Kompromitující vyzařování z hlediska kybernetické bezpečnosti

Bc. Marian Jačo

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Marian Jačo**
Osobní číslo:	**L19640**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kompromitující vyzařování z hlediska kybernetické bezpečnosti**

Zásady pro vypracování

1. Vymezte základní pojmy a legislativu týkající se kybernetické bezpečnosti.
2. Seznamte se s problematikou kompromitujícího vyzařování.
3. Zhodnoťte současný stav zabezpečení vybrané budovy z hlediska ochrany proti úniku utajovaných informací.
4. Navrhněte opatření ke zlepšení stávajícího stavu vzhledem k předchozímu bodu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. SILBERBERG, Adam. *Všichni máme právo na soukromí: konspirativní techniky*. Praha: Restart project, 2018. ISBN 978-80-270-4239-5.
3. WHITMAN, Michael E. a Herbert J. MATTORD. *Management of Information Security. 5. vydání*. Boston: Cengage Learning, 2017. ISBN 978-1-305-50125-6.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 7. 5. 2021

Jméno a příjmení studenta: Bc. Marian Jačo

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou kompromitujícího vyzařování. Je rozdělena do dvou částí, na část teoretickou a praktickou. V teoretické části se diplomová práce věnuje problematice legislativy v oblasti ochrany utajovaných informací a kompromitujícího vyzařování. Dále se teoretická část zabývá možnostmi zneužití kompromitujícího vyzařování a ochranou proti němu. Praktická část diplomové práce je zaměřena na současný stav zabezpečení vybrané budovy z hlediska kompromitujícího vyzařování a je zde provedena analýza hrozeb. Na základě analýzy je poté navrhnuto řešení zabezpečení jednotlivých hrozeb.

Klíčová slova: Kompromitující vyzařování, ochrana utajovaných informací, elektromagnetické vyzařování, akustické vyzařování, zabezpečení, informace, kybernetický prostor, kybernetická ochrana.

ABSTRACT

The diploma thesis deals with the issue of compromising emanation. It is divided into two parts, a theoretical and a practical part. In the theoretical part, the diploma thesis deals with the issue of legislation in the field of protection of classified information and compromising emanation. Furthermore, the theoretical part deals with the possibilities of misuse of compromising emanation and protection against it. The practical part of the diploma thesis is focused on the current state of security of the selected building in terms of compromising emanation and there is an analysis of threats. Based on the analysis, a security solution for individual threats is then proposed.

Keywords: Compromising emanation, protection of classified information, electromagnetic emanation, acoustic emanation, security, information, cyberspace, cyber protection.

„To, že něco nevidíme, nebo o tom nevíme, neznamená, že to neexistuje.“

Na tomto místě bych chtěl poděkovat panu Ing. Petru Baloghovi a panu Ing. Jindřichu Rozsypalovi za jejich odborné rady, vstřícnost a ochotu při vzájemné komunikaci. Dále bych chtěl poděkovat panu Ing. Pavlovi Tomáškovi, Ph.D. za jeho odborné vedení diplomové práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Diplomová práce se věnuje problematice kompromitujícího vyzařování elektronických zařízení. Již od prvních počátků, kdy lidstvo začalo existovat, bylo potřeba znát a předávat si mezi sebou důležité informace. Bez informací by člověk v dobách pravěku nemohl přežít. Velmi důležitými sděleními byly informace jak rozdělat oheň, případně jak se ubránit šelmám. Postupem doby se informace začaly předávat pomocí písmen vytesaných do kamenů či napsanými na kůže, tkaniny, papyrus a nakonec i papír.

V dobách kdy proti sobě začali lidé bojovat a začaly vznikat nároky na území, se informace předávaly více zabezpečeně. Prvními typy zabezpečení komunikace na dálku byly kouřové signály. Dále ve středověku byly informace posílány přes spojky, a svitky papíru byly opatřeny pečetí majitele. Důležité bylo předávat vojenské či jinak důležité informace o postupu jednotek, či rozmístění jednotek protivníka.

Moderní technologie již v dobách 2. světové války přinesly lidstvu mnoho výhod, jak spolu komunikovat na dálku. Bylo čím dál více důležité své operační plány a rozmístění jednotek nějak zabezpečit. V těchto dobách vznikl fenomén šifrování. Asi nejznámějším šifrovacím přístrojem během 2. světové války byl přístroj Enigma. Pro jeho dešifrování bylo nutné jej získat a to tak, aby o tom protistrana nevěděla a nemohla tak šifry změnit.

Čím více se moderní technologie rozvíjely, tím lepší měli lidé přístup k informacím. V dobách nástupu počítačů mohl člověk své myšlenky a data ukládat přímo do pevných disků počítače nebo na diskety a později CD nebo flash disky. V době vzniku internetu se úložištěm stal vzdálený server, ke kterému má přístup v podstatě kdokoliv.

Digitalizací, vzdáleným přístupem a čím dál větší závislostí na moderních výpočetních technologiích ovšem vznikl problém bezpečnosti těchto uložených a zpracovávaných dat. Případný útočník je schopen vynaložit veškeré možné úsilí, aby se dostal k datům a heslům uživatele. Toto riziko také platí pro státy, které si chtějí uchovávat své strategické informace. Softwarové nebezpečí je pouze jedním menším odvětvím, kterému se bezpečnost informací může věnovat. Ne příliš známým pojmem v podvědomí lidstva je kompromitující vyzařování, které je už jen pro jeho neznalost větším problémem, než se může zdát. Kompromitující vyzařování ovšem není tak jednoduché zachytit, dekódovat a zobrazit. Z tohoto důvodu je pro obyčejné uživatele menším nebezpečím jako softwarová hrozba, ale pro státy, případně aliance, je kompromitující vyzařování velkou hrozbou, jelikož útočník (např. jiný stát) má mnoho prostředků a času takovým způsobem data získat.

Teoretická část diplomové práce je zaměřena na zpracování literární rešerše k tématu kompromitujícího vyzařování. Problematika kompromitujícího vyzařování v teoretické části je rozdělena do 4 kapitol, základní pojmy, legislativa, kybernetická bezpečnost a kompromitující vyzařování V první kapitole jsou popsány základní pojmy důležité pro pochopení samotné problematiky. V kapitole legislativy jsou popsány nejdůležitější zákony a vyhlášky týkající se problematiky kybernetické bezpečnosti, ochrany utajovaných informací a kompromitujícího vyzařování. V kapitole kybernetické bezpečnosti jsou popsány základní vlastnosti kybernetického prostoru a jeho bezpečnosti. V poslední kapitole je definována problematika kompromitujícího vyzařování a jsou zde popsány možnosti získání dat vlivem tohoto vyzařování.

V praktické části je diplomová práce zaměřena na zabezpečení vybrané budovy z hlediska ochrany utajovaných informací vlivem kompromitujícího vyzařování. Prostřednictvím analýzy hrozeb byly vybrány největší hrozby pro vybraný objekt a tyto hrozby byly následně ošetřeny různými metodami. Hlavním cílem diplomové práce je přiblížit problematiku kompromitujícího vyzařování na konkrétním příkladu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

V této kapitole diplomové práce budou uvedeny základní pojmy pro lepší orientaci v odborných textech. Pro kybernetickou bezpečnost je nezbytné znát alespoň nejdůležitější pojmy, jakými jsou:

- Odpovědnost je definována jako mechanismus pro řízení přístupu, který zajistí, že všechny provedené autorizované i neautorizované akce v systému budou dohledatelné vůči odpovědné identitě (osobě), (Whitman a Mattord, 2017).
- Autorizace je mechanismus řízení přístupu. Tento mechanismus představuje shodu ověřené osoby se seznamem infomačních aktiv a také s odpovídající úrovní přístupu (Whitman a Mattord, 2017).
- Dostupnost znamená, že informace musí být vždy dostupná autorizované osobě v nezměněné a původní podobě bez jakéhokoliv rušení a překážek (Whitman a Mattord, 2017).
- Triáda C.I.A. je průmyslový standard pro počítačovou bezpečnost, který se používá již od výroby prvního sálového počítače. Tato norma je založená na třech vzájemně se propojujících podmínkách. Těmito podmínkami jsou důvěrnost, integrita a dostupnost. Tyto tři podmínky zajišťují celkovou bezpečnost systému (Whitman a Mattord, 2017).
- Důvěrnost je pojem, který popisuje, jak jsou data chráněna před prozrazením. Tato podmínka uživateli systému zabezpečuje, že informaci dostává z autorizovaného zdroje a že informace nebyla prozrazena neoprávněným osobám či systémům (Whitman a Mattord, 2017).
- Integrita je atribut, který zajišťuje, že informace se k uživateli dostala nezměněná, nepoškozená a celá (Whitman a Mattord, 2017).
- Informační systém je celek, který je funkční a zjišťuje cílevědomé a systematické shromažďování, uchovávání, zpracovávání a zpřístupňování informací. Informační systém zahrnuje nosiče dat, technické a programové prostředky, technologie a postupy. Dále také zahrnuje veškeré související normy a pracovníky (Doucek, Konečný a Novák, 2019).

