou NATO.[12] Poslední zásadní změnou, která se vztahuje k tomuto zákonu, je zřízení Národní bezpečnostního úřadu, který se stal garantem v oblasti ochrany UI.[13]

Jak je výše zmíněno, zákon nedefinoval utajovanou informaci, ale utajovanou skutečnost, a to jako: „*utajovaná skutečnost je taková skutečnost, se kterou by neoprávněné nakládání mohlo způsobit újmu zájmům české republiky nebo zájmům, k jejíž ochraně se Česká republika zavázala, nebo by mohlo být pro tyto zájmy nevýhodné, a která je uvedena v seznamu utajovaných skutečností*“.[14]

Zákon je platný dodnes, ale je nutné upozornit, že v současné době z tohoto zákona zbylo prakticky je torzo, v podobě aktualizace zákona č. 2/ 1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR, kde v § 2 byl doplněn Národní bezpečnostní úřad, jako ústřední orgán státní správy.[15] Nicméně, tento zákon původně poprvé stanovil konkrétní požadavky a zavedl postup prověřování, který je nezbytný pro získání oprávnění

[12] Blíže se předpisům NATO věnuje kapitola 1.2.3.
[13] Blíže se Národnímu bezpečnostnímu úřadu věnuje kapitola 1.3.1.
[14] *Zákon č. 148/1998 Sb. o ochraně utajovaných skutečností*. [online]. [cit. 10.04.23]. Dostupné z:https://www. zakonyprolidi.cz/cs/1998-148/zneni-0#f1877594
[15] Blíže viz *Zákon č. 2/1969 Sb*. *Zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky.* Dostupné z: https://www.zakonyprolidi.cz/cs/1969-2

k přístupu k UI. Byly definovány podmínky, za jakých se mohou osoby a organizace seznamovat, přistupovat nebo manipulovat s UI.

NATO, a později i Evropská unie, vyjádřily připomínky k některým nedostatkům zákona a postupně vyvíjely tlak na jeho změnu. Velmi kritizována byla například absence možnosti přezkumu rozhodnutí o nevydání osvědčení, a to jiným orgánem než NBÚ, který tyto dokumenty vydává nebo zamítá. V důsledku všech připomínek byl zákon několikrát novelizován, a byla přijata novela v roce 2000, která urychlila proces šetření a zavedla možnost přezkumu rozhodnutí o nevydání osvědčení. I přes provedené novely bylo nutné zákon dále upravovat a upřesňovat. V roce 2005 byl přijat současně platný a účinný **zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**. Tento zákon zajistil soulad s mezinárodními právními předpisy, zejména s právem EU a NATO. Dále také upřesnil některé kritizované části. Příkladem je definování podmínek přístupu k UI, specifikace podmínek pro přidělení stupně utajení, což znamená, že z informace se stává utajovaná informace. Dále definuje způsob, jak tyto informaci ochránit. Zákon v § 3 definuje výši újmy, která by vznikla v případě jakékoli chybné manipulace a v návaznosti pak v § 4 klasifikuje stupně utajení.

- **VYHRAZENÉ** (označení V) je stanoven u informací, jejichž vyzrazení nebo zneužití muže být pro Českou republiku **nevýhodné.**
- **DŮVĚRNÉ** (označení D) je klasifikována informace, která při vyzrazení nebo zneužití může způsobit **prostou újmu** zájmům České republiky. Prostá újma může mít za následek například zhoršení vztahů ČR s cizí mocí, ohrožení bezpečnosti jednotlivce nebo závažné narušení ekonomických zájmů ČR.
- **TAJNÉ** (označení T)**.** Při vyzrazení nebo zneužití informace, která je klasifikována tímto stupněm, může být způsobena **vážná újma** zájmům České republiky. Vážná újma může představovat značnou škodu ČR ve finanční, měnové nebo hospodářské oblasti, případně ztráty na lidských životech nebo ohrožení zdraví obyvatel.
- **PŘÍSNĚ TAJNÉ** (označení PT) Jedná se o nejvyšší stupeň utajení a v tomto případě by vyzrazení, nebo zneužití informace způsobilo **mimořádně vážnou újmu** zájmům ČR, což může, mimo jiné, znamenat bezprostřední ohrožení svrchovanosti, územní celistvosti nebo demokratických základů ČR a dále rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel.

Zákon č. 412/2005 Sb., je rozložen do devíti hlavních částí, přičemž každá z nich se zabývá specifickým aspektem ochrany a bezpečnosti informací. První část zákona, známá jako „**Základní ustanovení“**, klade základy pro celý zákon tím, že definuje jeho předmět a vysvětluje základní pojmy spojené s utajovanými informacemi. Tato část je základem pro porozumění celému zákonu a jeho aplikaci. Zákon také v první části podrobně popisuje různé druhy ochrany utajovaných informací, jako je personální, průmyslová, administrativní a fyzická bezpečnost, a bezpečnost informačních a komunikačních systémů, včetně kryptografické ochrany. Tyto formy ochrany jsou podpořeny doprovodnými vyhláškami vydávanými NBÚ, které upřesňují a doplňují ustanovení zákona v rámci jednotlivých oblastí ochrany UI. Druhá část, „**Ochrana utajovaných informací**“, se zaměřuje na definici a kategorizaci stupňů utajení a vymezuje typy opatření potřebných pro ochranu utajovaných informací. Zde se stanovují různé úrovně ochrany a přístupy k zajištění bezpečnosti těchto informací. Ve třetí části, „**Bezpečnostní způsobilost**“, jsou specifikovány požadavky pro vykonávání činností, které vyžadují přístup k utajovaným informacím, a definují se podmínky pro udělení bezpečnostní způsobilosti osobám, které s těmito informacemi pracují. Čtvrtá část, „**Bezpečnostní řízení**“, stanovuje obecné principy pro správu a řízení bezpečnostních procesů a systémů, které jsou součástí ochrany utajovaných informací. Pátá část, „**Výkon státní správy**“, se zabývá pravomocemi a odpovědnostmi různých státních orgánů v oblasti bezpečnosti a ochrany utajovaných informací, a definuje jejich roli v celém systému ochrany. Šestá část, „**Kontrola**“, popisuje mechanismy a postupy státního dohledu nad dodržováním předpisů a standardů pro ochranu utajovaných informací. Sedmá část se zaměřuje na **kontrolu činnosti úřadu**, který má klíčovou roli v systému ochrany utajovaných informací. Osmá část, „**Přestupky“**, uvádí možné přestupky spojené s ochranou utajovaných informací a stanovuje sankce pro jejich porušení. Devátá a závěrečná část obsahuje „**Přechodná a závěrečná ustanovení**“, která se zabývají implementací zákona a jeho platností.[16]

První část zákona dále vymezuje některé pojmy, orgány státu a jejich odpovědné osoby a v § 5 definuje jednotlivé druhy zajištění ochrany utajovaných informací. Tyto druhy ochrany jsou následně jednotlivě popsány. Jedná se o:

- **personální bezpečnost**, podstatou této bezpečnosti je výběr vhodných osob, které mají mít přístup k UI,

[16] Blíže viz *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. [online]. Dostupné z: https://www.zakonyprolidi.cz

- **průmyslovou bezpečnost**, kterou tvoří systém opatření pro zajištění přístupu podnikatelů k UI,
- **administrativní bezpečnost**, která se zabývá zabezpečením UI od jejího vzniku přes evidenci, zpracování, odesílání, přepravě, přenášení, ukládání až po skartačním řízení nebo archivaci UI,
- **fyzickou bezpečnost**, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,
- **bezpečností informačních nebo komunikačních systémů,** kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost UI v informačním systému,
- **kryptografická ochrana**, kterou tvoří systém opatření na ochranu UI za použití kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání UI.[17]

Jednotlivé, výše vyjmenované druhy ochrany UI jsou doprovázeny upřesňujícími vyhláškami, vydanými NBÚ.

Vyhláška č. 363/2011 Sb., o personální bezpečnosti.

Vyhláška č. 363/2011 Sb., o personální bezpečnosti, se věnuje klíčovým aspektům týkajícím se personální bezpečnosti, poskytuje rozsáhlý přehled o dokumentech nutných pro získání certifikátu pro jednotlivce a bezpečnostního oprávnění. Toto nařízení podrobně popisuje proces žádání, včetně příkladů a formulářů, které jsou potřebné pro podání takové žádosti, a také vyžadovaná prohlášení. Kromě toho zdůrazňuje význam informování o jakýchkoli změnách v údajích, které jsou součástí dotazníku fyzické osoby. Tímto způsobem Vyhláška o personální bezpečnosti nastavuje jasná a podrobná kritéria jak pro procesní, tak pro obsahové požadavky spojené s udělováním těchto certifikátů a akreditací, což významně přispívá k zefektivnění a zpřesnění celého procesu vyřizování žádostí v oblasti personální bezpečnosti.[18]

[17] Blíže viz *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. [online]. Dostupné z: https://www.zakonyprolidi.cz

[18] Blíže viz *Vyhláška č. 363/2011 Sb., o personální bezpečnosti.* Dostupné z: https://www.zakonyprolidi.cz/

Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti.

Vyhláška č. 405/2011 Sb., která se týká průmyslové bezpečnosti, je v mnoha ohledech analogická vyhlášce o personální bezpečnosti, avšak je specificky upravena pro právnické osoby a podnikatelské subjekty. Toto nařízení klade důraz na zpřesnění a definici podmínek, které jsou nezbytné pro udělení bezpečnostních certifikátů pro podnikatele. Kritickým aspektem je zahrnutí konkrétního oboru podnikání, který je považován za základní kritérium pro posouzení žádosti o přístup k citlivým informacím. Vyhláška také poskytuje šablony pro žádosti a upravuje proces oznámení jakýchkoliv změn, které mohou nastat v průběhu času a ovlivnit podmínky pro přístup k utajovaným informacím. Kromě toho, nařízení vysvětluje, jak má být postupováno v případě, že dojde ke změnám v informacích poskytnutých podnikateli, což může mít dopad na jejich oprávnění k přístupu k citlivým datům. Cílem tohoto přístupu je zajistit, aby byla správa a hodnocení těchto změn efektivní a reflektovala aktuální stav v oblasti průmyslové bezpečnosti, což je klíčové pro zachování integrity a bezpečnosti citlivých informací v obchodním prostředí.[19]

Vyhláška č 275/2022Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

Vyhláška č. 275/2022 Sb. se zaměřuje na oblast administrativní bezpečnosti a reguluje registraci utajovaných informací. Tento dokument klade důraz na vymezení a dodržování administrativních standardů a postupů, a zároveň specifikuje různé administrativní nástroje, jejichž cílem je zajištění bezpečného a efektivního využívání. Dále poskytuje podrobný náhled na procesy a metody, které jsou nezbytné pro manipulaci s utajovanými dokumenty, přičemž zohledňuje různé klasifikace těchto informací. Významnou částí vyhlášky je také popis organizační struktury a funkce centrálního registru, pomocného registru a kontrolního bodu. Tyto entity hrají klíčovou roli v regulaci a správě dokumentů, zejména v mezinárodním kontextu a v rámci vztahů ČR s cizími státy či mezinárodními organizacemi, především NATO a EU. Nařízení také stanovuje přesné postupy pro zacházení s kryptografickým materiálem, což je zásadní pro zajištění bezpečnosti a integrity UI.[20]

[19] Blíže viz *Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti*. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1083-vyhlaska-c-4052011-sb-o-prumyslove-bezpecnosti/

[20] Blíže viz *Vyhláška č.275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací*. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1088-vyhlaska-c-2752022/

Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.

Vyhláška č. 432/2011 Sb. se zaměřuje na zavedení a zajištění kryptografické ochrany utajovaných informací, přičemž poskytuje vyčerpávající směrnice pro jejich efektivní zabezpečení. Toto nařízení podrobně vysvětluje různé metody a techniky, které jsou nezbytné pro manipulaci s kryptografickými nástroji a materiály, přičemž klade zvláštní důraz na bezpečné a správné postupy při jejich využívání. Vyhláška také stanovuje kritéria pro složení specifické odborné zkoušky, která je vyžadována pro osoby pracující v oblasti kryptografické ochrany. Tuto podmínku pro práci stanovuje zákon o ochraně utajovaných informací. Zákon o ochraně utajovaných informací vyžaduje, aby každý pracovník v této oblasti prokázal svou odbornou způsobilost. Kvalifikace a schopnosti uchazečů jsou ověřovány prostřednictvím odborné zkoušky, která je hodnocena Národním úřadem pro kybernetickou a informační bezpečnost.[21] Po úspěšném složení této zkoušky je uchazečům uděleno "Osvědčení o zvláštní odborné způsobilosti" od NUKIB. Tento dokument je považován za zásadní pro ty, kteří se zabývají kryptografickou ochranou utajovaných informací, jelikož potvrzuje jejich schopnost správně a bezpečně manipulovat s kryptografickými technologiemi a materiály, což je nezbytné pro zajištění integrity a bezpečnosti citlivých informací.[22]

Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

Tato vyhláška upřesňuje podmínky pro certifikaci kryptografických prostředků a kryptografického pracoviště a stanovuje náležitosti žádosti o certifikaci. Přílohou této vyhlášky jsou konkrétní vzory žádostí o certifikaci.[23]

Vyhláška 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

Vyhláška č. 523/2005 Sb. se zaměřuje na zabezpečení informačních a komunikačních systémů, stejně jako dalších elektronických zařízení, které zpracovávají utajované informace. Tato vyhláška stanovuje přesné požadavky na prevenci úniku citlivých dat

[21] Národní úřad pro kybernetickou a informační bezpečnost dále NUKIB
[22] Blíže viz *Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací*. Dostupné z: https://www.nbu.cz/download/pravni-predpisy/432_2011.pdf
[23] Blíže viz *Vyhláška č. 525/2005 Sb o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací*. Dostupné z: https:/ /nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

z těchto systémů a zařízení. V první části vyhlášky jsou definovány klíčové pojmy, jako jsou aktivum informačního systému, hrozby a zranitelná místa, což pomáhá vytvořit jasné a konzistentní rámce pro další obsah. Druhá část se podrobně věnuje bezpečnostním aspektům informačních systémů a určuje minimální požadavky pro zajištění jejich bezpečnosti. Zahrnuje také výklad zásad bezpečnostní politiky a stanovuje požadavky na bezpečnostní dokumentaci, což je zásadní pro správné řízení a udržování bezpečnostních protokolů. Třetí část je zaměřena na komunikační systémy a popisuje postupy pro schválení bezpečnostních projektů těchto systémů. Kromě toho se zde řeší problematika kompromitujícího vyzařování z elektronických zařízení, což je identifikováno jako potenciální hrozba. Vyhláška zde také představuje koncept stínící komory, uzavřeného prostoru s ochranou proti šíření elektromagnetického, optického a akustického vyzařování. Další části se věnují bezpečnému provozování kopírovacích a zobrazovacích zařízení a stanovují podmínky pro jejich použití. Sedmá a závěrečná část upřesňuje obecnou platnost a účinnost celé vyhlášky od 1. ledna 2006, čímž zajišťuje komplexní pokrytí klíčových aspektů bezpečnosti informačních systémů. Příloha č. 3 vyhlášky se pak věnuje fyzické bezpečnosti informačních systémů a uvádí kritéria pro hodnocení těchto systémů, včetně metod autentizace a bezpečnostních ekvivalentů pro různé typy úschovných objektů. Tato část zdůrazňuje význam certifikace informačních systémů pro ochranu utajovaných informací, proces, který provádí NUKIB. Tento úřad provádí důkladné ověřování a certifikaci informačních systémů, aby zajistil, že jsou schopny účinně chránit utajované informace před neoprávněným přístupem nebo únikem.

Příloha č. 3 vyhlášky obsahuje všechna bodová ohodnocení informačních systémů, např.: „*Předmět používaný pro autentizaci musí být schválen Úřadem v rámci certifikace informačního systému. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 2“.*[24]

Tyto hodnoty jsou zcela zásadní při zpracování PFB.

[24] Příloha č. 3 bod 1.3.3. *Identifikace jménem a autentizace předmětem,* vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. [online]. [cit. 15.06.23] Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Vyhláška č. 528/2005 Sb. rozšiřuje základní pojmy ZOUI o několik klíčových definic, které jsou nezbytné pro správné pochopení a realizaci projektů v oblasti fyzické bezpečnosti. Mezi tyto pojmy patří:

- **Hranice objektu** – tento pojem se vztahuje na fyzické hranice budovy, což může zahrnovat vnější stěny budovy, oplocení nebo jinou fyzicky zřetelnou hranici, která vymezuje objekt.
- **Hranice zabezpečené oblasti nebo jednací oblasti** - specifikuje prostor, který je stavebně nebo jiným způsobem ohraničen a vymezen pro zabezpečení nebo jednání.
- **Riziko** - vyjadřuje pravděpodobnost, že se daná hrozba stane skutečností, což je klíčové pro posouzení bezpečnostních hrozeb.
- **Hrozba** - označuje možnost vyzrazení nebo zneužití utajované informace, která může nastat v důsledku porušení fyzické bezpečnosti.
- **Technický prostředek** - zahrnuje bezpečnostní prvky a zařízení, které slouží k prevenci, ztížení, detekci nebo dokumentaci jakéhokoli narušení bezpečnosti objektu, zabezpečené a jednací oblasti.
- **Úschovný objekt** - definuje trezor nebo jinou uzamykatelnou schránku, která je určena pro bezpečné uchování utajovaných informací, jak je specifikováno v příloze č. 1 vyhlášky.

Tyto pojmy jsou zásadní pro pochopení opatření v rámci fyzické bezpečnosti, zvláště při tvorbě PFB. Každý z těchto pojmů představuje specifický aspekt nebo úroveň ochrany, která je nezbytná pro komplexní zabezpečení objektů, prostor a informací proti různým hrozbám a rizikům.

V další části vyhlášky č. 528/2005 Sb. se nachází příloha, která obsahuje **tabulku pro bodové hodnocení opatření v oblasti fyzické bezpečnosti.** Tato tabulka je nezbytná pro efektivní plánování a implementaci fyzických bezpečnostních opatření. Kromě toho příloha obsahuje tabulku pro hodnocení rizik. Hodnocení rizik je založeno na kategorizaci UI, odhadu jejich množství a posouzení potenciálních důsledků, které by mohly vzniknout v případě jejich vyzrazení nebo zneužití. Další důležitý aspekt přílohy je popis hrozeb, kterým jsou utajované informace vystaveny. Součástí je i analýza zranitelností těchto informací vzhledem k identifikovaným hrozbám, a výsledné stanovení

míry rizika. Vyhláška specifikuje charakteristiku oblasti, zabezpečené oblasti a jednací oblasti, a také postupy pro ukládání utajovaných informací. Dále jsou zde uvedeny požadavky na provádění režimových opatření a systém bodového ohodnocení jednotlivých fyzických bezpečnostních opatření, přičemž je kladen důraz na dosažení co nejnižší bodové hodnoty míry zabezpečení.