- Informační a komunikační technologie je veškerá technika (a její programové vybavení), která se zabývá zpracováním a přenosem informací (Doucek, Konečný a Novák, 2019).
- Elektromagnetická kompatibilita (EMC) je vysokofrekvenční rušení nebo analýza elektromagnetické interference, které souvisí s elektrickým zařízením. Elektromagnetická kompatibilita snižuje neúmyslné generování, šíření a příjem elektromagnetické energie v elektrickém systému (Vuagnoux a Pasini, 2009).
- Šifrování dat je jedním ze základních nástrojů na ochranu dat před jejich kompromitací. Data, která jsou zašifrovaná, jsou k dispozici pouze tomu uživateli, který zná klíč pro jejich rozšifrování (Autocont, 2021).
- Analýza chování uživatelů, která je označována anglickou zkratkou UEBA (User and Entity Behavioral Analyse), označuje nástroj k identifikaci typického a atypického chování lidí, ale také zařízení. Chování osob a zařízení je poměrově hodnoceno v reálném čase pomocí výpočtu bezpečnostního skóre (Autocont, 2021).

2 LEGISLATIVA

Problematikou kompromitujícího vyzařování se zabývá zákon č. 412/2005 Sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, který je v účinnosti od 1. 1. 2006. Dalším zákonem, který se okrajově dotýká problematiky z hlediska kybernetiky, je zákon č. 181/2014 Sb. zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zkráceně zákon o kybernetické bezpečnosti).

2.1 Oblast kompromitujícího vyzařování

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti se zabývá zásadami pro stanovení utajovaných informací. Stanovuje také podmínky přístupu k těmto informacím a další požadavky na jejich ochranu (Maisner, 2015).

Pro problematiku kompromitujícího vyzařování je nejdůležitější § 45 toho zákona:

„(1) Ochranou utajovaných informací stupně utajení Přísně tajné, Tajné nebo Důvěrné před jejich únikem kompromitujícím vyzařováním je zabezpečení elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu.

(2) Je-li ochrana utajované informace před únikem kompromitujícím vyzařováním zabezpečena stínicí komorou, musí být tato komora certifikována Národním úřadem pro kybernetickou a informační bezpečnost [§ 46 odst. 1 písm. e)].

(3) Ověřování způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním zajišťuje Národní úřad pro kybernetickou a informační bezpečnost při certifikaci informačního systému nebo kryptografického prostředku, při schvalování projektu bezpečnosti komunikačního systému nebo na základě odůvodněné písemné žádosti orgánu státu nebo podnikatele v souvislosti s ochranou utajovaných informací.

(4) K provádění měření možného úniku utajovaných informací podle odstavce 3 může Národní úřad pro kybernetickou a informační bezpečnost uzavřít s orgánem státu nebo podnikatelem smlouvu podle § 52 o zajištění této činnosti.

(5) K provádění měření zařízení, zabezpečené oblasti nebo objektu podle odstavce 3, které jsou provozovány nebo užívány zpravodajskými službami, jsou oprávněny zpravodajské služby. V těchto případech není vyžadováno uzavření smlouvy podle § 52. Pro potřeby certifikace informačního systému nebo kryptografického prostředku, nebo při schválení

projektu bezpečnosti komunikačního systému předají zpravodajské služby Národnímu úřadu pro kybernetickou a informační bezpečnost zprávy o provedeném měření včetně jeho výsledku.

(6) Při provádění měření podle odstavce 5 jsou zpravodajské služby povinny dodržovat ustanovení tohoto zákona, prováděcích právních předpisů a bezpečnostních standardů Národního úřadu pro kybernetickou a informační bezpečnost.“ (Maisner, 2015).

2.2 Oblast kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti se oproti zákonu č. 412/2005 více zabývá problematikou používání informační infrastruktury, aby tyto systémy byly co nejodolnější vůči případnému napadení, lidské chybě či živelné pohromě (Autocont, 2021).

V tomto zákoně je v § 7 definována kybernetická bezpečnostní událost a kybernetický bezpečnostní incident:

„1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací1).

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací1) v důsledku kybernetické bezpečnostní události.

(3) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.“ (Maisner, 2015).

2.3 Vyhlášky Národního bezpečnostního úřadu

Národní bezpečnostní úřad (dále jen NBÚ) je orgánem výkonné moci. Je zařazen mezi ústřední úřady a také mezi správní úřady. NBÚ vydává osvědčení o bezpečnostní způsobilosti jak fyzickým osobám, tak i podnikatelům. Tímto garantuje, že u držitelů těchto osvědčení nejsou zjištěny skutečnosti, které by bránily těmto osobám přístupu k utajovaným informacím nebo vykonávat citlivé činnosti. Kontrolu nad NBÚ dle zákona 412/2005 Sb., který nabyl účinnosti 1. ledna 2006, vykonává Poslanecká sněmovna, která k tomuto účelu zřídila stálou komisy pro kontrolu činnosti NBÚ (Národní bezpečnostní úřad, 2021).

NBÚ vydává vyhlášky, které se týkají bezpečnosti informací a provozu informačních a komunikačních zařízení (Národní bezpečnostní úřad, 2021)

Vyhláška Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Touto vyhláškou je stanovena certifikace na informační a komunikační systémy, které nakládají s utajovanými informacemi. Dále jsou zde stanoveny podmínky a pravidla pro schvalování projektů bezpečnosti a podmínky pro ochranu utajovaných informací v zobrazovacím zařízení, kopírovacím zařízení, v psacím stroji s pamětí a ochrany utajovaných informací před jejich únikem vlivem kompromitujícího vyzařování. Dále jsou zde popsány prováděcí certifikace stínících komor (Česko, 2005a).

Část čtvrtá této vyhlášky se zabývá přímo problematikou kompromitujícího vyzařování, kde je definováno kompromitující vyzařování jako: „*Kompromitující vyzařování je vyzařování elektrických a elektronických zařízení, které by mohlo způsobit únik utajované informace stupně utajení Přísně tajné, Tajné nebo Důvěrné.“* (Česko, 2005a).

Způsob hodnocení způsobilosti elektronických zařízení z hlediska úniku utajovaných informací vlivem kompromitujícího vyzařování se provádí měřením úrovně vyzařovaného elektromagnetického pole a tyto naměřené údaje se porovnávají s bezpečnostními standardy. Pokud by v průběhu měření byly zjištěny jakékoliv nedostatky, vyzve úřad žadatele k jejich odstranění (Česko, 2005a).

Vyhláška Národního bezpečnostního úřadu č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, která se zabývá náležitostmi pro certifikaci kryptografického prostředku, kde se přesně definuje, co žádost o tuto certifikaci musí obsahovat. Dále také obsahuje popis náležitosti žádosti o certifikaci kryptografického pracoviště. V této vyhlášce je definována dokumentace, která je nezbytná k provedení certifikace kryptografického prostředku (Česko, 2005b)

Vyhláška Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Tato vyhláška bodově stanovuje hodnocení jednotlivých opatření v oblasti fyzické bezpečnosti. Paragraf 2 této vyhlášky vymezuje základní pojmy v oblasti fyzické bezpečnosti, jako jsou například:

- **Objekt**, kterým se rozumí budova nebo jiný ohraničený prostor, kdy v tomto objektu se nacházejí zpravidla zabezpečené nebo jednací oblasti.

- **Hranicí objektu** se rozumí plášť budovy, fyzická bariéra případně oplocení nebo jinak viditelná hranice.
- **Vstup** do zabezpečené oblasti nebo jednací oblasti je stavebně nebo jinak viditelně ohraničený objekt.
- **Hrozba** je možnost zneužití nebo vyzrazení utajované informace, ke které dojde při narušení fyzické bezpečnosti (Česko, 2005c).

Vyhláška také stanovuje zabezpečení objektu a zabezpečené oblasti z hlediska přístupu, kdy zařazení zabezpečené oblasti nebo hranici objektu do příslušné třídy stanoví odpovědná osoba, nebo jí pověřená osoba (Česko, 2005c).

Třídy zabezpečených oblastí dle zákona č. 412/2004 Sb.:

- přísně tajné,
- tajné,
- důvěrné,
- vyhrazené (Maisner, 2015).

Paragraf 3 této vyhlášky vzhledem k třídám zabezpečení určuje, jakými prostředky budou tyto třídy zabezpečeny vzhledem k tomu, zda se jedná o objekt nebo zabezpečenou oblast.

Objekt je zabezpečován dle druhu kategorie tohoto objektu, dle charakteru hranice objektu a také v závislosti na vyhodnocení rizik:

- Vyhrazené – zabezpečení mechanickými zábrannými prostředky.
- Důvěrné a tajné – zabezpečení pomocí elektrické zabezpečovací signalizace a mechanickými zábrannými prostředky.
- Přísně tajné – zabezpečení mechanickými zábrannými systémy, elektrické zabezpečovací prostředky, speciální televizní systémy, systémy pro kontrolu vstupů, zařízení pro požární signalizaci. Speciální televizní systémy lze také nahradit tísňovými systémy (Česko, 2005c).

Dále se tato vyhláška zabývá zabezpečením technických zařízení, režimovými opatřeními pro vstup osob a vozidel, režimem manipulace s klíči a identifikačními prostředky (karty pro vstup). V příloze této vyhlášky jsou definovány úschovné objekty a typy jejich zámků (Česko, 2005c).

Vyhláška Národního bezpečnostního úřadu č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací. Touto vyhláškou se stanovují podrobnosti o odborné zkoušce pro práci s kryptografickým materiálem, způsoby a manipulace s tímto materiálem a podrobnosti způsobu vyznačování náležitostí na utajované informaci z oblasti kryptografické ochrany (Česko, 2011)

2.4 Národní úřad pro kybernetickou bezpečnost

Ústředním správním orgánem pro kybernetickou bezpečnost, který také zahrnuje ochranu utajovaných informací je Národní úřad pro kybernetickou bezpečnost (NÚKIB). NÚKIB v oblasti ochrany utajovaných informací řeší oblast informačních a komunikačních systémů a kryptografické ochrany. Zahrnuje také problematiku a správu veřejně regulované služby v rámci družicového systému Galileo. Úřad vznikl na základě zákona 205/2017 Sb., kterým se mění zákon č. 191/2014 Sb., o kybernetické bezpečnosti (NÚKIB, 2021).

Zákon č. 205/2017 Sb., o kybernetické bezpečnosti se zabývá zajišťováním bezpečnosti elektronických komunikací a informačních systémů. Tento zákon také zpracovává příslušné předpisy Evropské unie (NÚKIB, 2021).

2.5 Směrnice NATO

Země, které jsou členy Severoatlantické aliance (NATO) musí zajišťovat dodržování bezpečnostních principů a bezpečnostních standardů uvedených v předpise C -M (2002)49. Tento předpis je sdělením generálního tajemníka, který stanovuje hlavní zásady a minimální bezpečnostní standardy (Balogh, 2018)

Směrnice AC-35-D -2000-REV8 – tato směrnice se zabývá personální bezpečností. Je osmou revizí této směrnice a nahrazuje předchozí směrnici AC-35-D -2000-REV6. Jsou zde uvedeny aspekty týkající se prověrek personální bezpečnosti, kritéria pro posouzení způsobilosti, požadavky na prodloužení platnosti jednotlivých prověrek. Směrnice také řeší povolení přístupu k utajovaným informacím NATO (AC/35-D /2000-REV8, 2020).

Směrnice AC-35-D -2001-REV3 – směrnice, kterou vydal bezpečnostní výbor NATO, upravuje fyzickou bezpečnost. Dle směrnice všechny prostory budov, kanceláří, místností a dalších oblastí, ve kterých jsou uložené utajované informace a materiály, nebo je s těmito materiály nějak manipulováno, musí být chráněny vhodnými fyzickými bezpečnostními opatřeními (AC/35-D /2001-REV3, 2020).

Směrnice AC-35-D -2002-REV5 – tato směrnice vydaná Bezpečnostním výborem NATO se zabývá aspekty klasifikací a označovaní informací, kontrolou a nakládáním s informacemi, kopírováním, překlady, příjmem a záznamem utajovaných informací. Dále se zabývá narušením a kompromitací informací a také jejich přenosem a šířením (AC/35-D /2002-REV5, 2020).

Směrnice AC-35-D -2003-REV5 – tento dokument se zabývá výběrovými řízeními a pronájmem zakázek v oblasti utajovaných informací. Určuje podmínky pro výběr subdodavatelů a dodavatelů zařízení pro výstavbu a ochranu zařízení pracujících s utajovanými informacemi (AC/35-D /2003-REV5, 2020).

Směrnice AC-35-D -2004-REV3 – směrnice vymezuje důležité aspekty pro nakládání s utajovanými informacemi. Přímo definuje důležité podmínky pro pojem informace, kterými jsou důvěrnost, integrita, dostupnost, autentizace, nepopiratelnost. Určuje také požadavky pro podpůrné systémové služby a zdroje včetně podpory komunikačních a informačních systémů (AC/35-D /2004-REV3, 2020).

Směrnice AC-35-D -2005 REV3 – směrnice určuje bezpečnostní politiku v rámci komunikačních a informačních systémů NATO. Určuje role uživatelů od správce systému až po obsluhu. Popisuje požadavky na bezpečnostní akreditace systémů, bezpečnostní dokumentaci a řízení bezpečnostních rizik. Nedílnou součástí je také na požadavky pro tvorbu bezpečnostního auditu těchto systémů (AC/35-D /2005-REV3, 2020).

3 KYBERNETICKÁ BEZPEČNOST

Kybernetickou bezpečnost chápeme jakou určitý souhrn právních, organizačních, technických opatření, které slouží k zajištění ochrany kybernetického prostoru. Nedílnou součástí kybernetické bezpečnosti jsou také vzdělávací prostředky. Kybernetickou bezpečnost dle normy ISO/IEC 27101 můžeme chápat jako soubor aktiv vedoucích k zajištění a udržení stability společnosti, k udržování kontinuity a ochrany jejích členů před všudypřítomnými a neodmyslitelnými riziky digitalizace. Pokud by došlo k narušení kybernetické bezpečnosti, jedná se o kybernetický incident. Rozlišujeme pět typů bezpečnostních kybernetických incidentů:

- Lidská chyba – k tomuto bezpečnostnímu incidentu dochází v důsledku neúmyslné operace, která poškodila počítačový systém, službu nebo síť.
- Prolomení ochrany důvěrnosti dat – data, která jsou uložena v systému, jsou kompromitována nebo zcizena.
- Závady v systému nebo špatná funkcionalita – tento incident nastane v případě, že napadený/poškozený systém nebo síť způsobí škodu systému třetí strany nebo systém dodavatele není funkční.
- Poškozující aktiva – řadíme zde například kybernetickou šikanu na sociálních sítích nebo snahu o získání přístupu k datům za účelem jejich smazání, případně také kybernetický podvod.
- Ztráta dostupnosti dat nebo porušení jejich integrity – nastane v případě, že data, která jsou uložená v systému, byla poškozena nebo smazána. K tomuto incidentu také dojde v případě, že je systém spravován nebo hostován třetí stranou (Doucek, Konečný a Novák, 2019).

Kybernetický prostor

Kybernetický prostor lze chápat jako prostor veřejný. To ovšem znamená, že kybernetický prostor nemá vlastníka. Není řízen úřadem, osobou ani národem. Z důvodu toho, že kybernetický prostor nemá určeného přímého vlastníka, musí být bezpečnostní aktiva koordinována mezi různými zúčastněnými subjekty. Subjekty v kybernetickém prostoru by měly mezi sebou sdílet informace o možných rizicích a anomáliích, které by mohly narušit bezpečnostní prostor (Doucek, Konečný a Novák, 2019).