V rámci vyhlášky je také popsána struktura a obsah žádosti o certifikaci technického prostředku dle ustanovení č. 11. Vyhláška stanovuje podmínky pro používání certifikovaných technických prostředků po uplynutí platnosti certifikátu a uvádí vzor certifikátu, včetně všech náležitostí, jak je vydává NBÚ. Tato část vyhlášky je klíčová pro správné používání a obnovu certifikovaných bezpečnostních zařízení v rámci zajištění fyzické bezpečnosti utajovaných informací.[25]

Mezi další hlavní prováděcí předpisy vztahující se k ochraně UI patří **Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.** V tomto nařízení se stanovují seznamy utajovaných informací v oblasti působnosti jednotlivých ministerstev a úřadů. Po bližším prozkoumání všech příloh, uvedených v tomto právním předpise, je nutné konstatovat, že není jednoduché vyhledat a určit, zda se jedná o UI a taktéž není jednoduché orientovat se v rozsahu stupňů utajení UI. Mimo jiné v úvodním ustanovení je uvedeno v § 2 „*Původce klasifikuje utajovanou informaci v rámci rozsahu stupňů utajení uvedených v přílohách č. 1 až 20 k tomuto nařízení tím stupněm utajení, který v případě jejího vyzrazení nebo zneužití odpovídá závažnosti možného způsobení újmy zájmu České republiky, anebo nevýhodnosti pro zájem České republiky ve smyslu § 3 zákona“.*[26] Rozhodnutí, kam se zařadí určitá informace, je zcela v kompetenci původce dokumentu.

3.2.2 Legislativa k ochraně utajovaných informací EU

Vstupem do Evropské unie dne 1. května 2004 se Česká republika stala plnohodnotným členem evropského společenství. Tato historická událost otevřela novou éru v rozvoji země a přinesla s sebou několik klíčových změn. Kromě politické a ekonomické integrace začala ČR plnit i některé specifické závazky vyplývající z členství v EU.

[25] Blíže viz *Vyhláška č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků.* [online]. Dostupné z: https://www.zakonyprolidi.cz
[26] Blíže viz. *Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací*. [online]. [cit. 10. 01. 24]. Dostupné z: https://www.zakonyprolidi.cz

To zahrnuje i soulad s unijní legislativou. Členství v EU přináší zemi nejen ekonomické výhody a možnosti spolupráce, ale zároveň vyžaduje dodržování určitých standardů.

Rozhodnutí Rady o bezpečnostních pravidlech na ochranu utajovaných informací EU ze dne 23. září 2013 (2013/488/EU). V tomto rozhodnutí jsou definovány základní zásady pro oblast ochrany UI v EU.

Rozhodnutí Komise ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU.

Dohoda mezi členskými státy Evropské unie zasedajícími v Radě **o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie.**

Dohody o výměně a vzájemné ochraně utajovaných informací upravují možnosti poskytování utajovaných informací mezi ČR a jiným státem a ochranu předaných utajovaných informací. Mimo jiné se v Článku 2 uvádí: *„Pro účely této dohody se „utajovanou informací" rozumí jakákoliv informace nebo materiál v jakékoli podobě, jejichž vyzrazení by mohlo v různé míře poškodit zájmy Evropské unie nebo jednoho či více členských států a které nesou jedno z níže uvedených označení stupně utajení EU nebo jiné odpovídající označení stupně utajení, jak jsou uvedena v příloze*".[27] Následně jsou v tomto článku uvedeny stupně utajení UI v EU.

TRÈS SECRET UE / EU TOP SECRET	PŘÍSNĚ TAJNÉ
SECRET UE / EU SECRET	TAJNÉ
CONFIDENTIEL UE / EU CONFIDENTIAL	DŮVĚRNÉ
RESTREINT UE / EU RESTRICTED	VYHRAZENÉ

Výše uvedené předpisy jsou uvedeny na oficiálních stránkách NBÚ.[28]

[27]Blíže viz NBÚ. *Dohoda mezi členskými státy Evropské unie zasedajícími v Radě o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie.* [online]. [cit. 11. 01. 24]. Dostupné z: https://www.nbu.cz/cs/mezinarodni-vztahy/941-mezinarodni-smlouvy-o-vymene-a-vzajemne-ochrane-utajovanych-informaci.

[28] Blíže viz NBÚ Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1077-predpisy-eu-vztahujici-se-k-ochrane-utajovanych-informaci/

3.2.3 Legislativa k ochraně utajovaných informací NATO

V březnu 1999 podepsaly na Pražském hradě přístupové listiny NATO, především pak Washingtonská smlouva, jakožto zakládající dokument Severoatlantické aliance. Od této doby je ČR plně zapojena do všech činností této Aliance a získala tak i plné bezpečnostní záruky. Již v prosinci 1999 začala pro ČR platit Dohoda o bezpečnosti informací mezi NATO a ostatními členskými státy. NATO klasifikuje utajované informace následovně:

COSMIC TOP SECRET	PŘÍSNĚ TAJNÉ
NATO SECRET	TAJNÉ
NATO CONFIDENTIAL	DŮVĚRNÉ
NATO RESTRICTED	VYHRAZENÉ

NATO ATOMAL. Jedná se o utajované informace týkající se oblasti zbraní hromadného ničení.

NATO COSMIC, přičemž toto označení je používáno na utajovaný materiál jednoznačně patřící do NATO.

Na webových stránkách NBÚ se k předpisům NATO můžeme dočíst, že nejsou volně k distribuci. Pouze, pokud by byl zájem o předpisy, které nejsou utajované a jsou označeny NATO UNCLASSIFIED, je možné podat písemnou žádost na NBÚ, na odbor administrativní a fyzické bezpečnosti. Žádost musí být zdůvodněna, případně doložena, jak informace souvisejí s činností organizace nebo podnikatele. Dále jsou na těchto stánkách uvedeny předpisy NATO. Jedná se celkem o 7 předpisů, které jsou staršího data. Například je zde **AC-35-D-2001-REV3 - DIRECTIVE ON PHYSICAL SECURITY**, která se věnuje fyzickému zabezpečení UI a fyzickou bezpečností informačních systémů. Jak je patrné už z označení, směrnice je z roku 2001. Poslední aktualizace je z roku 2020. [29] V souvislosti se zaměřením diplomové práce je uvedena také směrnice **AC-35-D-2004-REV3 – PRIMARI DIRECTIVE ON CIS SECURITY,** která je závazná pro všechny IS, které zpracovávají nebo přenášejí UI NATO. Jedná se o zásadní dokument, kterým se definují podmínky pro přenos UI v systému NATO. [30]

[29] Blíže viz NBÚ Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1077-predpisy-eu-vztahujici-se-k-ochrane-utajovanych-informaci/

[30] Blíže viz NBÚ. *Mezinárodní právní předpisy*. [online]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

NBÚ dále uvádí, že ZOUI je kompatibilní s legislativními předpisy NATO.

3.3 Výkon státní správy zabývající se ochranou utajovaných informací.

Ochrana utajovaných informací představuje klíčovou součást národní bezpečnosti, která je zajišťována prostřednictvím koordinovaného výkonu státní správy. Tento výkon se opírá o soubor činností, jež jsou prováděny státními orgány dle specifických právních norem a předpisů. Mezi primární instituce zodpovědné za ochranu utajovaných informací patří NBÚ, NÚKIB, zpravodajské služby, Ministerstvo vnitra a Policie ČR. Tyto instituce vykonávají širokou paletu činností, které začínají od preventivních opatření až po reakce na konkrétní hrozby. Spolupráce mezi MV ČR, zpravodajskými službami a NBÚ je nezbytná pro efektivní ochranu UI. Tato spolupráce zahrnuje sdílení relevantních informací, koordinaci bezpečnostních opatření a vzájemnou podporu při plnění bezpečnostních úkolů. Pravomoci zainteresovaných orgánů umožňují nejen využívání údajů z interních záznamů pro potřeby bezpečnostního hodnocení, ale také požadování informací od ostatních státních orgánů, které mohou být klíčové pro posouzení bezpečnostní situace. V rámci svých činností se tyto instituce zaměřují na šetření ve sféře personální a průmyslové bezpečnosti, což zahrnuje ověřování, zda jednotlivci a podniky dodržují normy a regulace nezbytné pro získání nebo udržení certifikátů a oprávnění v oblasti bezpečnosti. Tyto procesy jsou klíčové pro udržení integrity a bezpečnosti státních, ale i soukromých sektorů, což zahrnuje ochranu citlivých informací před neoprávněným přístupem.

Ministerstvo vnitra, Policie ČR a zpravodajské služby mají navíc povinnost informovat NBÚ o jakýchkoli zjištěních, která nasvědčují, že osoby nebo organizace již nesplňují kritéria pro držení bezpečnostních certifikátů. Tato komunikace je zásadní pro rychlou reakci na potenciální bezpečnostní rizika a udržení celkové bezpečnostní situace pod kontrolou. Tyto informace pak slouží jako základ pro rozhodnutí v bezpečnostních řízeních, která NBÚ provádí. Důležitost těchto řízení spočívá v schopnosti identifikovat a řešit potenciální hrozby pro bezpečnost státu. Tímto způsobem je zajištěna komplexní ochrana UI, což představuje nezbytný předpoklad pro zachování státní suverenity a bezpečnosti.[31]

[31] Blíže viz *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. [online]. Dostupné z: https://www.zakonyprolidi.cz

3.3.1 Národní bezpečnostní úřad

Národní bezpečnostní úřad, jako ústřední správní orgán ČR, plní zásadní roli v rámci ochrany UI a zajištění bezpečnostní způsobilosti. Jeho působnost se odvíjí od přísného dodržování českých zákonů, které určují rámec pro vykonávání státní správy v oblastech významu pro národní bezpečnost. NBÚ je pověřen nejen zajišťováním jednotné strategie ochrany UI na národní úrovni, ale také vykonáváním státního dozoru a poskytováním metodického vedení v této oblasti. Správa centrálních registrů utajovaných informací, které NBÚ zastřešuje, umožňuje efektivní sdílení a ochranu citlivých dat v rámci mezinárodních vztahů. Díky tomu může ČR plnit své závazky vyplývající z členství v EU a NATO a z mezinárodních smluv, které se týkají ochrany UI. Kromě toho NBÚ vykonává bezpečnostní řízení a státní dozor, což zahrnuje rozhodování o udělení, obnovení nebo zrušení bezpečnostních osvědčení pro fyzické osoby a podnikatele, čímž zajišťuje, že přístup k UI mají pouze oprávněné osoby.

Vznik NBÚ, datovaný 1. srpna 1998. NBÚ tak stojí v čele systému, jenž garantuje, že osoby a instituce, jimž bylo uděleno oprávnění k manipulaci s UI, splňují přísné bezpečnostní požadavky a jsou schopny vykonávat činnosti, pro které byly osvědčeny. Řízení NBÚ je svěřeno řediteli, jehož jmenování a odvolání je v pravomoci vlády ČR. Ředitel odpovídá předsedovi vlády nebo jinému vládou pověřenému členu, což zajišťuje integritu a odpovědnost vůči nejvyšším státním autoritám. Kromě toho Poslanecká sněmovna vykonává nad NBÚ kontrolní funkci prostřednictvím speciálně zřízené Stálé komise pro kontrolu činnosti NBÚ, což představuje další úroveň dohledu nad jeho činností. Tato komise má za úkol monitorovat dodržování zákonných a procedurálních pravidel, avšak bez možnosti zasahovat do personálních rozhodnutí, což zajišťuje nezávislost úřadu na politickém tlaku a možném konfliktu zájmů.

Národní bezpečnostní úřad představuje klíčový pilíř v systému národní bezpečnosti ČR, jehož úkoly a pravomoci jsou zásadní pro ochranu UI a zajištění bezpečného prostředí pro občany i stát. Jeho činnost a struktura jsou navrženy tak, aby odpovídaly moderním bezpečnostním výzvám a zároveň respektovaly demokratické principy a právní stát.

3.3.2 Národní úřad pro kybernetickou a informační bezpečnost

Za ústřední správní orgán v oblasti kybernetické bezpečnosti, včetně zabezpečení utajovaných informací v rámci informačních a komunikačních systémů a kryptografie, byl ustanoven Národní úřad pro kybernetickou a informační bezpečnost. Jeho založení bylo

provedeno dne 1. srpna 2017 na základě legislativního aktu, konkrétně zákona číslo 205/2017 Sb., kterým došlo ke změně předchozího zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně dalších souvisejících zákonů. V rámci své činnosti, jak je stanoveno zmíněným zákonem, se úřad věnuje širokému spektru aktivit. Mezi ty patří monitorování a analyzování kybernetických hrozeb.

V rámci organizační struktury NUKIB je zahrnut bezpečnostní tým, známý jako vládní CERT ČR. Tento tým úzce spolupracuje s dalšími CERT týmy a bezpečnostními skupinami CSIRT, přičemž jeho úkolem je nejen poskytování bezpečnostních informací a podpora státním orgánům, organizacím a občanům, ale také působení jako primární zdroj v oblasti kybernetické bezpečnosti. Kromě toho úřad zastřešuje činnosti spojené s veřejně regulovanou službou v rámci Evropského programu družicové navigace Galileo[32], čímž se rozšiřuje jeho působnost do dalších klíčových oblastí, u kterých je zapotřebí řešit bezpečnost. Takto široké spektrum odpovědností a činností, které NUKIB vykonává, zajišťuje komplexní přístup k zabezpečení kritické infrastruktury a informačních systémů v ČR. Zahrnuje to nejen prevenci a reakci na kybernetické útoky, ale také poskytování klíčových služeb a informací, které podporují bezpečnost a odolnost státu, jeho institucí a občanů v digitálním prostředí.[33]

3.4 Ochrana utajovaných informací

V legislativě týkající se ochrany UI je vymezeno šest základních druhů bezpečnostních opatření, které jsou nezbytné pro celkovou ochranu a bezpečný přístup k UI. Tyto opatření se navzájem doplňují a tvoří komplexní systém ochrany, který zajišťuje integritu, dostupnost a důvěrnost citlivých informací.

Personální bezpečnost se zaměřuje na zajištění důvěryhodnosti jednotlivců, kteří mají přístup k utajovaným informacím. Proces personální bezpečnosti zahrnuje pečlivý výběr a ověření osob na základě jejich minulosti, kvalifikací a dalších relevantních faktorů. Opatření v této oblasti zahrnují bezpečnostní prověrky, školení zaměřené na bezpečnostní problematiku. Pro získání přístupu k utajovaným informacím je vyžadováno Osvědčení fyzické osoby, které je vydáváno po důkladné kontrole splnění zákonem stanovených požadavků.

[32] Galileo je Evropský globální navigační družicový systém (EGNSS)
[33] Blíže viz *Národní úřad pro kybernetickou a informační bezpečnost*. [online]. Dostupné z:https: https://nukib.gov.cz/cs/o-nukib

Průmyslová bezpečnost se týká ochrany utajovaných informací v podnikatelském prostředí. Průmyslová bezpečnost zahrnuje procesy ověřování podnikatelů, auditů bezpečnostních opatření v organizaci a zajištění, že všechny procesy a systémy používané pro manipulaci s utajovanými informacemi splňují přísné bezpečnostní standardy. Podnikatel, který má ve své činnosti práci s utajovanými informacemi, musí být držitelem Osvědčení pro podnikatele. Osvědčení vydává NBÚ, a to na základě žádosti, která mimo jiné obsahuje důvod a zároveň i rozsah práce s UI.

Administrativní bezpečnost představuje soubor pravidel a postupů, které evidují tvorbu, distribuci, uchovávání a likvidaci dokumentů obsahujících utajované informace. Zahrnuje správné označování dokumentů, jejich bezpečné uchovávání - archivaci, omezení přístupu a zajištění, že veškerá manipulace s dokumenty je řádně zaznamenávána a monitorována.

Kryptografická ochrana je klíčovou složkou ochrany UI, zejména při jejich přenosu nebo ukládání v digitální formě. Používání šifrovacích a dešifrovacích technologií zajišťuje, že informace zůstanou chráněny před neoprávněným přístupem. Kryptografie hraje zásadní roli v zabezpečení komunikace, datových úložišť a přenosových kanálů.

Bezpečnost informačních a komunikačních systémů se věnuje ochraně hardwaru, softwaru a infrastruktuře, která umožňuje zpracování a přenos utajovaných informací v IS a je stanovena § 34 až § 35 zákona o ochraně UI a upřesněna v doprovodné vyhlášce, vydané NBÚ. Tato oblast se bezprostředně dotýká zabezpečení proti kybernetickým útokům, zneužití informačních systémů, kryptografické ochrany, kompromitujícímu vyzařování, datovým únikům a jiným hrozbám. Opatření jsou specifikována v bezpečnostní dokumentaci informačních systémů, kde jsou, mimo jiné, specifikovány pojmy **hardware,** který představuje procesor, paměti, terminál, datová úložiště a **software**, který představuje aplikační programy a operační systém. A dále **data,** což jsou data v zařízeních, data v databázi, vstupní a výstupní data. **Hardware, software a data** tvoří tzv. aktiva.

Fyzická bezpečnost znemožnění neoprávněného přístupu k UI za použití fyzických a technických opatření. To znamená, že použití technických a mechanických prostředků, jako jsou bezpečnostní dveře, mříže, zámky, trezory a jiné, má ochránit prostor, kde se nachází UI. Dalším úkolem fyzické bezpečnosti je zaznamenání neoprávněného přístupu. K těmto účelům slouží systémy kontroly, poplachové systémy, detektory a kamerové systémy. Fyzická bezpečnost zahrnuje i protipožární opatření.

V ZOUI je fyzické bezpečnosti věnována Hlava 5, kde jsou definovány následující pojmy.

Objekt – budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast. Objekty se dělí do kategorií, a to podle nejvyššího stupně UI informace, která se v něm zpracovává a ukládá. UI se zpracovává v objektu příslušné kategorie nebo vyšší, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba. Zákon umožňuje, aby v odůvodněných případech, a to pouze s písemným souhlasem odpovědné osoby nebo bezpečnostního ředitele, bylo možné ukládat a zpracovávat UI i objektu jiné kategorie, než je stupeň utajení zpracovávané UI, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba. V odůvodněných případech s písemným souhlasem odpovědné osoby nebo bezpečnostního ředitele je umožněno zpracovávat a ukládat UI i mimo objekt, ale taktéž za podmínky, že je zajištěno, že k UI nemá přístup neoprávněná osoba.