Kybernetický prostor má několik základních charakteristik s určitými významnými specifiky:

- Asymetričnost – jakákoliv činnost provedená v kybernetickém prostoru může mít významný dopad na kteréhokoliv uživatele sítě. Tato vyvinutá činnost je bez ohledu na význam a důvěryhodnost uživatele, který činnost způsobil.
- Anonymita – není zcela jasně prokazatelná a garantovaná identita uživatele, který v kybernetickém prostoru vyvíjí aktivitu.
- Interakce – v kybernetickém prostoru interaktivní činnosti vytváří znalosti a vedou k významnému ovlivnění ostatních uživatelů.
- Okamžitost – jakákoliv provedená činnost v kybernetickém prostoru může mít okamžitý celosvětový dopad.
- Neexistence hranic – vytvořené aktivity v kybernetickém prostoru nejsou omezovány žádnou jurisdikcí, nebo suverenitou.
- Volný vstup i ukončení pobytu v něm – kdykoliv a kdokoliv může do prostoru vstoupit a kdykoliv může kybernetický prostor opustit (Doucek, Konečný a Novák, 2019).

4 KOMPROMITUJÍCÍ VYZAŘOVÁNÍ

Již v 19. století byla objevena problematika kompromitujícího vyzařování, přesněji elektromagnetického. Z důvodu rozsáhlého používání kabelových telefonů se stávalo, že v hovoru dvou účastníků mohlo být slyšeno někoho dalšího. Dříve se tomuto problému říkalo přeslechy. V průběhu 2. světové války začala americká armáda využívat dálnopisnou komunikaci šifrovacím zařízením typu BELL 131-B2. Alexander Graham Bell později objevil, že tento stroj vyzařuje elektromagnetické vyzařování, které lze zachytit, dešifrovat a na dálku obnovit přenášené texty. Pomocí osciloskopu inženýři ze společnosti Bell, byly schopni zachytit elektromagnetické vyzařování v budově přes ulici na vzdálenost přibližně 25 metrů a získali tak až 70 % čistého textu přenášeného tímto zařízením (Vuagnoux a Pasini, 2009; History of codename: Tempest, 2020).

Kompromitující vyzařování je definováno jako neúmyslné elektromagnetické vyzařování zařízení, kdy toto zařízení při svém provozu vyzařuje elektromagnetické vlny, které mohou být zachyceny a analyzovány. Tyto signály mohou odhalit přenášené, přijímané nebo zpracovávané informace, které mohou poškodit zájmy organizace. Tyto signály může vyzařovat jakékoliv zařízení zpracovávající informace. Kompromitující vyzařování není přenášeno pouze pomocí elektromagnetických vln, ale jedná se i o akustické nebo optické kompromitující vyzařování. (G. Kuhn, 2003).

Elektromagnetické vyzařování se může dělit na přímé vyzařování a nepřímé vyzařování. (G. Kuhn, 2003).

Přenos kompromitujícího vyzařování se dá rozdělit dle způsobu přenášení:

- vzduch,
- vodní potrubí (kovové potrubí),
- kovové armatury,
- vzduchotechnika,
- rozvody topení,
- elektrické rozvody (G. Kuhn, 2003).

V informačních technologiích jsou nejohroženějšími zařízeními:

- monitor,

- klávesnice,
- pevný disk,
- síťové prvky (LAN kabely, Wi-Fi),
- Počítačové kabely (VGA, DVI apod.), (G. Kuhn, 2003).

V informačních technologiích jsou nejohroženější kabely daného počítače. Veškeré propojení klávesnic, zdrojů a kabelů propojujících monitor s počítačem.

4.1 Tempest

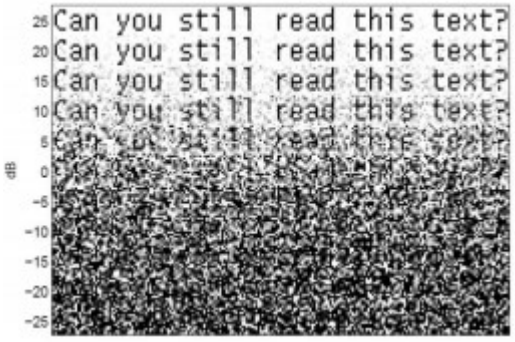
Tempest může být zkratkou z anglického Telecommunications Elektronic Material Protected from Emanating Spurious Transmissions, nebo také zkratkou ze standardu Transient Elektromagnetic Pulse Emanation Standart. Slovem TEMPEST byl nazván program ochrany informací před únikem vlivem kompromitujícího vyzařování a přímo souvisí s elektronickým vyzařováním (Webopedia, 2020)

Mezi odborníky na danou problematiku, se nejčastěji setkáme s pojmem tempestové měřící zařízení, tempestované zařízení nebo tempestový útok. Tempestové měřící zařízení se nejčastěji skládá z přijímače a antény, které monitorují elektromagnetické vyzařování. Tempestované zařízení znamená, že námi použité zařízení (například počítač) splňuje požadavky na omezení kompromitujícího zařízení. Tempestový útok je zneužití vyzařovaného elektromagnetického pole k získání dat (Balogh, 2018).

4.2 Odposlech kompromitujícího vyzařování

Pro potenciálního útočníka, který se zaměřuje na únik informací vlivem kompromitujícího vyzařování, existuje několik možností a zásad pro jejich získání. Jednou ze zásad je znalost kmitočtů, kde tyto kmitočty nesou utajovanou informaci. Případný útočník může tyto kmitočty zjistit experimentálně nebo výpočtem. Důležitým nástrojem pro získání kompromitujících signálů je sledovací zařízení na bázi přijímače a záznamového zařízení. Účinnost tohoto zařízení lze zvýšit pomocí antény s vysokým ziskem, která je přímo nasměrovaná na cílové místo. Možností pro útočníka získat kompromitující vyzařování je vyhledávat ho v takzvané tiché části kmitočtového spektra. Tato část spektra je taková, kde se nevyskytují žádné vysílače nebo radiové služby. Aby útočník potlačil nechtěné signály, které se nacházejí v okolí, je možno tyto signály potlačit použitím pásmových zádrží. Pásmové zádrže se používají v případech, kdy se potřebný signál získává z pásma určeného

pro vysílání rozhlasového nebo televizního signálu. Pro oddělení požadovaného vyzařování od rušivých signálů se mohou používat metody zpracování signálu. Pokud se v zachyceném signálu objevuje šum, klesá rozpoznatelnost signálu. Špatnou čitelnost signálu v šumu zobrazuje obrázek 1 (Balogh, 2018).



Obrázek 1: Čitelnost textu signál/šum (G. Kuhn, 2003)

V případě městské zástavbě je úspěšnost zachycení kompromitujícího vyzařování v řádech desítek metrů. Vždy ovšem záleží na technickém vybavení protivníka (Balogh, 2018).

4.3 Metody zneužití kompromitujícího vyzařování

V této kapitole se diplomová práce zabývá metodami získávání a odposlechů dat uživatelů vlivem kompromitujícího vyzařování. Mezi nejčastější a nejlépe realizované metody patří například Wiretapping.

4.3.1 Wiretapping

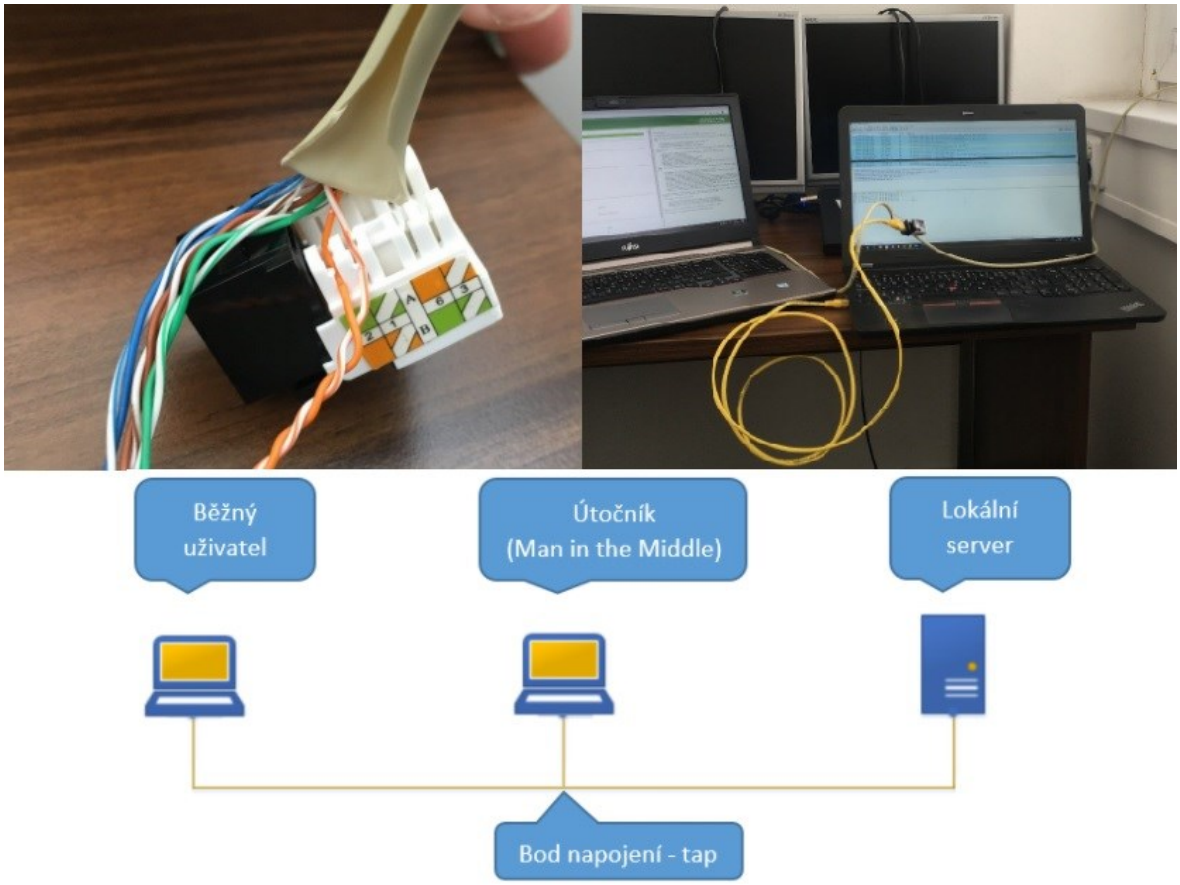
Je jeden z jednoduchých a primitivních odposlechů v počítačové síti. K realizaci této metody je zapotřebí mít přístup ke kabelům nejčastěji kroucené dvoulince. Tento útok je cílen přímo na toto fyzické médium. Je tedy realizován na nejnižší vrstvě ISO/OSI modelu, kterou je fyzická vrstva (Hackinglab, ©2019).

Kabely se dělí podle různých parametrů:

- dle konstrukce na Unshielded Twisted Pair (UTP) a Shielded Twisted Pair (STP),
- dle rychlosti na Fast Ethernet (100BASE-TX) - kategorie 5E a Gigabit Ethernet (1000BASE-T) - kategorie 6E (Hackinglab, ©2019).

Kabely jsou rozděleny do dvojic, které jsou barevně označeny. Nejčastěji se používají dva typy zapojení v konektoru. Těmito typy jsou T568A a T568B. V České republice se velmi často setkáváme s typem T568B (Hackinglab, ©2019).

Při odposlouchávání touto metodou se používá half duplex. Tento typ odposlechu tedy probíhá pouze na jednom páru vodičů. Odposlech probíhá na jednom páru vodičů z důvodu toho, že nástroje pro odposlech (sniffery) pracují pouze jedním směrem. Pro odposlech je tedy nutné nastavit síťovou kartu do promiskuitního módu. To znamená, že karta pracuje v módu, kde pouze data přijímá, ale nevysílá. Mimo jiné, tento mód znamená, že zařízení je připraveno přijímat veškeré packety v síti a to i takové, které nejsou určeny pro toto zařízení. K dosažení tohoto módu lze použít i softwarové nástroje jako je program. V praxi, kterou vidíme na obrázku 2, stačí odizolovat síťový kabel a rozmotat dva páry vodičů. Tyto dva páry poté stačí připojit do datové zásuvky s portem RJ45 (keystone). Wireshark (Hackinglab, ©2019).



Obrázek 2: Příklad wiretappingu se schématem zapojení (Hackinglab, ©2019)

Mezi uživatelem a routerem probíhá běžná komunikace a v případě, že útočník vstoupí do tohoto zapojení, začne útočníkův počítač pomocí nástroje Wireshark zachytávat data uživatele (Hackinglab, ©2019).

4.3.2 Elektromagnetické vyzařování kabelových a bezdrátových klávesnic

Mnoho lidí si neuvědomuje, že klávesnice jako periferní počítačové zařízení, přenáší naše nejcitlivější data, jako jsou hesla. Jelikož klávesnice obsahuje elektronické zařízení, vyzařuje tak určité elektromagnetické vlny (Vuagnoux a Pasini, 2009).

Metoda spočívá v použití spektrálního analyzátoru, který detekuje signály nosiče (například klávesnice). Tato metoda je ovšem velmi nepřesná, jelikož signál, který chceme zachytit, musí být vysílán po delší dobu. Nejlepší metodou pro zachycení elektromagnetického vyzařování je širokopásmový přijímač. Proces detekce vln spočívá ve skenování celého frekvenčního rozsahu amplitudové nebo frekvenční modulace. V praxi se poté dají použít širokopásmové přijímače typu R -1250 nebo R -1550, které vyrábí společnost Dynamic Sciences International, Inc., kde typ R1550B je zobrazen na obrázku 3 (Vuagnoux a Pasini, 2009).

Obrázek 3: Širokopásmový přijímač R -1550B (Dynamicsciences, 2021)

Tyto dvě zmíněné zařízení splňují podmínky pro měření Tempest a mohou být využity pro měření elektronických zařízení v místech, kde se budou zpracovávat utajované informace (Dynamicsciences, 2021).

4.3.3 Kompromitující vyzařování LCD monitorů

Bezpečnostním odborníkům neuniklo, že žádné zařízení, které je umístěno v přímé viditelnosti k úkrytu útočníka, by mohlo být sledováno pomocí obyčejného dalekohledu. Právě z toho důvodu je nesmírně nutné dodržovat určité bezpečnostní standarty týkající se orientace a viditelnosti monitorů počítačů, ale také tabulí nebo dokumentů. Samozřejmě jsou ohrožena i periferní zařízení jako jsou klávesnice (G. Kuhn, 2003).

Dalším nebezpečným jevem je elektromagnetické vyzařování monitorů. V případě CRT monitorů je využito světelné energie. Jsou sledovány vysokofrekvenční změny vyzařovaného světla, které může být dokonce rozptýleno odrazem. Z CRT monitorů lze dokonce signál rekonstruovat do čitelné podoby ze zdeformovaného nebo odraženého světla. Vlivem šumu je informace možné získat pouze v relativně tmavém prostředí. Tato informace se týká i monitorů typu LCD. Na rozdíl od všeobecné představy, že monitory typu LCD, které jsou novější a tudíž bezpečnější, je nebezpečí těchto plochých obrazovek riskantnější. CRT monitory již najdeme velmi málo. Proto je problematika monitorů LCD mnohem důležitější. Jelikož LCD monitory jsou nejčastěji v dnešní době propojeny číslicovým rozhraním s rychlostí až v Gbit/s je způsobeno, že signál je zachytáván v mnohem lepší kvalitě než u CRT obrazovek (Dynamicsciences, 2021)