Zabezpečená oblast – ohraničený prostor v objektu. Zabezpečené oblasti se dělí podle nejvyššího stupně utajení utajované informace, která se v nich ukládá. Vstup do zabezpečené oblasti a výstup z ní musí být kontrolován opatřeními (ostraha, režimová opatření, technické prostředky). UI se ukládá v zabezpečené oblasti příslušné kategorie nebo vyšší a v ní popřípadě v trezoru, uzamykatelné skříni nebo jiné schránce za podmínek stanovených prováděcím právním předpisem to vyhláškou č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků. ZO se dělí do tříd podle možnosti přístupu k UI.

Třída I. Vstupem do této oblasti DOCHÁZÍ k seznámení s utajovanou informací.

Třída II. Vstupem do této oblasti NEDOCHÁZÍ k seznámení s utajovanou informací. Neoprávněná osoba může vstoupit do zabezpečené oblasti třídy II., a to s osobou, která má přístup do této ZO. V zákoně je popsána možnost změny v odůvodněných případech a s písemným souhlasem odpovědné osoby, že lze na nezbytně nutnou dobu změnit třídu I. na třídu II., pokud je zajištěno, že k UI nebude mít přístup neoprávněná osoba.

Jednací oblast - ohraničený prostor v objektu, ve kterém se pravidelně projednávají UI stupně T nebo PT. Vstup do jednací oblasti a výstup z ní musí být kontrolován opatřeními fyzické bezpečnosti, kterými podle § 27 ZOUI jsou ostraha, režimová opatření a technické prostředky.

Ostraha zabezpečené oblasti či zabezpečeného objektu, kde se nachází UI kategorie T a PT se dle ZOUI nepřetržitě zabezpečuje:

„a) Přísně tajné, nejméně 2 osobami u objektu,

b) Tajné, nejméně 1 osobou u objektu a 1 další osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno.“[34]

Mezi režimová opatření zejména patří režim vstupu a vjezdu oprávněných osob, režim vjezdu dopravních prostředků do objektu, oprávnění pro vstup do zabezpečené oblasti a jednací oblasti a dále způsob kontroly těchto oprávnění. Způsob manipulace s klíči a identifikačními prostředky, které se používají pro vstup do objektu nebo zabezpečené oblasti. Patří sem také způsob manipulace s technickými prostředky a jejich používání. Technické prostředky představují dle ZOUI mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, tísňové systémy, zařízení elektrické požární signalizace, zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů, zařízení fyzického ničení nosičů informací, zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.

K zabezpečení zabezpečených oblastí nebo objektů se používají certifikované nebo necertifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za podmínek stanovených ve vyhlášce č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků.[35]

Každá, z výše jmenovaných druhů ochrany UI, představuje nezbytnou složku v komplexním systému ochrany UI. Spolupráce a koordinace mezi jednotlivými druhy ochrany zajišťuje celkovou bezpečnost a ochranu UI a citlivých dat.[36]

3.4.1 Tempest – kompromitující vyzařování

Kompromitující vyzařování, známé také jako Tempest, je podrobně definováno a regulováno v zákoně o ochraně utajovaných informací, konkrétně ve 45. paragrafu. Tento paragraf klade důraz na ochranu utajovaných informací s různými stupni utajení - Přísně

[34] Blíže viz Zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412#cast6
[35] Tamtéž
[36] Tamtéž

tajné, Tajné, nebo Důvěrné - před únikem prostřednictvím kompromitujícího vyzařování z elektrických a elektronických zařízení, zabezpečených oblastí, nebo objektů.

V praxi každé elektrické a elektronické zařízení během svého provozu emituje určité množství elektromagnetického záření. Toto záření může být potenciálně zachyceno a analyzováno, což vede k riziku získání utajovaných informací. Kompromitující vyzařování může zahrnovat elektromagnetické, optické nebo akustické vyzařování, které je obzvláště relevantní při zobrazování informací na monitoru, zadávání dat na klávesnici, používání tiskáren, nebo ukládání dat na nosiče. Ochrana před kompromitujícím vyzařováním zahrnuje použití technologie Transient ElectroMagnetic Pulse Electronic Surveillance Technology, zkráceně TEMPEST. V rámci odborné terminologie se setkáváme s pojmy jako tempestované zařízení, což je přijímač a anténa pro monitorování elektromagnetického vyzařování. Tempestový útok pak představuje neoprávněné získání dat či samotných utajovaných informací prostřednictvím elektromagnetického pole. Tempestový počítač je počítač, který splňuje požadavky na minimalizaci kompromitujícího elektromagnetického vyzařování. Zabezpečení informačních systémů, zabezpečených oblastí a objektů, které zpracovávají utajované informace, musí být provedeno tak, aby se zabránilo úniku informací prostřednictvím kompromitujícího vyzařování. Informační systémy a osobní počítače mohou během zpracování dat emitovat záření, které je možné zachytit na vzdálenost několika desítek metrů. Moderní přístupy k zabezpečení informačních systémů zahrnují specifické normy a technologie, které se zaměřují na omezení tohoto vyzařování. Výzkum v této oblasti je neustálý a s rostoucím významem informačních technologií se stává stále důležitějším faktorem při návrhu a výrobě IT komponent.

Podle zákona musí být ochrana utajovaných informací před kompromitujícím vyzařováním, pokud je zabezpečena stínící komorou, certifikována Národním úřadem pro kybernetickou a informační bezpečnost. Toto ustanovení zdůrazňuje význam certifikace a standardizace bezpečnostních opatření v oblasti ochrany utajovaných informací.

3.4.2 Certifikace

Certifikace představuje proces, který prokazuje záruku a potvrdí, že produkt nebo služba splňuje stanovené normy a požadavky.

Certifikace hraje klíčovou roli v prokázání spolehlivosti a kvality výrobku či služby. Získání certifikátu od renomované certifikační organizace přináší řadu výhod. Rozhodně zvyšuje důvěru zákazníků, kteří mají jistotu, že produkty nebo služby splňují určité

standardy. Certifikační proces obvykle zahrnuje několik klíčových kroků. Za prvé, organizace se přihlásí k certifikaci a podstoupí předběžné hodnocení. Poté následuje hlavní certifikační audit, během kterého certifikační tým posuzuje organizaci nebo produkt ve vztahu k příslušným normám. Výsledky jsou zaznamenány v zprávě, která je základem pro udělení či odmítnutí certifikátu.

V souvislosti s ochranou UI je certifikace technických prostředků a informačních technologií naprosto nezbytná. Seznam certifikovaných technických prostředků je uveřejněn na webových stránkách NBÚ. Doba, po kterou platí certifikát je stanovena na 5 let. Technický prostředek, který je použit k ochraně UI musí být pořízen v době platnosti certifikátu, ale je možné jej používat i po uplynutí platnosti certifikátu. Podmínkou je však jeho funkčnost, která se pravidelně ověřuje funkční zkouškou. O této zkoušce je nutné vypracovat protokol, který je ukládám v Projektu fyzické bezpečnosti.

Novelou vyhlášky č. 528/2005 Sb., došlo ke zrušení certifikace technických prostředků, které nejsou hodnoceny a zařazovány do tříd nebo stupňů. Jedná se o speciální televizní systémy, zařízení elektrické požární signalizace, zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů, zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.

Národní bezpečnostní úřad vydává certifikáty na tyto technické prostředky:

- mechanické zábranné prostředky
- elektrická zámková zařízení a systémy pro kontrolu vstupů
- zařízení elektrické zabezpečovací signalizace
- tísňové systémy
- zařízení fyzického ničení nosičů informací nebo dat

Certifikace uvedených druhů technických prostředků pro ochranu utajovaných informací se řídí pravidly dokumentu „Certifikační postup NBÚ“, který je uveden na webových stránkách NBÚ.

Obdobné je to i u informačních systémů. Certifikát informačního systému vydává Národní úřad pro kybernetickou a informační bezpečnost a ten také stanovuje jeho platnost pro daný stupeň utajení. Pro utajovanou informaci stupně Tajné a Přísně tajné je platnost certifikátu určena nejdéle na 2 roky. Pokud je tento systém používán i po skončení platnosti

certifikátu je nutné znovu požádat NUKIB o jeho certifikaci. Toto platí i o certifikaci stínících komor.

Náležitosti certifikátu technických prostředků dle zákona o ochraně UI:

„a) *evidenční číslo certifikátu,*

b) *název a typové označení technického prostředku,*

c) *identifikaci výrobce technického prostředku obchodní firmou (dále jen "firma") nebo názvem, identifikačním číslem osoby (dále jen „identifikační číslo“) a sídlem, jde-li o právnickou osobu, nebo jménem, příjmením, rodným číslem a místem trvalého pobytu, jde-li o osobu fyzickou,*

d) *identifikaci držitele certifikátu technického prostředku podle písmene c),*

e) *hodnocení technického prostředku,*

f) *datum vydání a dobu platnosti certifikátu a*

g) *otisk úředního razítka a podpis oprávněného zástupce Úřadu; otisk úředního razítka se nevyžaduje, byl-li certifikát vydán v elektronické podobě*.“[37]

K provedení certifikace informačního systému žadatel předloží následující podklady

„a) bezpečnostní politiku informačního systému a výsledky analýzy rizik,

b) návrh bezpečnosti informačního systému,

c) sadu testů bezpečnosti informačního systému, jejich popis a popis výsledků testování,

d) bezpečnostní provozní dokumentaci informačního systému,

e) popis bezpečnosti vývojového prostředí a

f) další podklady nezbytné k certifikaci informačního systému, vyplývající ze specifikace informačního systému.“[38]

Bezpečnostní dokumentace informačního systému se skládá z projektové bezpečnostní dokumentace, obsahující bezpečnostní politiku informačního systému, výsledky analýzy rizik, návrh bezpečnosti informačního systému zajišťující splnění bezpečnostní politiky systému a také dokumentaci k testům bezpečnosti. Pro zajištění bezpečnosti informačního

[37] Blíže *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti*. [online]. [cit. 6.10.23] Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[38] Blíže *Vyhláška č. 523/2005 Sb o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.* Dostupné z: https:/ /nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

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.

V budoucnosti lze očekávat, že certifikace bude hrát ještě větší roli, zejména v oblastech jako kybernetická bezpečnost. Rozvoj nových technologií a globalizace pravděpodobně povede k vytváření nových certifikací, které budou odpovídat dynamickým potřebám současného světa.

3.5 Analýza současného stavu ochrany utajovaných informací

Tato kapitola analyzuje současný stav ochrany utajovaných informací a zaměřuje se na identifikaci rizik v různých klíčových oblastech.

Legislativně je problematika ochrany utajovaných informací dostatečně zabezpečena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, který velmi dobře doplňují Vyhlášky NBÚ. Všechny ochrany, vyplývající ze zákona se navzájem prolínají a velmi dobře doplňují.

Rizika ochrany UI, vidí autor spíše v jednotlivých ochranách. Například v personální oblasti se rizika týkají nedostatečného prověřování zaměstnanců, a porušování povinností v důsledku nedostatečného školení. Administrativní rizika zahrnují chybné stanovení stupně utajení a nevhodné postupy při odtajňování, neevidované a neautorizované kopírování na neověřených zařízeních. V komunikační a informační oblasti mohou rizika zahrnovat nebezpečné zpracování informací mimo zabezpečené oblasti, neoprávněný přístup k certifikovaným systémům a nedostatečné zacházení s utajovanými informacemi. V oblasti fyzické ochrany jsou rizika spojená s nedostatečnou nebo chybně vytvořenou analýzou rizik a nesprávným nastavením režimových opatření. Společným prvkem v těchto rizikových faktorech je lidský faktor, neboť nesprávné jednání osoby v dané roli, představuje významné riziko pro narušení ochrany informací.

Klíčové je, nejen dodržování předpisů, ale také pravidelná kontrola a důsledné uplatňování bezpečnostních opatření. Význam kontinuálního vzdělávání zaměstnanců, pravidelného monitorování jejich činnosti a implementace účinných opatření vedoucích k minimalizaci lidských chyb je nezbytnou součástí ochrany utajovaných informací a posílení celkového bezpečnostního rámce organizace.

3.6 Přehled studií ochrany utajovaných informací v ČR a zahraničí

Autor při vyhledávání zahraničních studií, které by mohl, porovnat se svou diplomovou prací narážel na obtížnost vyhledat jakékoli informace o ochraně utajovaných informací v zahraničí. Je logické, že každý stát si chrání vybrané informace. Nicméně autor se domnívá, že utajování některých informací, které se jeví pouze spíše jako citlivé informace, může být způsobeno také tlakem či příkladem Severoatlantické aliance. K této domněnce autora přivádí fakt, že sama Severoatlantická aliance nezveřejňuje své předpisy, a to ani ty, které jsou označeny jako neutajované čili Unclassified. Autor při svém bádání vyhledal studii ***„Návrh zákona o ochraně utajovaných informací - studie a připomínky“***. Jedná se o velmi zajímavou studii k úpravě utajovaných skutečností v historii, v zahraničí a rozbor návrhu nového zákona o utajovaných informacích ve verzi z prosince 2003, která byla zpracována pro Transparency International Czech Republic v roce 2004 Mgr. Ing. Helenou Svatošovou, a která byla předložena Legislativní radě vlády. Mimo jiné je v ní uvedeno: „*Na podobu zákona má ovšem rovněž fakticky vliv bezpečnostní politika NATO, resp. její klíčové dokumenty. Vzhledem k jejich faktickému spíše neprávnímu působení však tento vztah nelze v žádném případě považovat za ekvivalentní působení závazků ČR v oblasti výše uvedených mezinárodních smluv o lidských právech. Ta obsahuje vůči státu závazek utajovat všechny informace, které samo NATO na základě své bezpečnostní politiky označí za utajené. Zásadní obtíží přitom je, že základní dokumenty této politiky – C-M(55)15(Final) z roku 1955 a C- M(2002)49 z června 2002 nemá veřejnost k dispozici. Ačkoli ani jeden z dokumentů není klasifikován jako utajovaná skutečnost, NATO je od padesátých let odmítá zpřístupnit veřejnosti a instruuje i členské státy, aby je, v rozporu se závazky států, v oblasti práva na informace občanům neposkytovaly.*[39]

Další studií, která se autorovi jeví, jako zajímavá je ***„Security Classified and Controlled Information: History, Status, and Emerging Management Issues“***.[40]

Autor studie poukazuje na nutnost více utajovat některé informace v souvislosti se životem po teroristickém útoku 11. září 2001. Dále zde uvádí, že:
„*V červenci 2005 deník New York Times redakčně poznamenal, že "Bushova administrativa“ utajuje dokumenty, které mají být utajeny před veřejností, rychlostí 125 % za minutu.*

[39] ***Návrh zákona o ochraně utajovaných informací - studie a připomínky, Mgr. Ing. Helena Svatošová Iuridicum Remedium, o.s.*** [online]. [cit. 10.01.24]. Dostupné z: https: //www.iure.org/sites/default/files/article/downloads/07navrh_zakona_o_ochrane_utajovanych_informaci.pdf
[40] ***Security Classified and Controlled Information: History, Status, and Emerging Management Issues,*** Harold C. Relyea Specialist in American National Government, Government and Finance Division. [online]. [cit. 10.01.24]. Dostupné z: https: https://apps.dtic.mil/sti/pdfs/ADA468627.pdf

Tento krok směrem k většímu utajení," pokračoval deník, "téměř zdvojnásobil počet utajovaných dokumentů.“

Autor diplomové práce se domnívá, že obě studie poukazují na snahu utajovat informace více, než zákonná norma požaduje, ale také na fakt, co k takové činnosti úřady či státy vede. Tím je jednoznačně obava o bezpečnost státu či organizace.

3.7 Shrnutí hlavních zjištění

Ochrana utajovaných informací v ČR je podrobně upravena v Zákoně o ochraně utajovaných informací a dalších prováděcích předpisech, vydaných Národním bezpečnostním úřadem a Národním úřadem pro kybernetickou bezpečnost. Tyto dva jmenované úřady také provádí dohled nad dodržováním těchto zákonných norem.

Ochrana utajovaných informací má v podstatě charakter ochrany všech informací. Pro mnoho firem a státních organizací představují informace nesmírnou hodnotu, a jakékoli ohrožení či ztráta může mít pro tyto subjekty nepředvídatelné důsledky.

Práce je strukturována s cílem podrobně vysvětlit základní pojmy v oblasti ochrany utajovaných informací a jejich právního kontextu. Začala od nejzákladnějších pojmů, jako je definice informace a její zakotvení v různých právních předpisech. Dále rozvinula koncept ochrany utajovaných informací, detailně popisujíc, co ochrana utajovaných informací obnáší a jaké formy zabezpečení jsou v této oblasti používány. Tento postup je zvolen ve snaze poukázat na různé možnosti vnímání potřeb v oblasti ochrany utajovaných informací. Z důvodu zaměření diplomové práce je pozornost věnována na fyzickou ochranu a ochranu informačních systémů.

Závěrem podrobné analýzy zákonných předpisů a způsobů ochrany utajovaných informací lze konstatovat, že při dodržování všech zákonem definovaných podmínek jsou vytvořeny dostatečné předpoklady, pro co nejbezpečnější nakládání s utajovanou informací. Ochrana UI je zajištěna na srovnatelné úrovni jako v EU a NATO.

4 Analytická část práce

4.1 Výzkumné otázky

1. Je legislativní vymezení ochrany utajované informace dostatečné?
2. Je možné, dle současně platných zákonných nařízení dostatečně ochránit utajované informace?
3. Je možné, podle současné platné legislativy, vypracovat kvalitní Projekt fyzické bezpečnosti?

4.2 Stanovení hypotéz

S využitím stávající legislativy a všech dostupných informací potřebných k vypracování analýzy rizik (aktiva, hrozby, rizika) je možné vypracovat Projekt fyzické bezpečnosti, tak aby ochrana utajovaných informací splňovala zákonné požadavky.

5 Projekt fyzické bezpečnosti

Všem organizacím a právním subjektům, kteří nakládají s utajovanou informací jakékoli kategorie je uložena povinnost zpracovat Projekt fyzické bezpečnosti. V ZOUI je stanovena jeho struktura.

„*Projekt fyzické bezpečnosti v případech, kdy se v objektu nacházejí zabezpečené oblasti kategorie* ***Přísně tajné, Tajné*** *nebo* ***Důvěrné****, obsahuje:*

a) určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí,

b) vyhodnocení rizik,

c) způsob použití opatření fyzické bezpečnosti,

d) provozní řád objektu a

e) plán zabezpečení objektu a zabezpečených oblastí v krizových situacích“.[41]

5.1 Analýza rizik IS

Analýza rizik se zaměřuje na odhalení a pochopení potenciálních nebezpečí. Tento proces zahrnuje identifikaci zdrojů rizik, jejich pozitivních a negativních dopadů a pravděpodobnosti výskytu těchto dopadů.[42] Během analýzy jsou zkoumány faktory, které ovlivňují jak následky, tak jejich pravděpodobnost. Rizika jsou pečlivě analyzována prostřednictvím spojení mezi očekávanými důsledky a pravděpodobností jejich výskytu.