4.3.4 Odposlech

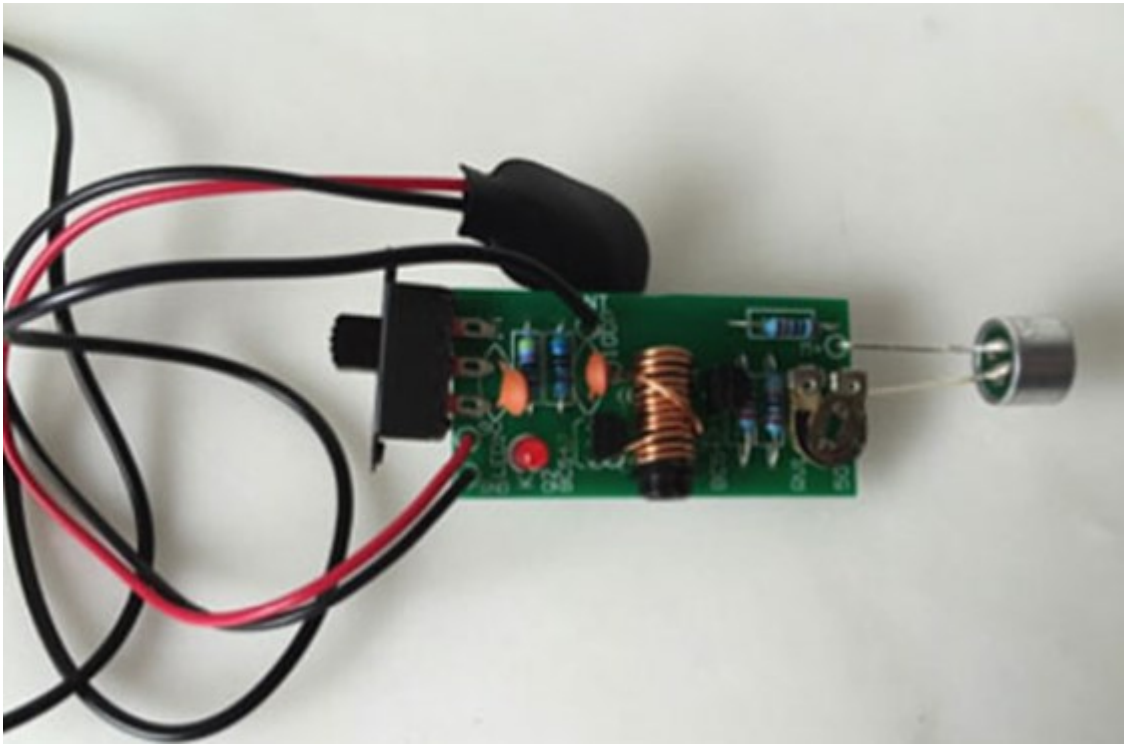
Odposlech zvuku z místnosti je v dnešní moderní době jedno z největších rizik. Pro případného útočníka je to levný a celkem dostupný zdroj úniku informací. Existuje mnoho internetových a kamenných prodejen poskytující jak levné, tak i profesionální zařízení pro odposlech. Nejčastější typy odposlechů jsou:

- odposlechy na bázi rádiového signálu,
- odposlechy ukládající na místní úložiště,
- ostatní formy odposlechu (EO Security, 2021).

Odposlechy na bázi rádiového signálu

Jedná se o miniaturní vysílač, který snímá okolní zvuky a vysílá je do prostoru podobně jako rozhlasová nebo televizní stanice. Jejich dosah se dle provedení může pohybovat od desítek metrů až po stovky metrů, případně v přímé viditelnosti i kolem 1 kilometru. Jejich obrovskou výhodou je vysoká citlivost a velmi nízká investice. Tyto zařízení se díky své

velikosti mohou ukrýt naprosto do jakéhokoliv zařízení, kdy pro kameru, nebo mikrofon stačí v ukrývaném předmětu malý otvor, viz obrázek 4 (Info Safe, 2020).



Obrázek 4: M radiový odposlech zvuku (EO Security, 2021)

GSM odposlechy fungují na principu klasického telefonního hovoru. Do těchto zařízení stačí vložit SIM kartu mobilního operátora, viz obrázek 5. Po vložení SIM karty operátora stačí poté na toto zařízení zatelefonovat a zařízení automaticky přenáší požadovaný zvuk. Některé typy zařízení disponují automatickým hovorem v případě detekce zvuku. V případě použití GPS můžeme sledovat i polohu tohoto zařízení, čehož se dá využít v případě jedoucího vozidla. Mezi hlavní výhody těchto zařízení patří jejich v podstatě neomezená vzdálenost (toto zařízení pouze limituje nedostupnost signálu mobilního operátora), (Topspy, 2020).

Obrázek 5: Špionážní štěnice TopSpy G10 (Topspy, 2020)

Odposlech fungující na principu Burst Transmitter patří také mezi odposlechy na bázi radiového signálu. Tento typ odposlechu není až tak známý mezi veřejností, je ovšem v dnešní době velkou hrozbou. Jedná se vlastně o „sdílení“ a odesílání dat například z mobilního telefonu. Náš mobilní telefon neustále odesílá data o své poloze, odesílá informace na BTS operátora, může být na dálku propojen s naším počítačem a může náš telefon na dálku ovládat hlasem. Každá tato funkce má samozřejmě potenciál být zachytávána a využita (CNET, 2021).

Odposlechy ukládající na místní úložiště

Tyto zařízení nepotřebují mít žádný vysílač, případně přijímač. Těmto zařízením stačí pouze místní úložiště (například paměťová karta). Mezi nejznámější, ale již celkem málo využívaná zařízení patří například diktafon. Nejdostupnějším způsobem je použití mobilního telefonu, který je nastaven v leteckém režimu (EO Security, 2021).

Pro takovou formu odposlechu mohou být využity i sofistikovanější zařízení jako jsou například odposlechy instalované do zařízení USB, které umožňují dlouhé nahrávání (dle kapacity USB zařízení) s poměrně čistým zvukem. Mezi jejich výhody patří nenápadné provedení. Hlavní nevýhodou je ovšem to, že zařízení je většinou viditelně připojené do konektoru USB (EO Security, 2021).

Keylogger viz obrázek 6, je zařízení, které umožňuje snímat a zaznamenávat otisky kláves. Jednoduše dokáže snímat to, co uživatel píše. Tyto zařízení mohou být umístěny přímo do klávesnice, případně lze tyto zařízení připojit mezi klávesnici a počítač (nejčastěji pomocí USB), (EO Security, 2021).

Obrázek 6: Vlevo keylogger vpravo zařízení USB pro odposlech (EO Security, 2021)

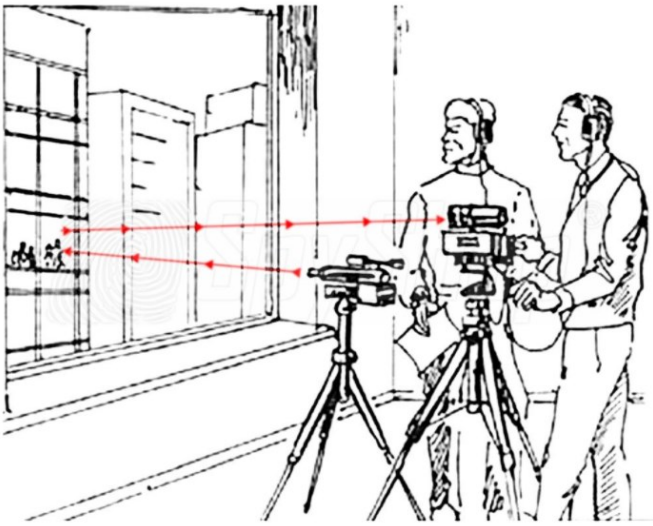
Ostatní formy odposlechu

Mezi tyto formy odposlechu patří například laserové odposlechy. Nejznámějším zařízením je v česku nazýváno zařízení Agáta, který je zobrazen na obrázku 7. Jedná se o zařízení IMSI Catcher, které se tváří jako falešná BTS mobilního operátora, která dokáže přesměrovat provoz ve svém okolí na vlastní HW a SW. Díky této technologii jsou odposlouchávány telefony a jednotlivé hovory (EO Security, 2021).

Obrázek 7: IMSI Catcher (EO Security, 2021)

Dalším zařízením pro zachytávání zvuku, je směrový odposlech pomocí citlivých antén. Dokáže zachytit konverzaci i na několik desítek metrů. Zde se může také využívat laserová technologie. Tyto laserové odposlechy jsou veřejně dostupné zařízení, které dle specifikací

mohou dosahovat až 400m. Pro příklad jdou použít mikrofony od firmy Spectra (Spyshop, 2021c).



Obrázek 8: Využití směrového mikrofonu (Spyshop, c2021)

Metod odposlechu je velmi mnoho. Nejhorší variantou je, pokud útočník použije kombinaci zmíněných typů odposlechu.

4.4 Metody ochrany před kompromitujícím vyzařování

Je důležité si uvědomit, že jakýkoliv únik utajované informace je hrozbou. K úniku utajované informace může dojít dvěma způsoby. Lidský faktor, který se dá ovlivnit pravidelným školením a poučením zainteresovaných osob, nebo pomocí technického prostředku. Způsoby ochrany jsou rozděleny do následujících kategorií:

- prověrka prostoru,
- detektory odposlechů,
- šifrované telefony,
- stíněná komora,
- šumový vysokofrekvenční generátor,
- síťové filtry,
- automatizovaný monitorovací systém,
- tempestované sestavy (Mudroch Labs s.r.o., 2021b).

Prověrka prostoru – jedná se o základní opatření. Toto opatření má za úkol odhalit nainstalované nebo vnesené zařízení, kterým lze získat kompromitující informace. Prověrka prostoru má také za úkol zamezit manipulaci s již nainstalovanými a používanými prostředky (Mudroch Labs s.r.o., 2021b).