Vzhledem k tomu, že je v této práci zvolen modelový a výhradně fiktivní objekt, není možné reálně vypracovat precizní analýzu rizik. Autor zvolil variantu, kdy je popsána podstata analýzy rizik a celý proces je veden spíše v teoretické rovině. Většinou jsou brána v úvahu již existující opatření, která mohou ovlivnit průběh rizikových událostí. Pro tuto část si autor vybral analýzu rizik informačního systému.

Aktivem, v rámci diplomové práce, je utajovaná informace. Jedná se o UI kategorie T a PT. V případě vyzrazení, zničení či znehodnocení UI by vznikla vážná až mimořádně

[41] Zákon č. 148/1998 Sb. o ochraně utajovaných skutečností. [online]. [cit. 10.12.23]. Dostupné z:https://www. zakonyprolidi.cz/cs/1998-148/zneni-0#f1877594

[42] ŠEBESTA, Václav.; ŠTVERKA, Václav.; STEINER, František.; ŠEBESTOVÁ, Marie. Systémy řízení bezpečnosti informací, Část 3: Směrnice pro management rizik bezpečnosti informací podle BS 7799-3:2005 s komentářem k managementu rizik v ISMS. Praha : Český normalizační institut, 2007. s 85 a dále.

vážná újma zájmům ČR. Jedná se o možné narušení či ohrožení svrchovanosti, územní celistvosti nebo demokratických základů ČR či dokonce možné rozsáhlé ztráty na lidských životech.

V případě informačních systémů jsou primárním aktivem taktéž utajované informace, dále procesy, jejichž narušení by mělo za následek neschopnost organizace plnit úkoly práce s utajovanou informací. Analýza informačních systémů pracuje i s podpůrnými aktivy, na kterých jsou závislá výše jmenované primární aktiva. Jedná se hlavně o HW a SW. Klíčovou charakteristikou aktiva je jeho hodnota, která může být stanovena, dle výše újmy, která by mohla vzniknou. Norma ČSN EN ISO/IEC 27002[43] dává jako příklad klasifikačního schématu čtyřstupňovou klasifikaci, kdy jednotlivé úrovně jsou popsány takto:

- prozrazení nezpůsobí žádné škody;
- prozrazení způsobí menší nepříjemnosti nebo menší provozní obtíže;
- prozrazení má významný krátkodobý dopad na provozní činnosti nebo taktické cíle;
- prozrazení má vážný dopad na dlouhodobé strategické cíle nebo vystavuje riziku pokračování organizace v činnosti.

5.1.1 Stanovení hrozeb a zranitelnost

Hrozby představují události či okolnosti, které mohou negativně ovlivnit bezpečnost utajovaných informací v informačních systémech, a jejich dopad může vést ke vzniku škod a újmy. Tyto hrozby mohou mít různý původ, od přírodních katastrof, přes chyby v software, až po úmyslné kybernetické útoky. Identifikace hrozeb zahrnuje proces rozpoznání potenciálních zdrojů ohrožení, které mohou zasáhnout aktiva IS a mít negativní dopad. Tento proces je klíčový pro efektivní hodnocení a řízení rizik v IS. Hodnocení hrozeb spočívá v analýze a určení pravděpodobnosti výskytu jednotlivých hrozeb a potenciálního dopadu na aktiva. Toto hodnocení umožňuje organizacím stanovovat priority k hrozbám a určit, kterým hrozbám je třeba věnovat největší pozornost. Příklady těchto hrozeb zahrnují:

Kybernetické útoky:

- Malware: škodlivý software, včetně virů, červů, trojských koní a ransomwaru, který může poškodit nebo ukrást data.

[43] ČSN EN ISO/IEC 27002 (369798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti. [online]. [cit. 10.1.24]. Dostupné z https://www.technicke-normy-csn.cz/csn-en-iso-iec-27002-369798-249194.html

- Phishing: podvodné e-maily nebo zprávy, které se snaží získat citlivé informace, jako jsou hesla nebo finanční údaje.
- DDoS útoky (Distributed Denial of Service): útoky zaměřené na přetížení a znefunkčnění webových služeb nebo sítí.

Fyzické hrozby:

- Požár nebo povodně: přírodní katastrofy, které mohou způsobit poškození hardwaru a ztrátu dat.
- Krádeže nebo vandalismus: neoprávněný fyzický přístup k zařízením, který může vést ke krádeži nebo poškození zařízení a dat.

Lidské faktory:

- Neoprávněný přístup nebo zneužití oprávnění: zaměstnanci nebo externí uživatelé, kteří zneužívají svá oprávnění k přístupu k citlivým informacím nebo systémům.
- Chybné ovládání nebo chyby uživatelů: omyly uživatelů, které mohou vést k nesprávnému nakládání s daty nebo k narušení systémů.

Technologické problémy:

- Zastaralý software nebo hardware: nedostatečně aktualizované systémy mohou obsahovat zranitelnosti, které jsou náchylné k útokům.
- Systémové selhání: poruchy hardwaru nebo softwaru, které mohou vést k přerušení provozu nebo ke ztrátě dat.

Organizační a procesní nedostatky:

- Nedostatečné zabezpečení politik a postupů: slabé nebo chybějící bezpečnostní politiky a postupy, které nezajišťují dostatečnou ochranu informací.
- Nedostatečné školení zaměstnanců: zaměstnanci nejsou dostatečně proškoleni v oblasti kybernetické bezpečnosti a mohou tak nevědomky přispět k bezpečnostním incidentům.

Právní a regulatorní rizika:

- Porušení zákonných předpisů: nedodržení zákonů a předpisů souvisejících s ochranou dat může vést k právním problémům a pokutám.

Každá z těchto hrozeb představuje specifické riziko pro informační systémy a vyžaduje odpovídající řízení a zabezpečovací opatření pro jejich zmírnění.

Zranitelnosti v IS představují slabá místa nebo nedostatky, které mohou být zneužity hrozbami k napadení nebo poškození aktiv. Identifikace zranitelností zahrnuje analýzu a rozpoznání slabých míst v systémech, procesech nebo politikách. Kritéria pro hodnocení

zranitelností jsou klíčová pro identifikaci a posouzení slabých míst v informačních systémech, které by mohly být zneužity potenciálními hrozbami. Tato kritéria umožňují organizacím systematicky analyzovat a prioritizovat zranitelnosti, což je nezbytné pro efektivní řízení rizik.

- **Závažnost zranitelnosti**: hodnocení závažnosti zranitelnosti zahrnuje určení míry, do jaké by mohla být zranitelnost využita k způsobení škody. Závažnost se obvykle hodnotí jako nízká, střední nebo vysoká, a závisí na potenciálním dopadu na důvěrnost, integritu a dostupnost informačních aktiv.
- **Snadnost zneužití**: hodnocení, jak snadné je zranitelnost využít. Některé zranitelnosti mohou vyžadovat vysokou úroveň technické expertízy nebo specifické podmínky pro jejich využití, zatímco jiné mohou být snadno zneužitelné i méně zkušenými útočníky.
- **Exploatační potenciál**: souvisí s tím, zda již existují známé metody nebo nástroje, které mohou využít danou zranitelnost. Zranitelnosti, pro které jsou již k dispozici veřejně dostupné exploit kódy, jsou považovány za vysoce rizikové.
- **Míra expozice**: týká se toho, do jaké míry je zranitelný systém přístupný potenciálním útočníkům. Zranitelnosti, které jsou přístupné z internetu, mají obvykle vyšší hodnocení expozice než ty, které vyžadují fyzický přístup.

5.1.2 Vyhodnocení rizik

Hodnocení rizik je proces, při kterém se kombinují hodnocení hrozeb a zranitelností, aby se určilo celkové riziko, kterému IS čelí. Tento proces zahrnuje určení pravděpodobnosti výskytu hrozby a odhad dopadu na aktiva, pokud by došlo k realizaci hrozby. Hodnocení rizik umožňuje organizacím pochopit, jaká rizika jsou nejvýznamnější a jak s nimi naložit. Varianty zvládání rizik zahrnují přijetí opatření k eliminaci nebo snížení rizika na akceptovatelnou úroveň. Tyto varianty mohou zahrnovat prevenci, převzetí, zmírnění nebo přenesení rizika. Přijetí opatření, jako jsou zlepšení bezpečnostních protokolů, aktualizace software, zavedení zálohovacích a obnovovacích procesů a školení zaměstnanců, může pomoci minimalizovat rizika.

Kritéria akceptovatelnosti rizika určují, do jaké míry je organizace ochotna přijmout riziko, aniž by podnikla další opatření k jeho snížení. Tato kritéria jsou závislá na povaze organizace, jejím regulatorním prostředí a dalších faktorech, jako je důležitost a hodnota aktiv, která jsou ohrožena. Akceptace rizika nastává, když organizace rozhodne, že potenciální dopad a pravděpodobnost výskytu hrozby jsou dostatečně nízké, aby byly

přijatelné. Tato volba se často používá, když náklady na zmírnění rizika převyšují potenciální ztráty způsobené realizací rizika. Akceptace rizika by měla být informovaným rozhodnutím a vždy zahrnovat plán sledování a přehodnocení rizika.

Snížení rizika zahrnuje implementaci opatření k omezení pravděpodobnosti výskytu hrozby nebo minimalizaci jejího dopadu na aktiva. Zahrnuje to opatření, jako jsou zlepšení bezpečnostních postupů, aktualizace software a hardware, školení zaměstnanců a zlepšení fyzické bezpečnosti. Cílem je snížit riziko na úroveň, která je pro organizaci akceptovatelná.

Vyhnutí se riziku je rozhodnutí zcela eliminovat riziko, obvykle změnou procesů, způsobů provozu nebo dokonce zastavením činností, které riziko představují. Tato strategie je obvykle používána, když riziko představuje potenciální hrozbu, která by mohla mít katastrofální následky, nebo když není možné riziko efektivně zmírnit.

Sledování rizika znamená pravidelné monitorování identifikovaných rizik, aby bylo možné rychle reagovat na jakékoli změny v jejich úrovni nebo v kontextu, který by mohl ovlivnit jejich dopad nebo pravděpodobnost. Tato strategie zahrnuje udržování stálého přehledu o bezpečnostním prostředí a zajišťuje, že opatření pro řízení rizik jsou stále účinná a relevantní.

Rozpoznání a efektivní řízení hrozeb, zranitelností a rizik je zásadní pro zajištění bezpečnosti informačních systémů a ochrany utajovaných informací. Procesy identifikace, hodnocení a zvládání rizik jsou klíčové pro udržení integrity, důvěrnosti a dostupnosti informací v digitálním prostředí.

Stanovená míra rizika ochrany utajované informace je hodnocena pomocí matice hodnocení rizik, ve které jsou zohledněny velikost vzniklé újmy pro zájmy ČR neoprávněnou manipulací s utajovanou informací, dále velikostí existující hrozby, která byla identifikována v místě hodnoceného objektu, a zranitelností fyzické bezpečnosti a zranitelností informačního systému. Postup při sestavování a hodnocení rizik je v utvoření přehledu, kde jsou identifikovány hrozby, dále přehledu zranitelných míst a pravděpodobnosti výskytu hrozby.

S ohledem na další skutečnost, že státní organizace nakládá, manipuluje, projednává a také ukládá UI v kategorii TAJNÉ a PŘÍSNĚ TAJNÉ, kdy je stanovena **vážná újma a mimořádně vážná** újma je analýzou rizik stanoveno **RIZIKO VELKÉ.**

5.2 Deskripce modelového informačního systému

V této kapitole je představen návrh informačního systému, který je navržen pro bezpečnou správu utajovaných informací do stupně utajení TAJNÉ a je používán fiktivní organizací. Informační systém, má za cíl poskytnout efektivní a bezpečné informační prostředí pro ukládání, správu, sdílení a přenášení utajovaných informací. Modelový případ vychází z reálií, kdy státní organizace čelí potřebě stále rostoucího objemu utajovaných informací a potřebuje sofistikované nástroje pro jejich správu. Informační systém vychází z potřeby efektivního a bezpečného systému, který splňuje požadavky státní organizace.

Hlavní funkce zahrnují uživatelské účty s příslušnými oprávněními, systém pro nahrávání a správu dokumentů a řízení přístupových práv. Systém je koncipován s důrazem na bezpečnost, efektivitu a uživatelskou přívětivost. Informační systém je navržen tak, aby byl postupně budován jako jednoduchá počítačová síť, která je tvořená jednotlivými síťovými komponentami umístěná v zabezpečeném objektu a tvořila samostatný logický celek. Tento informační systém nebude žádným způsobem propojen s jinými systémy organizace a bude zcela oddělen od okolního informačního prostředí čili internetu.

Informační systém je rozdělen do funkčních komponent, z nichž každá má specifický účel. Modul pro správu uživatelských účtů umožňuje registraci a správu rolí. Modul pro nahrávání a správu dokumentů poskytuje uživatelům prostředky pro efektivní práci s utajovanými informacemi. Řízení přístupových práv zajišťuje bezpečnost dat a kontroluje oprávněný přístup. Informační systém je koncipován jako jednodoménový model. Z důvodu, udržitelnosti a podpory informačního systému jsou jednotlivé hardwarové komponenty pořizovány od renomovaných výrobců, jako jsou Microsoft, IBM, Cisco. Na serverech je používán operační systém Windows Server 2019 a na pracovních stanicích operační systém Windows 10. Informační systém je navržen jako dvoučlenný skládající se z datového centra určeného k ukládání utajovaných informací a koncových pracovních stanic, jež jsou určeny k zobrazování a zpracovávání utajovaných informací. Na pracovních stanicích, vyjma možnosti ukládání na externí zařízení, nebude technickými opatřeními povolena možnost ukládání na interní paměťová média. Pro zajištění bezpečnosti a spolehlivosti informačního systému jsou definovány technické požadavky. Ty zahrnují šifrování citlivých dat, dvoufaktorovou autentizaci pro uživatele a monitorování aktivit pro prevenci bezpečnostních hrozeb. Bezpečnostní opatření zahrnují pravidelné kontroly přístupových práv a uživatelských aktivit pro udržení integrity a důvěrnosti dat. Synchronizace uživatelských účtů je řešena pomocí Active Directory. Systém obsahuje

funkce pro správu a údržbu, jako jsou automatické zálohování a obnova dat. Bezpečnost informačního systému je řešena pomocí standardních bezpečnostních nástrojů, kterými jsou firewall, antivirové nástroje, nástroje pro ochranu výstupů na externí zařízení a analýza chování uživatelů. Dále, je v informačním systému provozován nástroj pro sběr a vyhodnocování auditních záznamů SIEM.

V rámci provozu informačního systému je zpracována bezpečnostní dokumentace a provozní směrnice pro správce IS a uživatele IS. Součástí procesu bezpečnosti jsou i pravidelná každoroční školení uživatelů z bezpečnosti IS. Součástí dokumentace je i plán rozvoje informačního systému a pro udržení systému aktuálního jsou naplánovány a prováděny aktualizace s opravami.

5.3 Deskripce modelového objektu

Objekt, který je určen pro zpracování, ukládání a projednávání UI kategorie tajné a přísně tajné se nachází v oploceném areálu na území hlavního města ČR. Objekt je majetkem státu a je výhradně používán státní správou. Celý areál fiktivního objektu je zařazen do kategorie PT. Zařazení objektu je provedeno dle nejvyššího stupně utajení ukládaných nebo projednávaných informací.

Jedná se o areál, který je situován v městské zástavbě. Okolní zástavba je tvořena rodinnými domy, které jsou na oplocených samostatných pozemcích. Okolní zástavba je od perimetru vzdálena nejméně 15 m po všech stranách. Jedná se běžnou městskou zástavbu, která je majetkem soukromých fyzických a právnických osob.

Celý areál je po celém obvodu oplocen. Perimetr je ohraničený zděným plotem s výškou 2 m a osazen speciálním kamerovým systémem[44] s osvětlením. Podle vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti je hodnocení perimetru typ 1.

„*Fyzické bariéře typu 1 odpovídá oplocení bez speciálních bezpečnostních požadavků. Účelem tohoto oplocení je vyznačit hranice a zajistit minimální úroveň odrazení nebo odolnosti. Fyzická bariéra typu 1 může být tvořena jakýmkoliv typem materiálu*.“[45]

SS10 = 1 bod

[44] Speciální televizní systémy (CCTV) Closed-circuit television, uzavřený televizní okruh, je instalován na sledování prostoru, zobrazení záběrů na monitoru a k archivaci záběrů.
[45] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci*. [online]. [cit. 10.12.23]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

Bezpečnostní osvětlení perimetru:

„Požadavky na instalaci bezpečnostního osvětlení vyplývají například z požadavků speciálního televizního systému na perimetru.“

SS14 = 2 body

Vyšší bodové hodnocení perimetru není možné, a to i přes osazení a kamerovým systémem. Důvodem je výška oplocení, která je 2 m. Pro vyšší bodové ohodnocení je stanovena minimální výška oplocení 2.15 cm.

Vstup do areálu je řešen vstupní brankou v oplocení, která je osazena systémem kontroly vstupu[46], to znamená, že vstup je možný pouze pomocí vstupní identifikační karty. Pro vjezd vozidel je vybudován vjezd, který je osazen bránou, která je taktéž napojena na elektronický systém kontroly vjezdu. Oba vstupy jsou nepřetržitě monitorovány kamerami.

„*Kontrola vstupu ve všech přístupových bodech perimetru.*“[47]

SS11 = 1 bod

Tato hodnota je maximální možná a je v souladu se zákonnou podmínkou, kdy v objektu kategorie Přísně tajné musí být provedena kontrola vstupu.

V areálu vykonávají ostrahu příslušníci ozbrojených sborů. Ostraha je vykonávána nepřetržitě čili režim 24/7. Stálé stanoviště ostrahy je umístěno za vstupními dveřmi do objektu. Na tomto stanovišti s nepřetržitou přítomností příslušníka je vyvedeno výstupní hlášení zařízení elektrické zabezpečovací signalizace[48] a speciálního televizního systému.

Výkon ostrahy je prováděn minimálně třemi příslušníky, kteří mají povinnost vykonávat nepravidelné obchůzky areálu v intervalu ne větším než 2 hodiny. Přesné intervaly kontrolních obchůzek jsou uvedeny v interních pravidlech pro fyzickou ostrahu areálu.

„*Ostrahu typu 5 zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávaná způsobem nepravidelných obchůzek.*

[46] Elektronická kontrola vstupu je určena k identifikaci vstupujících osob a k zamezení vstupu neoprávněné osobě. Dále jen EKV.