Detektory odposlechu – jedná se o paměťové analyzátory RF spektra a detektory odposlechů. Tyto přístroje ovládá sám uživatel. Existují již zařízení, které jsou ovládat na dálku proškoleným personálem (Mudroch Labs s.r.o., 2021b).

Šifrované telefony – pro kvalitní ochranu je nezbytné použití dvou stejných zařízení se stejným nastavením šifrování. Pro použití mezi obyčejnými uživateli je toto zabezpečení nereálné. Jedná se o upravený software pro odesílání SMS, případně pro hovory je použito vlastní VPN (Mudroch Labs s.r.o., 2021b).

Stíněná komora - je místnost, která funguje na principu Faradayovy klece. Ta funguje na principech reflexe a absorpce při průchodu elektromagnetické vlny prostředím. Pro dosažení co nejlepšího útlumu je nutno použít feromagnetický materiál, který je dobře povrchově vodivý a má dostatečnou tloušťku (Balogh, 2018).

Síťové filtry – jsou elektronická zařízení, která zabraňují tomu, aby se vysokofrekvenční signály generované zařízením dostaly do napájecího kabelu, ale také, aby se vysokofrekvenční signály dostaly z rozvodné sítě do zařízení (SOSelectronic, 2021).

5 METODY A CÍLE PRÁCE

Hlavním cílem diplomové práce je přiblížit problematiku kompromitujícího vyzařování na vybraném typu objektu v zastavěné oblasti, kde v okolních budovách sídlí jiné společnosti.

Při tvorbě diplomové práce byla zpracována literární rešerše z dostupné odborné literatury. Literární rešerší byl utvořen pohled na problematiku ochrany utajovaných informací z hlediska legislativy. Další použitou metodou v diplomové práci byla použita syntéza, tedy sjednocení jednotlivých částí do celku.

V praktické části diplomové práce byla použita metoda analýzy a sběru dat získaných pozorováním vybrané budovy a jejího podrobnějšího zkoumání, díky které se odhalily hrozby spojené s únikem utajovaných informací. Pro hodnocení důležitosti hrozeb byla použita metoda PNH. V praktické části byly identifikovány i hrozby z ostatních oblastí úniku utajovaných informací. V oblasti utajovaných informací je jakákoliv hrozba úniku dat nebezpečná pro danou organizaci. Pro jednodušší pochopení oblasti ochrany utajovaných informací a možným únikem utajovaných informací byla zvolena organizace Ministerstvo obrany. Možný únik informací vlivem kompromitujícího vyzařovaní, může být využit i u soukromých společností, kde by tyto informace mohly společnost poškodit ve prospěch konkurence. Opatření zvolené v praktické části mohou být tedy využity v jakékoliv společnosti.

Omezení práce

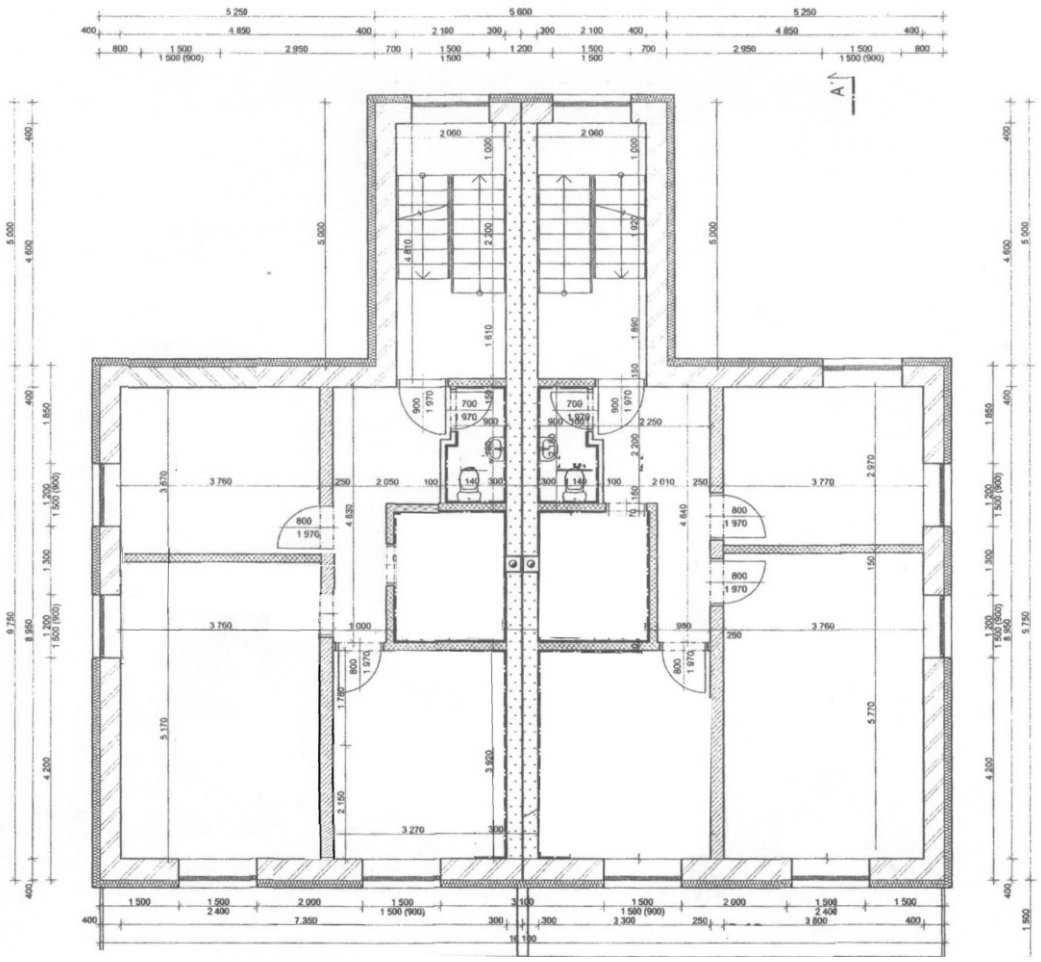
Tato diplomová práce se zabývá pouze kompromitujícím vyzařováním a ochranou před ním. Diplomová práce se nezabývá cenovým návrhem jednotlivých stavebních úprav. Při navrhování stavebních úprav jsou využity pouze orientační modelovací programy bez hodnocení statika a projektanta. Tato diplomová práce se nezabývá oficiální budovou, kde se zpracovávají utajované informace. Budova není majetkem Ministerstva obrany a není ani budoucí záměr, že by tato budova k podobným účelům sloužila. V diplomové práci nejsou zmíněny jména osob ani technika pro možné získávaní dat vlivem kompromitujícího vyzařování. V diplomové práci jsou uveřejněny pouze informace, které jsou veřejně dostupné.

II. PRAKTICKÁ ČÁST

6 POPIS OBJEKTU

Předmětem praktické části diplomové práce je zkoumání zabezpečení budovy, ve které se zpracovávají utajované informace. Pro tento účel byla vybrána budova, která byla postavena v roce 2018. Nachází se v zastavěné oblasti na okraji města Uherský Brod. Budova bude pro účely diplomové práce sloužit jako majetek Ministerstva obrany a také celá budova bude sloužit jako prostory pro kanceláře Ministerstva obrany. Jak bylo zmíněno v kapitole Metody a cíle, budova pro tyto účely bude sloužit pouze pro tuto diplomovou práci.

Jak již bylo zmíněno, budova byla postavena v roce 2018, kde v říjnu 2018 proběhala kolaudace budovy. Dle půdorysu budovy se obvodové zdivo skládá z cihel POROTHERM 40 Si s pevností P10 s izolací 25cm. Stěna, která odděluje budovy je postavena ze zdiva POROTHERM 30 AKU s pevností P10, tato stěna je postavena z každé strany, tedy tloušťka stěny mezi budovami je 60cm. Vnitřní příčky oddělující hlavní místnosti jsou postaveny ze zdiva POROTHERM 24 P +D s pevností P10. Příčky v místnostech jsou pouze z příčkovek o síle 11,5cm. Strop mezi podlažím je vytvořen pomocí stropní vložky MIAKO. Dále je použita 50mm minerální kročejová vrstva, cementový potěr o síle 60mm a poslední nášlapná vrstva. Střecha budovy je tvořena sádrokartonovými podhledy v posledním podlaží, izolací skelnou vatou a vrstvou polystyrenového zateplení. Na tomto zateplení je vytvořen základ z desek OSB, na kterých jsou položeny asfaltové pásy. Topení v celé budově je řešeno pomocí stropních infrapanelů. Obrázek 9 zobrazuje půdorys objektu, kde tento půdorys zobrazuje 2. nadzemní podlaží vybrané budovy.