[47] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci*. [online]. [cit. 11.12.23]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

[48] Elektrická zabezpečovací signalizace byla označována jako EZS. V současné době je taktéž známa jako poplachové zabezpečovací a tísňové systémy, které se uvádějí pod zkratkou PZTS. V současné době se používá nové i starší označení. V aktuálním znění Vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, je stále uvedeno pro elektrickou zabezpečovací signalizaci označení EZS. Z tohoto důvodu je v DP uvedena zkratka EZS.

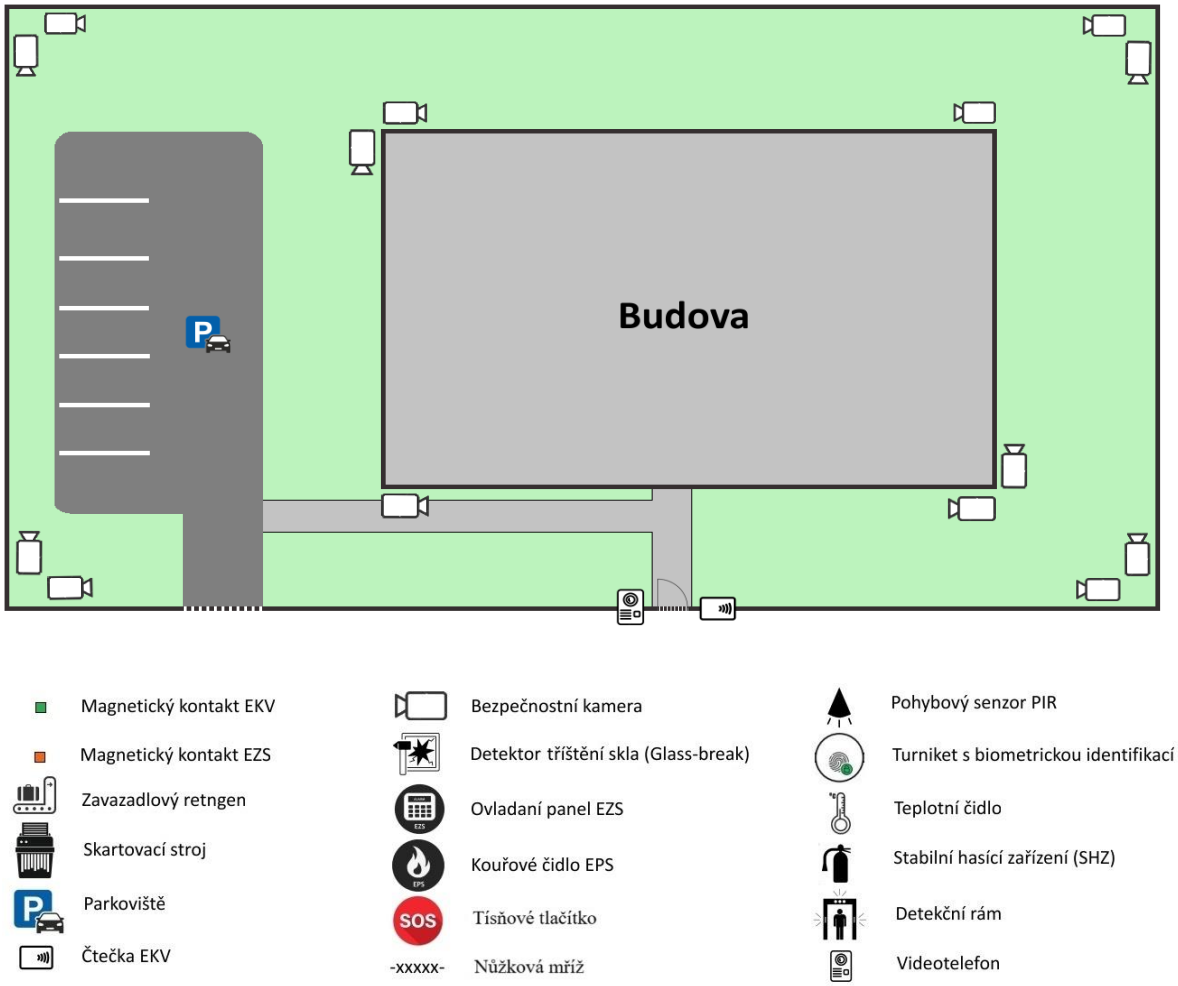
Ostraha provádí obchůzky po náhodně vybraných trasách v náhodných intervalech ne větších než 2 hodiny. V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy".[49]

SS8 = 5 bodů

Budova má suterénní prostory a další 3 nad podlažní patra – označení 1. NP, 2. NP a 3. NP. Je postavena z cihel – tloušťka obvodových zdí je 180 mm. Všechny vnitřní příčky jsou taktéž z cihel o šíři 150 mm. Výška 1.NP nad okolním terénem je 1800 mm, výška 2. NP je 5500 mm a výška 3. NP je 9000 mm nad okolním terénem. Střecha je rovná se sklonem 5°s přesahem nad budovou 40 cm. Ze střechy nelze jednoduše proniknout do nižších pater, ani za pomoci hromosvodů a jiných stavebních a technických prvků. V bezprostřední blízkosti objektu nejsou stromy a ani jiné stavby, kterých by bylo možné využít ke vniknutí do objektu.

[49] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci*. [online]. [cit. 11.12.23]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

Obrázek č. 1 - Schéma modelového areálu



Zdroj: vlastní zpracování

Vchod do budovy je osazen vchodovými dvoukřídlými dveřmi. Vzhledem k tomu, že objekt je zařazen do kategorie Přísně tajné jsou po obvodu budovy instalovány bezpečnostní kamery a plášťová ochrana.

„*Instalace zařízení elektrické zabezpečovací signalizace typ 3* je *realizovaná v zabezpečené oblasti v rozsahu:*
a) *prostorová ochrana,*
b) *plášťová ochrana,*
c) *tísňový systém nebo speciální televizní systém snímající nepřetržitě průlezné otvory zabezpečené oblasti“.*[50]

SS92 = 3 body

[50] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* [online]. [cit. 11.01.24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

U stanoviště ostrahy je vystaven prostor pro návštěvy. Ten je vybaven zařízením určeným k vyhledávání nebezpečných látek nebo předmětů. Jedná se o detektor kovu a rentgenový přístroj pro kontrolu zavazadel. Toto zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů je ze zákona povinné u objektů kategorie Přísně tajné anebo jednací oblasti, ve které se pravidelně projednávají utajované informace stupně utajení Přísně tajné. V případě návštěv se uplatňuje vstup pouze s doprovodem odpovědného zaměstnance. Návštěva musí být zaevidována v systému návštěv, povolena odpovědným pracovníkem případně bezpečnostním ředitelem a musí být doprovázena po celou dobu.

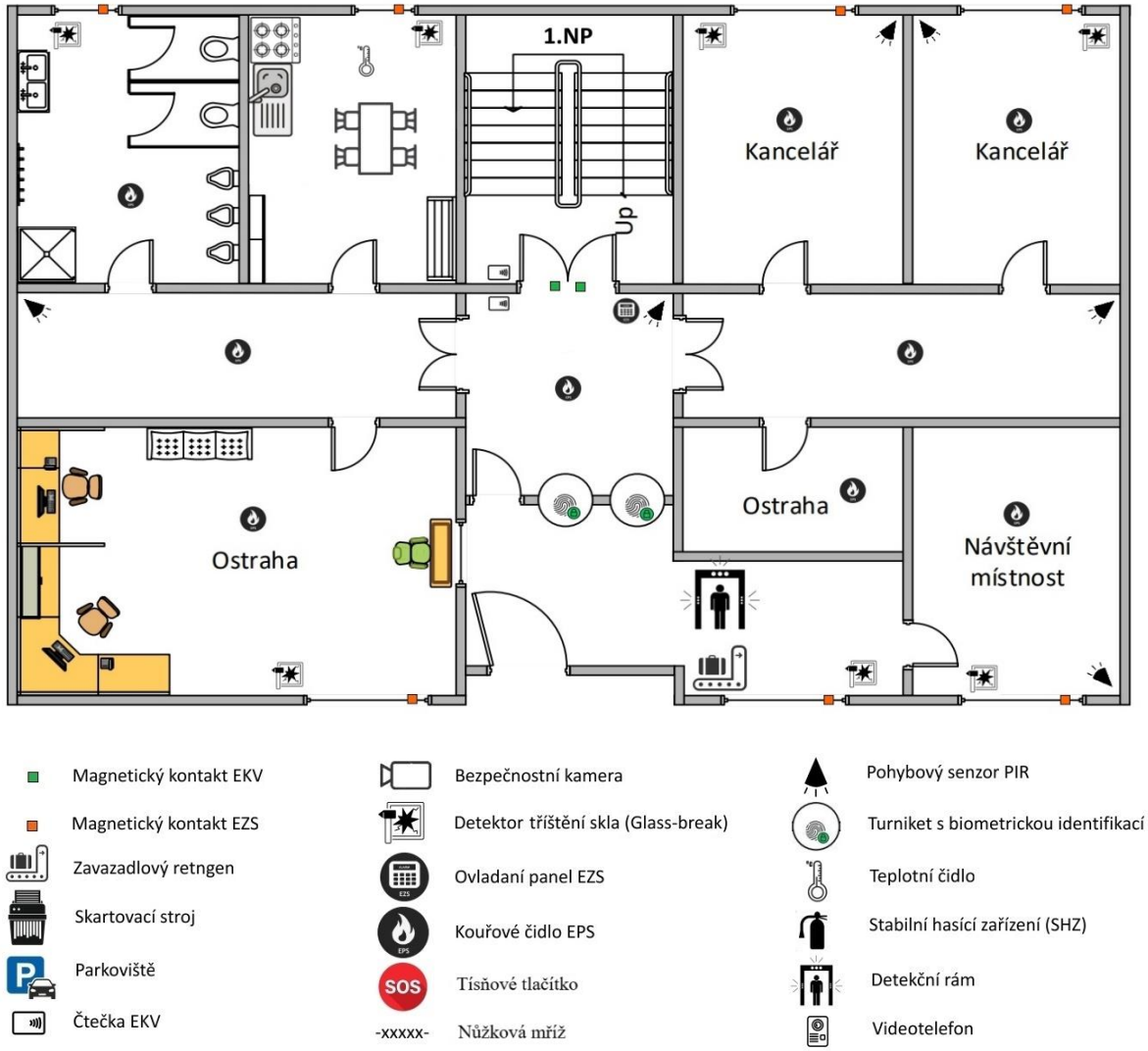
„Návštěvy musí být doprovázeny po celou dobu pobytu v objektu.
Musí být vedena evidence údajů o návštěvách, která obsahuje osobní identifikační údaje návštěv, doprovázejících osob a časové údaje o tom, kdy byla návštěva vykonána“.[51]

SS7 = 3 body

Dále jsou ve vstupním vestibulu umístěny elektronické turnikety, které slouží ke kontrolovanému vstupu zaměstnanců. Turnikety jsou osazeny čtečkou a vstup je možný pouze za pomoci identifikačního prvku čili vstupní karty a zadáním vstupního PINu. Všechna podlaží v budově (1. PP, 1. NP, 2.NP a 3. NP) jsou přístupná z centrálního schodiště vybudovaného v prostoru za vstupními turnikety. Od tohoto schodiště jsou vstupy na jednotlivá podlaží oddělena bezpečnostními dveřmi.

[51] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* [online]. [cit. 11.01.24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

Obrázek č. 2 - Schéma modelového objektu - vstupu do budovy



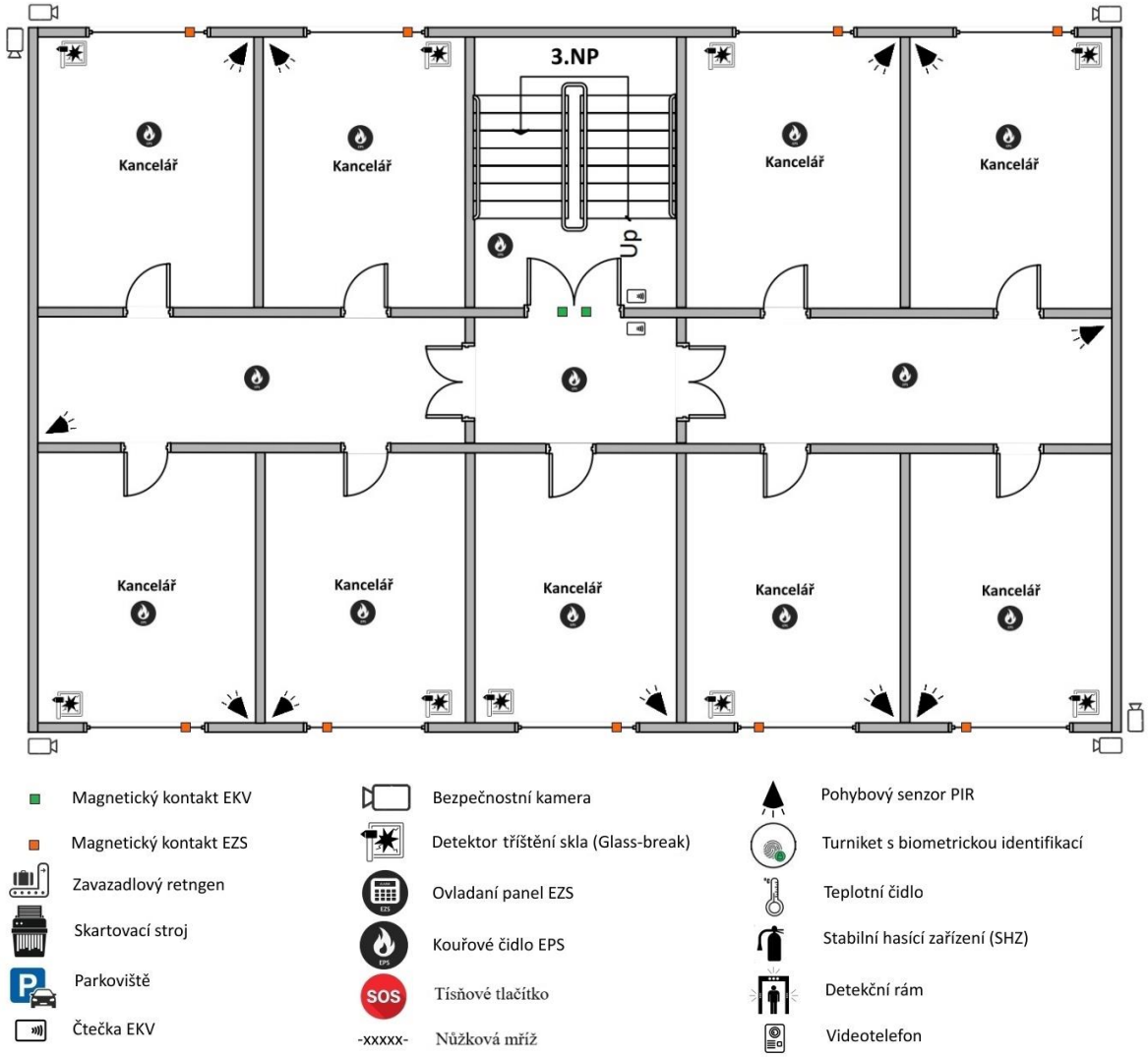
Zdroj: vlastní zpracování

Objekt kategorie PT musí být dle Vyhlášky č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků se objekt pro kategorii Přísně tajné zabezpečuje mechanickými zábrannými prostředky, zařízením elektrické zabezpečovací signalizace a speciálními televizními systémy, přičemž speciální televizní systémy nesmí narušit ochranu utajovaných informací. Tato podmínka je v rámci navržené studie splněna. Spodní okraj průlezného otvoru (okno) se v 1.NP nachází pod výškou 5,5 m[52], z těchto důvodů je posílena plášťová ochrana objektu pomocí čidel EZS (magnet, glass break)[53]

[52] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

[53] Detektor rozbití skla je senzor, který detekuje, zda došlo k rozbití nebo rozbití skleněné tabule. Nejčastěji se tyto senzory používají v blízkosti skleněných dveří, oken nebo výloh. Jsou využívány v elektronických poplašných systémech proti vloupání.

Obrázek č. 3 – Schéma modelového objektu - 3. NP



Zdroj: vlastní zpracování

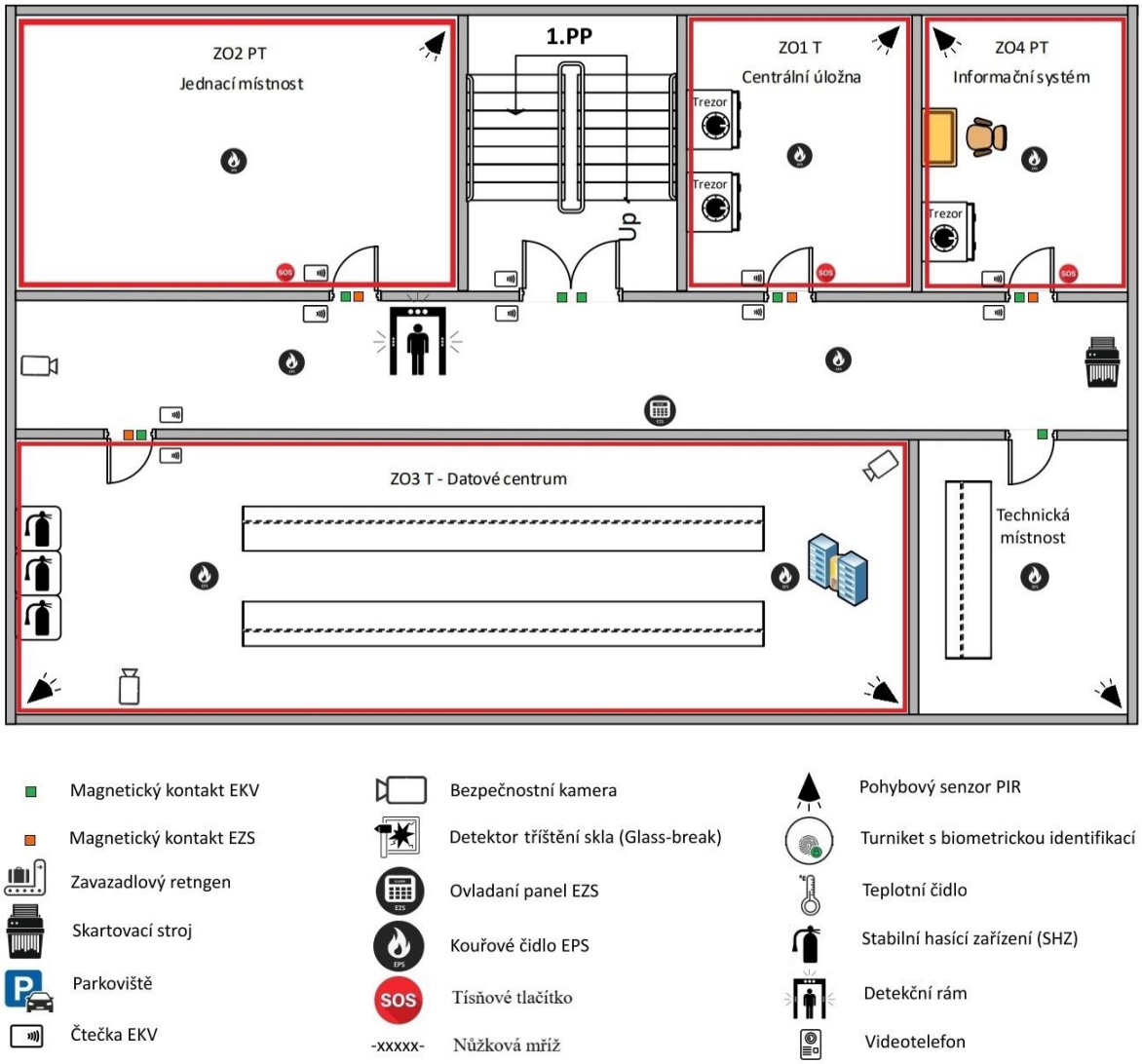
Z důvodu dostupnosti průlezných otvorů ze střechy objektu byla posílena plášťová ochrana budovy o prvky EZS (magnet, glass break), přestože se v 3. NP nenachází žádné ZO. V tomto případě vycházíme z logiky vyhlášky, která obecně pojednává o dostupnosti průlezných otvorů.

5.4 Zabezpečené oblasti 1 PP

Zabezpečené oblasti se nacházejí v suterénu, pro potřeby této práce je označeno 1. PP a v 2 nad podlažním patře s označením 2. NP. V ostatních patrech tj 1. NP a 3. NP jsou kanceláře, které slouží zabezpečení chodu organizace. Například to jsou prostory využívané ekonomickým odborem, personálním odborem a odborem administrativní bezpečnosti či slouží, jako technické místnosti případně sklady. Vstup do 1. PP je zprostředkován po schodišti, které se nachází za vstupními turnikety, které slouží ke kontrolovanému vstupu

zaměstnanců. Schodiště je v každém podlaží odděleno od ostatních prostor dveřmi, které jsou osazeny systémem kontroly vstupu. Všechny zabezpečené oblasti zařazeny do bezpečnostní třídy II, kdy vstupem do této oblasti nedochází k seznámení s UI.

Obrázek č. 4 – Schéma modelového objektu - zabezpečené oblasti v 1. PP



Zdroj: vlastní zpracování

V 1. PP jsou vybudovány 4 zabezpečené oblasti.[54] Od schodiště, které vede z 1. NP, jsou odděleny uzamykatelnými protipožárními dveřmi. Všechny prostory (chodba a místnosti) v 1. PP jsou bez oken, protože se nachází pod úrovní pozemku. V tomto podlaží je vybudována centrální úložna listinných dokumentů v kategorii Tajné a Přísně tajné. Pro přehlednost autor stanovil označení ZO1 T, PT. Dále je zde vybudována jednací místnost v kategorii PT, zde se pravidelně projednávají UI ve stupni utajení T a PT. Autor stanovil pro zabezpečenou oblast označení ZO2 PT. Další zabezpečenou oblastí, umístěnou v tomto podlaží, je datové centrum. Datové centrum je zabezpečená oblast kategorie T, ve které se nachází počítačové servery a další informační technologie. Zde se ukládají veškerá data z informačních systémů organizace. Autor stanovil označení pro datové centrum ZO3 T.

[54] Zabezpečená oblast dále jen ZO

Další zabezpečenou oblastí s označením ZO4 T je místnost určená pro zpracování UI v IS ve stupni utajení PT.

Zabezpečené oblasti jsou umístěny v tomto podlaží z důvodu minimální frekvence pohybu zaměstnanců a dále z ekonomický důvodů - výstavba ZO pod úrovní terénu a bez stavebních prvků, jako jsou okna, vyžaduje mnohem menší náklady na zabezpečení. Dalším a velmi podstatným důvodem je bezpečnost z pohledu kompromitujícího vyzařování. Ochrana informací před únikem, v důsledku kompromitujícího vyzařování v ZO prostoru výše popsaných parametrů, je velice vysoká.

5.4.1 Centrální úložna ZO1 T v 1. PP

Zabezpečená oblast je vybudována v souladu s Vyhláškou NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, jako zabezpečená oblast kategorie TAJNÉ třídy II (dále jen ZO1-T). Je určena jako centrální uložiště listinných dokumentů s UI. Jedná se o úložnu, kde organizace ukládá veškeré listinné dokumenty s UI, které jsou určeny k archivaci, nebo které jsou ukládány dle skartační lhůty do doby jejich zničení. Pro centrální úložnu je vhodné vybudovat ZO v 1. PP z důvodu možného většího počtu úschovných objektů. Vzhledem k tomu, že v této centrální úložně je možné uchovávány listinné dokumenty do kategorie T, je nutné pořídit certifikované úschovné objekty. Váha úschovných objektů se pohybuje kolem 500 kg a více. Prostory je možné využívat k ukládání dokumentů nižších stupňů utajení. Pro tyto dokumenty může být místnost vybavena trezory typu KOVONA a v případě stupně utajení VYHRAZENÉ je možné místnost vybavit i plechovými skříněmi, které jsou samostatně uzamykatelné. Utajované informace s označením KRYPTO je nutné ukládat do stejných úschovných objektů, jako dokumenty stupně utajení T. Tato pravidla platí i pro UI s označením NATO. Tyto dokumenty se ukládají zcela samostatně ve výhradně určeném úschovném objektu.

Místnost je vybavena certifikovanými úschovnými objekty bezpečnostní třídy I., které jsou vybaveny 3 polohovým mechanickým kombinačním zámkem.

„Úschovný objekt typu 3 je certifikovaný Úřadem a splňuje požadavky bezpečnostní třídy I podle ČSN EN 1143-1+A1.“[55]

SS1 = 3 body

„*Zámek typu je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky bezpečnostní třídy A podle ČSN EN 1300+A1*“.[56]

SS2 = 2 body

Vstup do zabezpečené oblasti je realizován bezpečnostními dveřmi osazenými bezpečnostním zámkem a elektronickou kontrolou vstupu a EZS magnety. Dále zabezpečená oblast vybavena EPS a prostorovými čidly EZS a tísňovým tlačítkem. Vstup do místnosti je snímám speciálním televizním systémem umístěných na chodbě.

[55] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* [online]. [cit. 11.1.24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

[56] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* [online]. [cit. 11.1. 24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

Tabulka bodového ohodnocení opatření fyzické bezpečnosti - ZO1 – kategorie T

Účel zabezpečené oblasti: **ukládání utajovaných informací v úschovném objektu**

Tabulka č. 1 Bodové ohodnocení ZO1[57]

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty	T. 3 - 3 body	SS1 = 3
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 2
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 6**
Zabezpečené oblasti	T. 2 - 2 body	SS3 = 2
Uzamykací systémy zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 4**
Bodové ohodnocení objektu		
Objekt		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**12**
Kontrola vstupu	T. 2 - 2 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	**SS9 = 3**
Celkové hodnocení ostrahy a systému EZS	**S5 = SS8 + SS9**	**S5 = 8**
Povinné (S4) + (S5)	**(S4) + (S5)**	**14**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery	1 bod	SS11 = 1
Bodové ohodnocení perimetru	0	SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 =1
Bezpečnostní osvětlení perimetru	2 body	SS14 = 2
Speciální televizní systém perimetru	2 body	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	TAJNÉ	3

Zdroj: vlastní zpracování

[57] Vlastní zpracování dle přílohy Vyhlášky č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků.

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky 528/2005 Sb.)

PRO ZABEZPEČENOU OBLAST KATEGORIE TAJNÉ

Tabulka č. 2 Požadované bodové ohodnocení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	5
Nepovinné: (S6)	5
Celkový výsledek	**20**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 3 Výpočet skutečného provedení

Povinné: (S1) + (S2) + (S3)	12
Povinné: (S4) + (S5)	14
Nepovinné: (S6)	6
Celkový výsledek	**32**

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 4 bodů.

5.4.2 Jednací oblast ZO2 PT v 1. PP

Zabezpečená oblast ZO2 PT je vybudována v souladu s Vyhláškou NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, jako zabezpečená oblast kategorie PŘÍSNĚ TAJNÉ třídy II JEDNACÍ OBLAST. Je určena k pravidelnému projednávání UI ve stupni utajení PT.

Vstup a výstup do jednací oblasti je, dle zákona o ochraně UI, kontrolován opatřeními podle § 27. Před vstupními dveřmi do jednací oblasti je nainstalováno zařízením sloužícím k vyhledávání nebezpečných látek nebo předmětů. Ten slouží pro kontrolu na zakázané prostředky, kterými jsou například mobilní telefony, nahrávací zařízení, vysílací zařízení.

Vstupní dveře jsou bezpečnostní s certifikátem NBÚ splňují požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627. Dále jsou osazeny uzamykacím systémem, jehož komponenty splňují požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627. A jsou osazený magnetickým kontaktem. Kontrola vstupu je provedena pomocí nainstalovaného EKV. V zabezpečené oblasti jsou nainstalovány prostorová čidla, elektrická požární signalizace a tísňové tlačítko. Na chodbě je speciální televizní systém, který monitoruje vstup do ZO jednací místnosti JO PT a bezpečnostní rám, který slouží pro kontrolu na zakázané prostředky (mobilní telefony, nahrávací zařízení, vysílací zařízení. Neoprávněná osoba, může vstoupit do jednací oblasti pouze s osobou, která má do této oblasti vstup povolen. Veškeré vstupy do jednací oblasti podléhají kontrole a evidenci.

Do této ZO je přísně zakázáno vnášet mobilní telefony, jakákoliv nahrávací zařízení, vysílací zařízení, jakákoliv testovací, měřící a diagnostická zařízení. Jednací místnost je vybavena nábytkem, který podléhá kontrole, a to písemným záznamem, kdy je zaevidováno inventární číslo, typ a dále historie jeho pohybu.

Tato ZO podléhá pravidelným obranně technickým prohlídkám. Obranné prohlídky jednacích oblastí se provádějí každých 6 měsíců nebo vždy po neautorizovaném vstupu osob, které provádějí údržbu nebo stavební úpravy.

Vzhledem k technickému vybavení lze jednací místnost využívat také k pravidelnému projednávání informací ve stupni utajení T.

Tabulka bodového ohodnocení opatření fyzické bezpečnosti - ZO2 – kategorie PT

Účel zabezpečené oblasti: **jednací oblast**

Tabulka č. 4 Bodové ohodnocení ZO2

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty		SS1 = 0
Zámky úschovných objektů		SS2 = 0
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 0**
Zabezpečené oblasti	T. 2 - 2 body	SS3 = 3
Uzamykací systémy zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 6**
Bodové ohodnocení objektu		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**8**
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	**SS9 = 2**
Celkové hodnocení ostrahy a systému EZS	**S5 = SS8 + SS9**	**S5 = 7**
Povinné (S4) + (S5)	**(S4) + (S5)**	**13**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery	1 bod	SS11 = 1
Bodové ohodnocení perimetru	0	SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 = 1
Bezpečnostní osvětlení perimetru	2 body	SS14 =2
Speciální televizní systém perimetru	2 body	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	PŘÍSNĚ TAJNÉ	4

Zdroj: vlastní zpracování

Bodová hodnota jednací oblasti kategorie PŘÍSNĚ TAJNÉ – 4 body

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky 528/2005 Sb.):

PRO ZABEZPEČENOU JEDNACÍ OBLAST KATEGORIE PŘÍSNĚ TAJNÉ

Tabulka č. 1 Požadované bodového ohodnocení JO

Povinné: (S1) + (S2) + (S3)	7
Povinné: (S4) + (S5)	7
Nepovinné: (S6)	5
Celkový výsledek	**19**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 6 Vypočet skutečného provedení JO

Povinné: (S1) + (S2) + (S3)	8
Povinné: (S4) + (S5)	13
Nepovinné: (S6)	6
Celkový výsledek	**27**

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 5 bodů.
Hodnota (S2) nesmí být rovna 0.

5.4.3 Datové centrum ZO3 T v 1. PP

Datové centrum je vybudováno jako zabezpečená oblast kategorie TAJNÉ. Jedná se o prostor, kde jsou umístěny počítačové techniky serverového typu. Data jsou ukládána nešifrovaná a přihlášení probíhá pomocí uživatelského jména a certifikovaného prostředku dle vyhlášky.

Vstup do datového centra je zabezpečen vstupními bezpečnostními dveřmi s certifikátem NBÚ a osazeny zámkem jehož komponenty splňují požadavky bezpečnostní třídy RC 4 podle ČSN EN 1627. Dále jsou osazený magnetickým kontaktem EZS a kontrolou vstupu přes EKV. V centrálním uložišti dat jsou instalována prostorová čidla, zařízení elektrické požární signalizace. V datovém centru i na chodbě před datovým centrem je instalován speciální televizní systém. Zabezpečená oblast je doplněna stabilním hasicím zařízením.

V níže přiložené tabulce bodové hodnocení podle vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

Tabulka bodového ohodnocení opatření fyzické bezpečnosti ZO3 – kategorie TAJNÉ

Účel zabezpečené oblasti: datové centrum

Tabulka č. 7 Bodové ohodnocení ZO3

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty	1 bod (vyhláška č. 523/2005 Sb.)	SS1 = 1
Zámky úschovných objektů	2 body (vyhláška č. 523/2005 Sb.)	SS2 = 2
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 2**
Zabezpečené oblasti	T. 2 - 2 body	SS3 = 2
Uzamykací systémy zabezpečené oblasti	T. 3 - 3 body	SS4 = 3
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 6**
Bodové ohodnocení objektu		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**10**
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	**SS9 = 3**
Celkové hodnocení ostrahy a systému EZS	**S5 = SS8 + SS9**	**S5 = 8**
Povinné (S4) + (S5)	**(S4) + (S5)**	**14**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery kontrola není realizována	1 bod	SS11 = 1
Bodové ohodnocení perimetru		SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 = 1
Bezpečnostní osvětlení perimetru je realizováno	2 body	SS14 = 2
Speciální televizní systém perimetru je realizován	2 body	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	TAJNÉ	3

Zdroj: vlastní zpracování

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky č 528/2005 Sb., a z vyhlášky č. 523/2005 Sb.):

PRO ZABEZPEČENOU OBLAST DATOVÉ CENTRUM KATEGORIE TAJNÉ

Tabulka č. 8 Požadované bodové ohodnocení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	5
Nepovinné: (S6)	5
Celkový výsledek	**20**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 9 Výpočet skutečného provedení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	14
Nepovinné: (S6)	6
Celkový výsledek	**30**

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 4 body.

5.4.4 Zabezpečená oblast určená pro IS PT – ZO4 PT v 1. PP

Zabezpečená oblast je určená pro zpracovávání UI v informačním systému kategorie PT. Informační systém je koncipován jako samostatně stojící pracovní stanice bez přístupu k jakýmkoliv vnitřním nebo vnějším komunikačním kanálům. Na stanici se trvale neukládají utajované informace. Tyto se nacházejí pouze na vyměnitelných nosičích informace náležejících každému konkrétnímu uživateli. Sdílení informací v tomto IS není možné. Každý uživatel IS odpovídá za zajištění ochrany dat zpracovávaných v informačním systému před vyzrazením, zneužitím, poškozením, ztrátou a zničením.

Sestava určená pro zpracování utajovaných informací stupně utajení PŘÍSNĚ TAJNÉ se skládá z přenosného počítače (notebooku) a tiskárny. Stanice slouží pouze pro zpracování dat a po ukončení práce na ní nezůstávají uloženy žádné zpracovávané informace. Utajované informace jsou za pomoci kancelářských aplikací na stanici pouze zpracovávány, interní pevný disk neslouží k trvalému ukládání zpracovávaných informací. Po ukončení práce jsou veškeré zpracovávané utajované informace uloženy a zálohovány na vyměnitelné nosiče informací a pracovní oblasti pevného disku jsou bezpečně vymazány. Přístup do IS je chráněn heslem, které je uloženo v zapečetěné obálce v odpovídajícím certifikovaném úschovném objektu. Do IS je zakázáno vkládat nosná média. Všechny komponenty IS, sestava pracovní stanice s tiskárnou a vyměnitelné nosiče informací, jsou uloženy v zabezpečené oblasti kategorie PT v certifikovaném úschovném objektu kategorie PT.

Vstup do ZO je zabezpečen bezpečnostními dveřmi s bezpečnostním zámkem s osazením EKV a EZS magnety. Zabezpečená oblast je vybavena úschovným objektem II. bezpečnostní třídy, který slouží k ukládání IS. Dále je vybavena prostorovým čidlem EZS, EPS, vchod do zabezpečené oblasti je trvale snímán speciálním televizním systémem.

Tabulka bodového ohodnocení opatření fyzické bezpečnosti ZO4 – kategorie PT

Účel zabezpečené oblasti: zpracovávání UI v IS

Tabulka č. 10 Bodové ohodnocení ZO4

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty	T. 4 - 4 body	SS1 = 4
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 2
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 8**
Zabezpečené oblasti	T. 2 - 2 body	SS3 = 2
Uzamykací systémy zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 4**
Bodové ohodnocení objektu		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**14**
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	**SS9 = 2**
Celkové hodnocení ostrahy a systému EZS	**S5 = SS8 + SS9**	**S5 = 7**
Povinné (S4) + (S5)	**(S4) + (S5)**	**13**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery	1 bod	SS11 = 1
Bodové ohodnocení perimetru		SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 = 1
Bezpečnostní osvětlení perimetru	2 body	SS14 = 2
Speciální televizní systém perimetru	2 body	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	PŘÍSNĚ TAJNÉ	4

Zdroj: vlastní zpracování

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky 528/2005 Sb.):

PRO ZABEZPEČENOU OBLAST UKLÁDÁNÍ V IS KATEGORIE

PŘÍSNĚ TAJNÉ

Tabulka č. 11 Požadované bodové ohodnocení

Povinné: (S1) + (S2) + (S3)	13
Povinné: (S4) + (S5)	7
Nepovinné: (S6)	5
Celkový výsledek	**25**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 12 Výpočet skutečného provedení

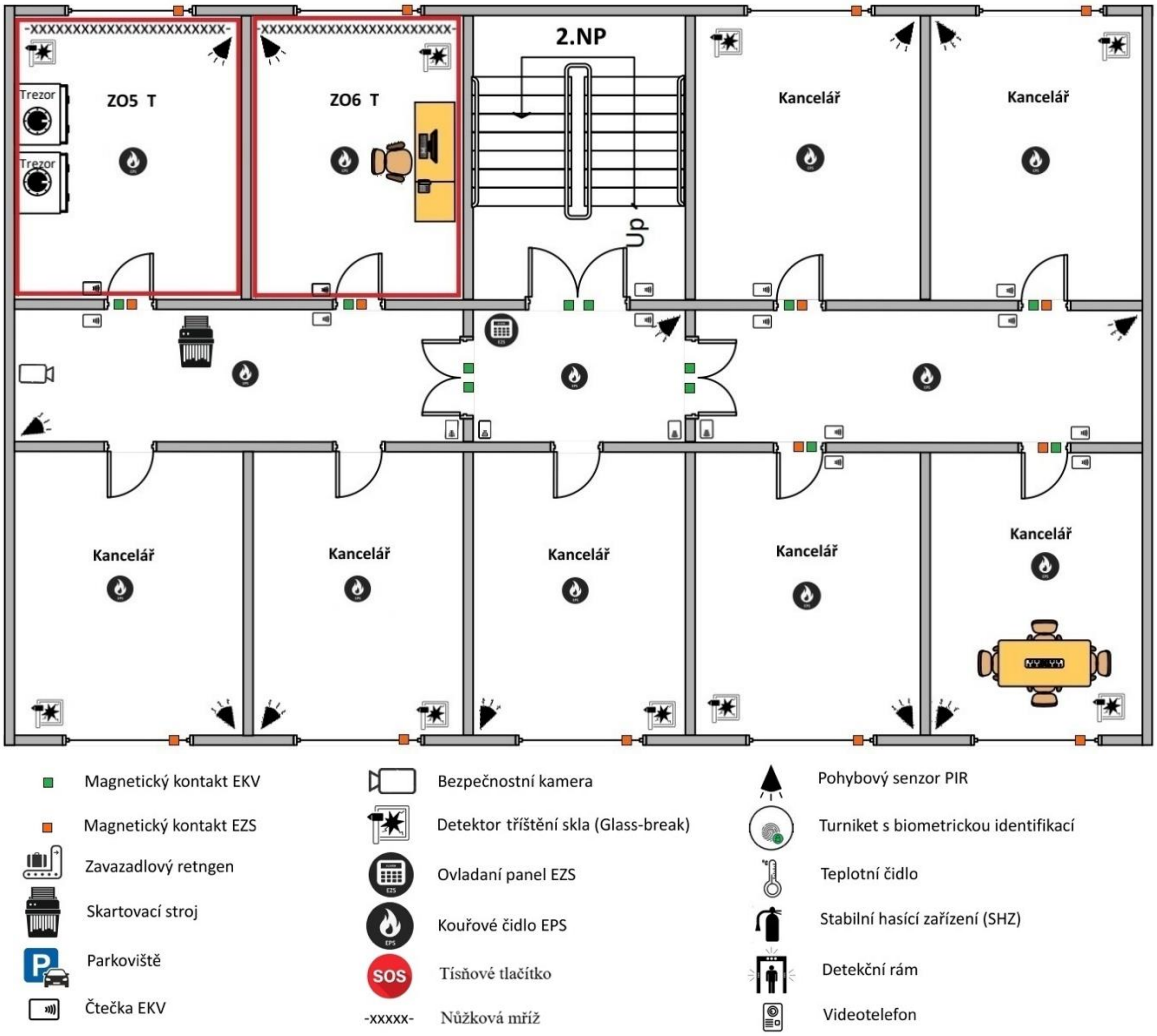
Povinné: (S1) + (S2) + (S3)	14
Povinné: (S4) + (S5)	13
Nepovinné: (S6)	6
Celkový výsledek	**33**

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 5 bodů.

5.5 Zabezpečené oblasti 2. NP

Obrázek č. 5 – Schéma modelového objektu - zabezpečené oblasti ve 2. NP



Zdroj: vlastní zpracování

5.5.1 Úložna ZO5 T ve 2. NP

Do místnosti je realizován vstup bezpečnostními dveřmi s certifikátem NBÚ, jež jsou osazený magnetickým kontaktem a kontrolou vstupu přes EKV. Spodní okraj průlezného otvoru – okna v zabezpečených oblastech je 5,5 m nad okolním terénem. Okno je osazena magnetickým kontaktem EZS. Dále jsou zde instalovány detektory rozbití skla, prostorová čidla, zařízení elektrické požární signalizace, speciální televizní systém. Před okny uvnitř místnosti je instalována vnitřní nůžková mříž, která splňuje požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627. Kamera, uvnitř zabezpečené oblasti, snímá pouze vstup do místnosti. Místnost je vybavena certifikovanými úschovnými objekty typu 3 s certifikovaným zámkem typu 2.

Tabulka bodového ohodnocení opatření fyzické bezpečnosti ZO5 – kategorie TAJNÉ

Účel zabezpečené oblasti: ukládání utajovaných informací v úschovném objektu

Tabulka č. 2 Bodové ohodnocení ZO5

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty	T. 4 - 3 body	SS1 = 3
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 2
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 6**
Zabezpečené oblasti	T. 3 - 3 body	SS3 = 3
Uzamykací systémy zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 6**
Bodové ohodnocení objektu		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**14**
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	**SS9 = 3**
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5 = 8
Povinné (S4) + (S5)	**(S4) + (S5)**	**14**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery kontrola je realizována	1 bod	SS11 = 1
Bodové ohodnocení perimetru		SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 =1
Bezpečnostní osvětlení perimetru je realizováno	2 bodů	SS14 = 2
Speciální televizní systém perimetru je realizován	2 bodů	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	TAJNÉ	3

Zdroj: vlastní zpracování

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky 528/2005 Sb.)

PRO ZABEZPEČENOU OBLAST PRO UKLÁDÁNÍ UI KATEGORIE TAJNÉ

Tabulka č. 14 Požadované bodové ohodnocení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	5
Nepovinné: (S6)	5
Celkový výsledek	**20**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 15 Výpočet skutečného provedení

Povinné: (S1) + (S2) + (S3)	14
Povinné: (S4) + (S5)	14
Nepovinné: (S6)	6
Celkový výsledek	**34**

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 4 bodů.

5.5.2 Zabezpečená oblast pro IS T – ZO6 T ve 2. NP

Zabezpečená oblast je kategorie T a je určená ke zpracování UI ve stupni utajení T v informačním systému. Na informačním systému je UI zobrazena a zpracována a dále se ukládá v datovém centru. Hodnocení informačního systému, jako úschovného objektu, je provedeno dle Vyhlášky č. 523/2005 o bezpečnosti informačních a komunikačních systémů

„Danou částí informačního systému mohou být utajované informace pouze zobrazeny a zpracovávány nebo přenášeny“

SS1 = 1 body

Identifikace jménem a autentizace předmětem

SS2 = 2 body

„Předmět používaný pro autentizaci musí být schválen Úřadem v rámci certifikace informačního systému. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 2.“

Do místnosti je realizován vstup bezpečnostními dveřmi s certifikátem NBÚ. Ty jsou osazeny certifikovaným bezpečnostním zámkem typu 3 a magnetickým kontaktem EZS a kontrolou vstupu pomocí systému EKV. Spodní okraj okna v zabezpečené oblasti je 5,5 m nad okolním terénem. Okno je osazeno magnetickým kontaktem EZS. Před okny uvnitř místnosti je instalována vnitřní nůžková mříž, která splňuje požadavky bezpečnostní třídy RC 3. Dále jsou na oknech instalovány detektory rozbití skla. Uvnitř zabezpečené oblasti jsou instalovány prostorová čidla, zařízení elektrické požární signalizace, speciální televizní systém. Kamera uvnitř zabezpečené oblasti snímá pouze vstup do místnosti.

Tabulka bodového ohodnocení opatření fyzické bezpečnosti ZO6 – kategorie TAJNÉ

Účel zabezpečené oblasti: ukládání utajovaných informací v IS

Tabulka č. 16 Bodové ohodnocení ZO6

Bezpečnostní opatření	**Typ**	**Bodové ohodnocení**
Úschovné objekty	1 bod (vyhláška 523/2005 Sb.)	SS1 = 1
Zámky úschovných objektů	2 body (vyhláška 523/2005 Sb.)	SS2 = 2
Celkové ohodnocení úschovného objektu a jeho zámku	**S1 = SS1 x SS2**	**S1 = 2**
Zabezpečené oblasti	T. 2 - 2 body	SS3 = 2
Uzamykací systémy zabezpečené oblasti	T. 2 - 2 body	SS4 = 3
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	**S2 = SS3 x SS4**	**S2 = 6**
Bodové ohodnocení objektu		**S3 = 2**
Povinné (S1) + (S2) + (S3)	**(S1) + (S2) + (S3)**	**10**
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu	Návštěva s doprovodem	SS7 = 3
Celkové hodnocení kontroly vstupu	**S4 = SS6 + SS7**	**S4 = 6**
Ostraha	T. 5 - 5 bod	SS8 = 5
Zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS91 = 3
Instalace zařízení elektrické zabezpečovací signalizace	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	SS9=(SS91+SS92)/2*SS92/OBL	SS9 = 3
Celkové hodnocení ostrahy a systému EZS	**S5 = SS8 + SS9**	**S5 = 8**
Povinné (S4) + (S5)	**(S4) + (S5)**	**14**
Fyzické bariéry	T. 1 - 1 bod	SS10 = 1
Kontrola vstupu v přístupových bodech bariery kontrola není realizována	1 bod	SS11 = 1
Bodové ohodnocení perimetru		SS13 = 0
Namátkové vstupní a výstupní prohlídky jsou prováděny	1 bod	SS12 = 1
Bezpečnostní osvětlení perimetru	2 body	SS14 = 2
Speciální televizní systém perimetru	2 body	SS15 = 2
Celkové hodnocení ochrany perimetru	**S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15**	**S6 = 6**
OBL	TAJNÉ	3

Zdroj: vlastní zpracování

Celkové bodové ohodnocení při vysoké míře rizika (údaj z vyhlášky č 528/2005 Sb., a z vyhlášky č. 523/2005 Sb.):

PRO ZABEZPEČENOU OBLAST PRO UKLÁDÁNÍ UI V IS KATEGORIE TAJNÉ

Tabulka č. 17 Požadované bodové ohodnocení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	5
Nepovinné: (S6)	5
Celkový výsledek	**20**

Zdroj: vlastní zpracování

SKUTEČNÉ PROVEDENÍ:

Tabulka č. 18 Výpočet skutečného provedení

Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	14
Nepovinné: (S6)	6
Celkový výsledek	30

Zdroj: vlastní zpracování

Poznámka (údaj z vyhlášky 528/2005 Sb.):
Hodnota (S5) musí dosáhnout alespoň 4 bodů.

5.6 Provozní řád

Projekt fyzické bezpečnosti musí obsahovat provozní řád objektu případně samotného pracoviště. Autor upřednostňuje vyhotovit Provozní řád pro každou zabezpečenou oblast zvlášť. Pro účely DP práce a z důvodu velké obsáhlosti je zvoleno vyhotovení jednoho dokumentu, který obsahuje všechny zabezpečené oblasti.

PROVOZNÍ ŘÁD REŽIMOVÉHO PRACOVIŠTĚ

Tento Provozní řád je jako součást dokumentace objektové bezpečnosti závazný pro všechny pracovníky organizace.

Stanovení zabezpečených oblastí

Zabezpečené oblasti v 1. PP budovy:

ZO č. 1 odpovídá požadavkům na zabezpečenou oblast kategorie TAJNÉ třídy II. Tato zabezpečená oblast je určena pro ukládání listinných dokumentů do stupně utajení T.

ZO č. 2 odpovídá požadavkům na zabezpečenou oblast kategorie PŘÍSNĚ TAJNÉ třídy II a je určena výhradně pro pravidelné projednávání UI kategorie PŘÍSNĚ TAJNÉ.

ZO č. 3 odpovídá požadavkům na zabezpečenou oblast kategorie TAJNÉ třídy II. Tato zabezpečená oblast je vybudována jako datové centrum a je určena k centrálnímu ukládání v IS.

ZO č. 4 odpovídá požadavkům na zabezpečenou oblast kategorie PŘÍSNĚ TAJNÉ třídy II a je určena výhradně pro zpracování UI v IS kategorie PŘÍSNĚ TAJNÉ a k ukládání UI kategorie PŘÍSNĚ TAJNÉ.

Zabezpečené oblasti ve 2. NP budovy:

ZO č. 5 odpovídá požadavkům na zabezpečenou oblast kategorie TAJNÉ třídy II. Tato zabezpečená oblast je určena pro ukládání listinných dokumentů do stupně utajení T

ZO č. 6 odpovídá požadavkům na zabezpečenou oblast kategorie TAJNÉ třídy II. Tato zabezpečená oblast je určena pro zpracování v IT systému stupně utajení T.

Režim ukládání utajované informace

Dokumentem T se rozumí každý písemný, obrazový, zvukový nebo jiný záznam, který vznikl z činnosti původce a tento dokument je klasifikován a označen stupněm utajení T.

Pro soustředěné ukládání dokumentů T určuji centrální úložnu, která je dislokována v 1. PP. Ukládání v tomto prostoru je možné pouze v instalovaných certifikovaných úschovných trezorech. Prostory centrální úložny je možné využívat i pro ukládání utajovaných informací nižších stupňů utajení, a to výhradně v instalovaných úschovných trezorech s označením.

Za ukládání dokumentu T zodpovídá zpracovatel, případně ten, který dokument T převzal.

Ukládání informačního systému kategorie PT. Zabezpečená oblast určená pro zpracovávání utajované informace kategorie PT je dislokována v 1.PP s označením ZO4-PT. V zabezpečené oblasti je umístěn úschovný objekt, ve kterém je umístěna informační stanice určená pro zpracování UI. Přihlášení do informačního systému je možné pouze za pomoci identifikace jménem a autentizace předmětem. Předmět je přidělen uživateli vedoucím organizačního celku, který zároveň provede proškolení uživatele před prvním přihlášením do informačního systému. Předmět používaný pro autentizaci musí být schválen Úřadem v rámci certifikace informačního systému. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu.

Po ukončení činnosti je uživatel povinen uložit tento informační systém zpět do úschovného objektu.

Bezpečnostní opatření

Vstup do zabezpečených oblastí je řízen systémem elektronické kontroly vstupu. Souhlas s oprávněním vstupu uděluje bezpečnostní ředitel na základě písemné žádosti vedoucího příslušného organizačního celku. Oprávněný uživatel vstupuje do zabezpečené oblasti prostřednictvím identifikační vstupní karty. Používání vstupních karet je upraveno vnitřním předpisem. Prostory zabezpečených oblastí jsou zajištěny elektronickou zabezpečovací signalizací prostorovou a plášťovou. Pravidla a postupy užívání elektronické zabezpečovací signalizace jsou uvedeny a upraveny vnitřním předpisem. Vstupní dveře všech zabezpečených oblastí jsou trvale monitorovány speciálním televizním systémem se záznamem obrazu, z chodby v příslušných podlažích, kde jsou umístěny kamery. Záznam z monitorovacích systémů je cyklicky přemazáván a uchovávají se pouze poplachové stavy. Speciální televizní systémy instalované uvnitř zabezpečených oblastí snímají pouze vchodové dveře, tak aby bylo možné identifikovat vstupující osobu

Vstup do jednací oblasti je možný pouze na základě povolení uděleném bezpečnostním ředitelem. Vstup je realizován po projití bezpečnostním rámem, který slouží ke kontrole

na zakázané prostředky. Zakázané prostředky musí být odloženy na ostraze objektu, kde jsou instalovány úschovné elektronické boxy. Ostraha vede evidenci vstupů do jednací oblasti a evidenci ukládání zakázaných prostředků. V jednací místnosti je zakázána manipulace s vybavením a jakýkoliv mimořádný vstup musí být předem nahlášen bezpečnostnímu řediteli. Na pracovišti bezpečnostního ředitele je vedena evidence obranně technických prohlídek jednací místnosti a pověřený pracovník zajišťuje pravidelné i mimořádné obranně technické prohlídky této oblasti.

Režim vstupu do zabezpečených oblastí je oprávněným osobám umožněn prostřednictvím osobní identifikační karty. Oprávněnost vstupu je udělena bezpečnostním ředitelem na základě písemné žádosti vedoucího organizačního celku.

Režim manipulace s klíči

Klíče od místností a od úschovných objektů jsou přiděleny vedoucím organizačního celku vždy ve dvou sadách. Jedna sada se přiděluje oprávněnému uživateli a druhá sada zůstává v zapečetěném obalu u vedoucího organizačního celku. Evidence přidělování klíčů je vedena písemnou formou a doplněna podpisem uživatele o převzetí klíčů.

Uživatel ukládá klíče v elektronické schránce. Tato schránka je přidělena pouze jedné osobě a není sdílena. Vstup do elektronické schránky v případě mimořádné události je podmíněn souhlasem bezpečnostního ředitele a pouze komisionálním způsobem. Tento vstup je upraven vnitřním předpisem.

Žádný klíč není dovoleno odnášet mimo areál pracoviště. Ztráta nebo poškození klíčů je okamžitě po zjištění nahlášena bezpečnostnímu řediteli. Případně vedoucímu ostrahy objektu k provedení opatření eliminace bezpečnostních rizik.

Ukládání dokumentů do úschovných trezorů s kódovým zámkem. Před prvním uložení zajistí vedoucí organizačního celku proškolení uživatele a dále zajistí překódování číselné kombinace. Zápis o nové číselné kombinaci uložený v zapečetěné obálce je uložen u vedoucího organizačního celku v úschovném objektu. Vedoucí organizačního celku je odpovědný za změnu číselné kombinace, která se provádí vždy do 6 měsíců od poslední změny případně okamžitě při změně oprávněného uživatele.

Režim používání zabezpečovacích systémů.

Všechny zabezpečené oblasti jsou vybaveny elektronickou kontrolou vstupu, elektronickým zabezpečovacím systémem, elektronickou požární signalizací, prvky speciálních televizních a tísňových systémů. Před prvním vstupem do zabezpečené oblasti je vedoucí organizačního celku povinen seznámit oprávněného uživatele s manipulací s těmito systémy. O provedeném seznámení a proškolení oprávněného uživatele je vyhotoven písemný záznam, který je potvrzen podpisem uživatele a zaslán bezpečnostnímu řediteli.

Je zakázána jakákoli manipulace s jednotlivými technickými prostředky zabezpečovacích systémů.

Závěrečné ustanovení

Ve všech prostorách budovy a zabezpečených oblastí je přísně zakázáno kouřit a manipulovat s otevřeným ohněm.

Pro zabezpečené oblasti platí přísný zákaz návštěv bez povolení bezpečnostního ředitele a bez osobního doprovodu. Součástí tohoto Provozního řádu je technická dokumentace, která zahrnuje přesné popisy a manipulaci s technickými prostředky a pravidla výkonu fyzické ostrahy objektu. Vedoucí organizačních celků jsou povinni seznámit oprávněné uživatele s těmito dokumenty a dále jsou povinni oznámit bezpečnostnímu řediteli veškeré změny tykající se zabezpečených oblasti.

5.7 Plán zabezpečení objektu při krizových situacích

Vzhledem k tomu, že autor popisuje fiktivní objekt, zvolil pro vypracování krizového plánu obecnou rovinu.

Krizový plán ochrany objektu stanovuje přesný postup ochrany UI při řešení mimořádných událostí. Krizovou či mimořádnou situací se rozumí stav, při kterém může dojít k poškození, znehodnocení, úniku či ztrátě UI.

Oblast mimořádných situací musí zahrnovat například živelné pohromy, napadení objektu, uložení výbušného nástražného systému, válečné nebezpečí a také mobilizace.

K řešení mimořádných situací, při kterých dojde k ohrožení bezpečnosti UI je zřízen krizový štáb. Do doby shromáždění krizového štábu řeší postup při mimořádné události

ostraha objektu. Ostraha objektu má stanovené postupy přesně definovány v dokumentaci Pravidla pro výkon fyzické ostrahy. Tento dokument je ze zákona povinně vypracován a je schválen bezpečnostním ředitelem a následně přiložen k Projektu fyzické bezpečnosti.

Stav ohrožení UI může vyhlásit statutární orgán organizace nebo jím pověřený pracovník, a to v případě zjištění zvýšeného rizika ohrožení. Vyhlášením stavu ohrožení znamená přijetí opatření nad rámec standardu stanoveného bezpečnostním projektem ochrany objektu. Samotný postup při řešení mimořádné události zahrnuje analýzu typu mimořádné události, vyhlášení stavu ohrožení, zvolení optimálního řešení s prioritou ochrany života a zdraví osob. Realizace fyzických opatření i ochraně UI a realizace odstranění následků mimořádné události. Fyzickými opatřeními se v tomto případě rozumí opatření, které následují po zjištění vzniku mimořádné události. Jejich cílem je minimalizace následků události.

Pro řešení krizové situace provozovaného informačního systému je v bezpečnostní dokumentaci informačního systému stanovena opatření zaměřená na jeho uvedení do stavu odpovídajícího bezpečnostní dokumentaci informačního systému. V případě mimořádné situace pro softwarové nebo hardwarové vybavení je uveden v bezpečnostní dokumentaci informačního systému způsob zálohování IS a uložení záložních médií. Bezpečnostní dokumentace IS uvádí zajištění nouzového provozu informačního systému s vyjmenováním minimálních funkcí, které musí být zachovány, a obnovy funkčnosti a uvedení informačního systému do známého bezpečného stavu.

5.8 Zhodnocení zabezpečených oblastí

Autor diplomové práce zvolil pro vybudování zabezpečených oblastí kategorie T a PT umístění v 1.PP z několika důvodů. Při svém rozhodování vzal v potaz stavební možnosti, ekonomické náklady a dále možnost porovnání zabezpečení v zabezpečených oblastí v místnostech umístěných podpodlaží a místnosti umístěné v horním patru.

Autor svou práci postavil na možnosti fiktivní stavby s prostory, které jsou pod povrchem terénu. V těchto prostorech vybudovat zabezpečenou oblast výše jmenovaných kategorií bezpečnostně nejméně náročné. Prostory jsou bez oken, a tento fakt snižuje nutnost zabezpečení mechanickými technickými prostředky, což přináší ekonomickou úsporu. Dále je v těchto prostorách maximálně snížena četnost pohybu neoprávněných osob. Autor umístil systém elektronické kontroly vstupu již na dveře vedoucí od schodiště do hlavní

chodby v 1. PP. Vstup do 1. PP je v tomto případě umožněn minimálnímu počtu pracovníků. Dalším důležitým aspektem je to, že dle vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti, je nutná kontrola vstupu do objektu nebo zabezpečené oblasti kategorie Přísně tajné. K tomuto účelu se používají zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů. Autor umístil jedno zařízení ve vstupní hale. To je pod dohledem pracovníků ostrahy a slouží ke kontrole návštěv. Druhé zařízení je umístěno před vstupem do jednací oblasti. I zde provádí kontrolu pracovník ostrahy, ale kontrola se vztahuje na všechny vcházející osoby. Umístění jednací oblasti v jiném patře je bezpochyby možné, ale umístění zařízení k vyhledávání nebezpečných látek nebo předmětů před vstupem do zabezpečené oblasti, by mohlo působit neesteticky a samotná prohlídka vcházejících osob, by také nebyla úplně komfortní v souvislosti s běžným provozem ostatních kancelářských prostor. Dalším aspektem pro zřízení jednací oblasti v prostorách 1. PP, je požadavek na zajištění proti pasivnímu a aktivnímu odposlechu, kdy vyhláška tyto požadavky definuje:

b) okna, větrací otvory nebo prostupy klimatizace musí být chráněny technickými prostředky certifikovanými Úřadem. Jednací oblast musí být chráněna proti odezírání z míst nacházejících se vně jednací oblasti,[58]

Svým umístěním jednací oblast tuto podmínku splňuje bez vysokých ekonomických nákladů.

Autor zvolil zabezpečení celého objektu tak, aby nejen splňovalo zákonné podmínky, ale také s ohledem na možné rozšíření zabezpečených oblastí. Organizace může bez větších úprav zřídit zabezpečené oblasti minimálně pro stupeň utajení Důvěrné v kterékoli kanceláři v objektu.

[58] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků* [online]. [cit. 19.1.24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

6 Výsledky

Analytická část práce potvrdila stanovenou hypotézu, že je možné vypracovat Projekt fyzické bezpečnosti s využitím stávající legislativy.

6.1 Vyhodnocení výzkumných otázek

Výzkumné otázky stanovené na počátku zpracování diplomové práce:

1. Je legislativní vymezení ochrany utajované informace dostatečné?
2. Je možné, dle současně platných zákonných nařízení dostatečně ochránit utajované informace?
3. Je možné, podle současné platné legislativy, vypracovat kvalitní Projekt fyzické bezpečnosti?

Na všechny uvedené otázky lze jednoznačně odpovědět kladně. Diplomová práce poukazuje na legislativní základ ochrany utajovaných informací. Ochranu utajovaných informací vymezuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a certifikaci technických prostředků. Platnost zákona je od 18. 10. 2005 s účinností od 01. 01. 2005. K dnešnímu dni byl 24 x novelizován. K tomuto zákonu se vztahuje Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Dále zákon upřesňují vyhlášky NBÚ. Jedná se o:

Vyhláška č. 363/2011 Sb., o personální bezpečnosti.

Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti

Vyhláška č 275/2022Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.

Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

Vyhláška 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Zákon a doplňující vyhlášky poskytují dostatečnou právní úpravu pro ochranu utajovaných informací a na jejich základě je možné, vypracovat kvalitní Projekt fyzické bezpečnosti, který je ze zákona nutný pro práci s utajovanou informací.

6.2 Porovnání výsledků s jinými studiemi

V souvislosti se zaměřením této kapitoly si autor vybral diplomovou práci, která je volně dostupná na internetu a je na velmi podobné téma.

Diplomová práce Ing. Josefa Kašpara je zpracována na téma „Ochrana utajovaných informací ve státní správě“[59]. Autor ve své práci vypracovává Projekt fyzické bezpečnosti v kategorii Důvěrné a porovnává zabezpečení v kategorii Tajné. Poměrně podrobně vysvětluje rozdíly v technickém zabezpečení těchto oblastí. Tato práce zaujme zvláště kvalitně zpracovanou analýzou rizik z pohledu fyzické bezpečnosti. Dále pak technická ochrana zabezpečené oblasti v kategorii Tajné je vypracována kvalitně a podrobně. Po komparaci technického zabezpečení lze konstatovat, že zabezpečení je na stejné úrovni. Určitý rozdíl je v instalaci EZS, kdy porovnávaná zabezpečená oblast je vybavena EZS typu 2 tedy SS92 = 2 body, instalace v rozsahu prostorová a plášťová ochrana. Tedy rozdílně než v této práci, kdy je u stejné zabezpečené oblasti instalována EZS v rozsahu prostorová a plášťová ochrana a tísňový systém nebo speciální televizní systém SS93 = 3 body. Důvodem tohoto zabezpečení je autor rozhodl o zabezpečení celého objektu prvky EZS, tak aby bodová hodnota objektu byla S3 = 3 body. Pokud bude celá budova zabezpečena EZS v rozsahu SS93 je možné, v případě nutnosti, zabezpečit další běžné kancelářské prostory a lehce vytvořit zabezpečenou oblast určenou pro ukládání utajovaných informací v kategorii Tajné.

6.3 Dopady práce pro výzkum a praxi

Diplomová práce přináší významný přínos v procesu přípravy a specifikace nových projektů v rámci fyzické bezpečnosti. Jednou z klíčových předností této práce je v její schopnosti poskytovat podrobné a strukturované informace, které hrají klíčovou roli při formování zadání projektu a výběru optimální technické struktury. Tato práce se tak může stát průvodcem pro týmy zabývající se vývojem a implementací nových projektů, poskytujíc jim nezbytné znalosti a směřování.

[59] KAŠPAR, Josef. *Ochrana utajovaných informací ve státní správě* [online]. 2020 [cit. 2024-01-30]. Dostupné z: https://is.ambis.cz/th/o6omt/. Diplomová práce. AMBIS vysoká škola, a.s. Vedoucí práce Jan KOLOUCH.

Dalším významným přínosem diplomové práce je její všestrannost v rámci studijních programů v oblasti bezpečnosti informací. Obsahuje dostatečně komplexní informace a analýzy, což ji činí vhodným studijním materiálem pro širší škálu úrovní studia specializovaného na bezpečnost informací.

Praktické návrhy prezentované v rámci diplomové práce jsou odvozeny z autentických zkušeností autora. Tato praktická orientace poskytuje konkrétní a aplikovatelné informace, které mohou přímo prospět projektovým týmům v oblasti informační bezpečnosti.

6.4 Omezení provedené studie

Předkládaná diplomová práce má několik omezení. Největším a velmi důležitým omezením je dostupnost informací ze zahraničí, potřebných pro porovnání postupů. Informace o ochraně utajovaných informací cizích mocností nejsou volně dostupné na internetu. V odborných článcích, které jsou k dispozici, je toto téma popisováno velmi nekonkrétně a spíše je zaměřeno na analýzu rizik, management řízení či všeobecně informacemi o rizicích. V teoretické části v kapitole pojednávající o legislativě Severoatlantické aliance, mohl autor čerpat pouze z předpisů, které jsou uveřejněny na webových stránkách NBÚ, a to z již dříve uvedených důvodů, že tato vojenská organizace své předpisy zpravidla nezveřejňuje.

V praktické části autor vytvořil návrh projektu fyzické bezpečnosti pro fiktivní státní organizaci, která pracuje s utajovanými informacemi ve stupni utajení TAJNÉ a PŘÍSNĚ TAJNÉ. Ačkoli autor má osobní pracovní zkušenosti s manipulací s utajovanými informacemi, tak z bezpečnostních důvodů, není možné čerpat informace z reálného prostředí, a proto je volen předložený postup.

Dalším omezením je doložení certifikátů technických prostředků. Technická dokumentace musí obsahovat certifikáty všech použitých technických prostředků. Společnosti, ve většině případů, certifikáty poskytují pouze na vyžádání. Z tohoto důvodu jsou uvedeny v diplomové práci pouze dva vzorové certifikáty.

7 Závěr

Diplomová práce se zaměřuje na problematiku ochrany utajovaných informací v rámci státní správy a hodnotí současný stav fyzické bezpečnosti. Hlavním cílem této práce bylo poskytnout komplexní informace o ochraně utajovaných informací a na základě shromážděných a systematizovaných dat, vlastních praktických zkušeností a odborných názorů navrhnout projekt fyzické bezpečnosti. Diplomová práce přináší podklady k aktuálním aktivitám v oblasti fyzické bezpečnosti, jež jsou utříděny a prezentovány, dále zobecnění zkušeností nabytých z realizovaných projektů v oblasti ochrany utajovaných informací a přenášení těchto zkušeností do konkrétního návrhu projektu fyzické bezpečnosti.

Diplomová práce poukazuje na fakt, že ochrana utajovaných informací musí být zajištěna systémově a musí být logicky začleněna do vnitřních struktur řízení, a to už v etapě zavádění systému ochrany utajovaných informací do praxe, tím je míněna realizace požadavků právních předpisů ve všech oblastech zajištění ochrany UI, zpracování dokumentace a její schválení NBÚ či NUKIB. Dozorová činnost těchto úřadů hraje velmi významnou roli. Další etapou je udržování a aktualizace po celou potřebnou dobu. V této etapě se jedná hlavně o důsledné kontroly, školení personálu na všech úrovních a aktualizace všech systémů.

Touto prací se autor snaží upozornit na současný stav ochrany utajovaných informací a navrhnout perspektivní zlepšení procesu fyzické bezpečnosti při realizaci projektů v oblasti fyzické bezpečnosti. Cílem je také přinést konkrétní doporučení pro zabezpečení Projektů fyzické bezpečnosti, včetně výběru technických prostředků dostupných na trhu.

Diplomová práce může posloužit jako podnět pro odpovědné osoby ve státní správě při řešení otázek fyzické bezpečnosti a při tvorbě nových interních předpisů a norem pro ochranu utajovaných informací a celkovou bezpečnost úřadu. Je nezbytné, aby subjekty orgánů státu a jejich odpovědné osoby, si uvědomily, že kromě odborných znalostí v oblasti ochrany utajovaných informací, je také velmi důležité těchto znalostí využívat v každodenní praxi.

Klíčovým aspektem efektivního řízení ochrany utajovaných informací je porozumět váze a hodnotě každé informace a rozhodnout, jak ji zabezpečit v souladu s platnou legislativou. Proto autor navrhuje, aby byla výuka o ochraně utajovaných informací zařazena na vysokých školách s bezpečnostním zaměřením, a dále aby případně přibylo více odborných kurzů a pedagogů na všech úrovních vzdělání, s cílem propojení teorie s praxí.

Jako opatření pro dosažení tohoto cíle by mělo být zapojení vrcholového managementu, specializovaného v oblasti ochrany utajovaných informací, do výuky.

Celkový přínos této práce spočívá v její schopnosti sloužit jako užitečný zdroj informací při přípravě zpracování Projektů fyzické bezpečnosti.

8 Seznam použitých zdrojů

1. ENISA. *Definition of Cybersecurity* [online]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

2. 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.

3. *Zákon č. 148/1998 Sb. o ochraně utajovaných skutečností*. [online]. Dostupné z:https://www. zakonyprolidi.cz/cs/1998-148/zneni-0#f1877594

4. *Latinský slovník*. [online]. [cit. 10. 04. 23]. Dostupné z: http://latinsky-slovnik.latinsky.cz/cesko-latinsky/formatio.html

5. BAWDEN, David a Lyn ROBINSON. *Úvod do informační vědy*. Doubravník: Flow, 2017. ISBN 978-80-88123-10-1.

6. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32016R0679.

7. Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1083-vyhlaska-c-4052011-sb-o-prumyslove-bezpecnosti

8. Vyhláška č. 363/2011 Sb., o personální bezpečnosti. Dostupné z: https://www.zakonyprolidi.cz/cs/2011-363

9. Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1088-vyhlaska-c-5292005/

10. Vyhláška č.275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Dostupné z: https://www.zakonyprolidi.cz/cs/2022-275

11. Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací. Dostupné z: https://www.nbu.cz/download/pravni-predpisy/432_2011.pdf

12. Vyhláška č. 525/2005 Sb ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. Dostupné z: https:/ /nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

13. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

14. JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

15. MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN isbn978-80-7478-817-8.

16. ŠEBESTA, Václav.; ŠTVERKA, Václav.; STEINER, František.; ŠEBESTOVÁ, Marie. *Systémy řízení bezpečnosti informací*, Část 3: *Směrnice pro management rizik bezpečnosti informací podle BS 7799-3*:2005 s komentářem k managementu rizik v ISMS. Praha: Český normalizační institut, 2007.

9 Seznam obrázků, tabulek a zkratek

9.1 Seznam obrázků

9.2 Seznam tabulek

9.3 Seznam použitých zkratek

CCTV..... SPECIÁLNÍ KAMEROVÉ SYSTÉMY

ČR..... ČESKÁ REPUBLIKA

EKV..... ELEKTRONICKÁ KONTROLA VSTUPU

EPS..... ELEKTRONICKÉ POŽÁRNÍ SYSTÉMY

EU..... EVROPSKÁ UNIE

EZS..... ELEKTRICKÁ ZABEZPEČOVACÍ SIGNALIZACE

FB..... FYZICKÁ BEZPEČNOST

GDPR..... GENERAL DATA PROTECTION REGULATION

IKS..... INFORMAČNÍ A KOMUNIKAČNÍ SYSTÉMY

IS..... INFORMAČNÍ SYSTÉM

IT..... INFORMAČNÍ TECHNOLOGIE

KS..... KOMUNIKAČNÍ SYSTÉM

MV..... MINISTERSTVO VNITRA

NP..... NADZEMNÍ PATRO

NATO..... SEVEROATLANTICKÁ ALIANCE

NBÚ..... NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

NÚKIB..... NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

PFB..... PROJEKT FYZICKÉ BEZPEČNOSTI

PP..... PODZEMNÍ PATRO

PT..... PŘÍSNĚ TAJNÉ

T..... TAJNÉ

UI..... UTAJOVANÁ INFORMACE

ZO..... ZABEZPEČENÁ OBLAST

ZOUI..... ZÁKONA O OCHRANĚ UTAJOVANÝCH INFORMACÍ

Přílohy

Příloha č. 1 Vzor certifikátu technického prostředku

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT

technického prostředku

Evidenční číslo: T0058/2021

Bezpečnostní rolovací mříž
typ RL A - RC 2

(Název a typové označení technického prostředku)

Výrobce: LIBRAX, společnost s ručením omezeným

Sídlo: Ještědská 103/85
460 08 Liberec
IČ: 40231976

Držitel: LIBRAX, společnost s ručením omezeným

Sídlo: Ještědská 103/85
460 08 Liberec
IČ: 40231976

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

2

Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:

SS3=2, SS4=1

Platnost certifikátu do: 28.02.2024

Datum vydání certifikátu: 29.06.2021

Náměstek ředitele
Národního bezpečnostního úřadu

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Ing. Jaromír Kadlec, CSc.

016248

Přílohy 1/1

(Příloha je nedílnou součástí certifikátu a lze je reprodukovat pouze společně)