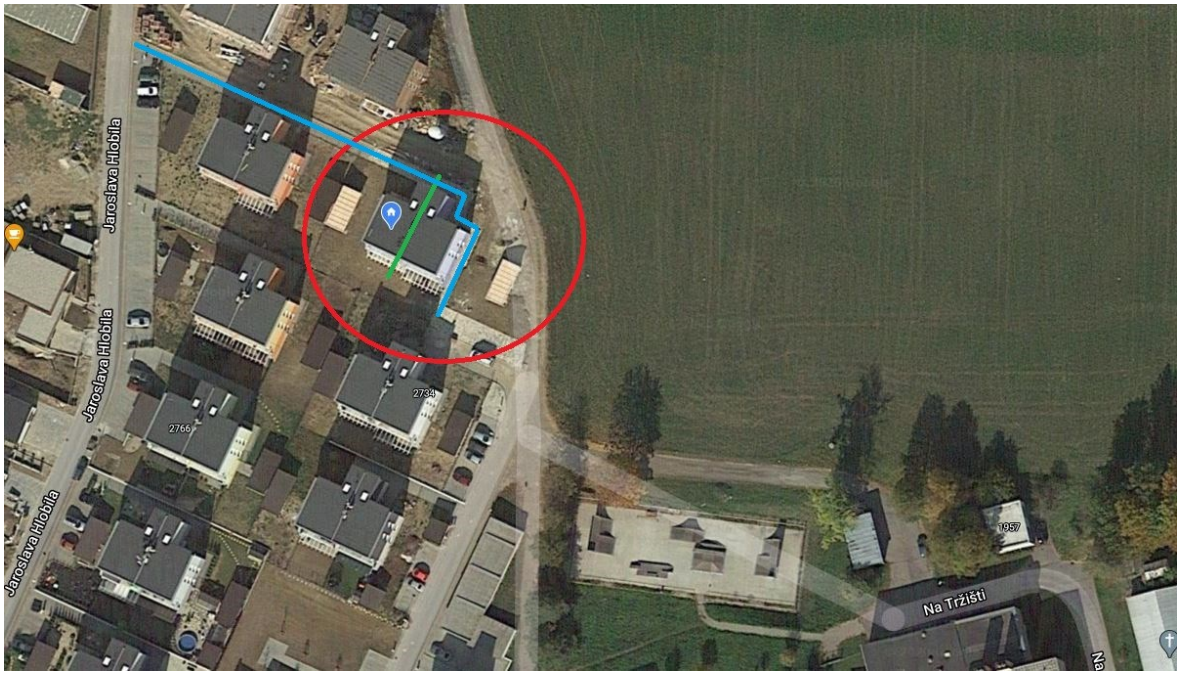


Obrázek 9: Půdorys budovy (Zdroj: Vlastní)

Rozložení jednotlivých oddělení budovy je dle pater, kde každé oddělení má k dispozici své patro, včetně sociálních zařízení. Společnými prostory jsou pouze chodby se schodištěm. Rozložení místností je v každém patře totožné.

6.1 Geografie objektu

Budova se nachází v zastavěné oblasti na okraji města. Budova se skládá s 1. nadzemního podlaží, 2. nadzemního podlaží a 3. nadzemního podlaží. Budova na první pohled působí jako jeden celistvý objekt. Tento objekt se skládá ze dvou vlastních vchodů a ze dvou čísel popisných. Jsou to tedy dvě stejné budovy, které jsou pouze zrcadlově otočeny. Pro potřeby diplomové práce musí být z hlediska kompromitujícího vyzařování a ochrany utajovaných informací zkoumány obě budovy. Přesný popis objektu a jeho rozdělení je zobrazené na Obrázku 10, kde se v červeném ohraničení nachází zkoumaná budova, zeleně je označeno rozdělení těchto budov a modře jsou vyznačeny chodníky.



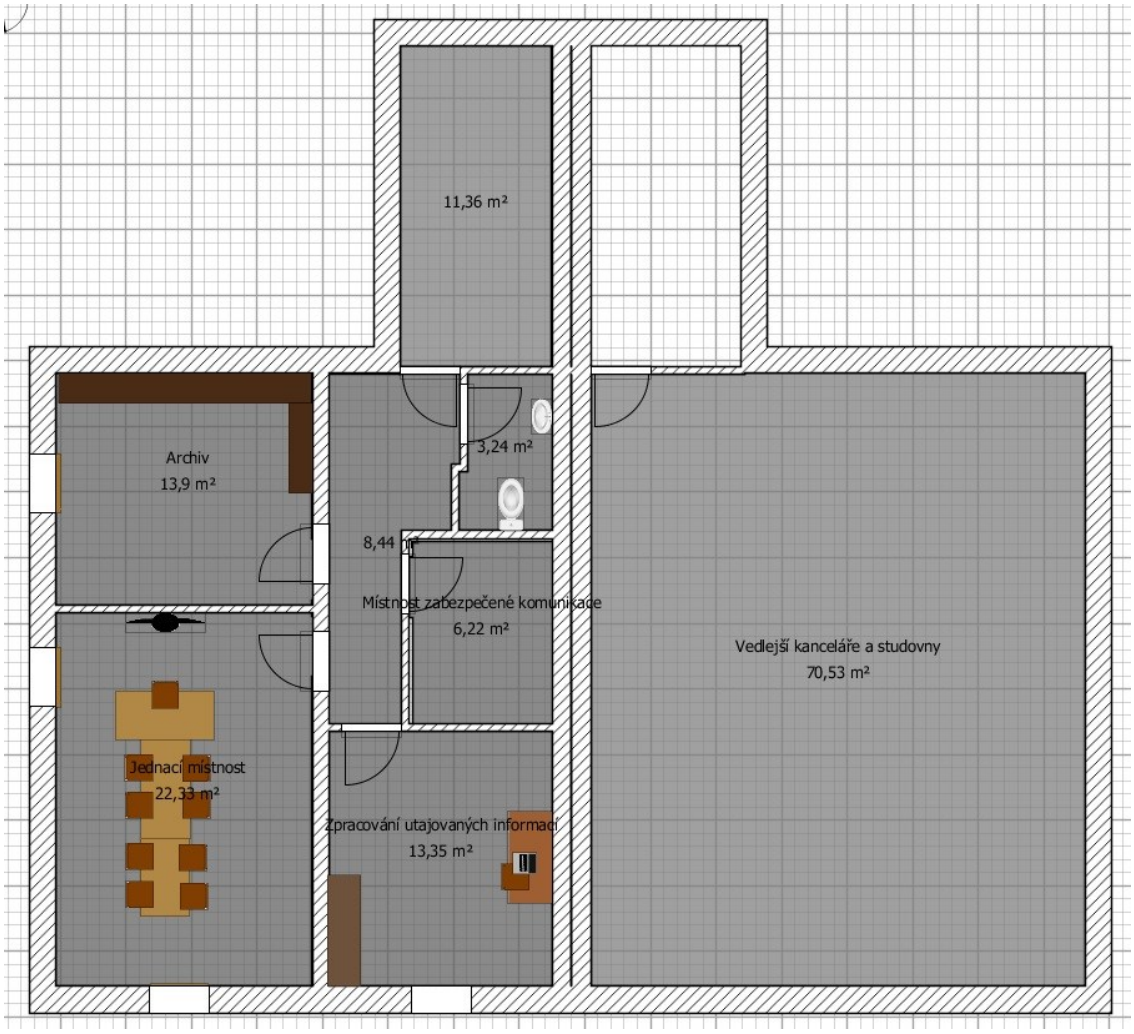
Obrázek 10: Letecký snímek budovy s rozdělením (Mapy Google, 2011)

Vchod do budovy se nachází na severozápadní straně. Kolem budovy vedou chodníky, po kterých se může pohybovat kdokoliv z kolemjdoucích osob.

6.2 Rozdělení místností

Pro potřeby oddělení na zpracování utajovaných informací bylo zvoleno 2. nadzemní podlaží. Toto podlaží není jednoduše přístupno ze střechy budovy a případně z přízemí budovy. Pro případné nedovoleného vniknutí do budovy, je tedy již od výběru podlaží částečně oddělení zabezpečeno proti jednoduchému vniknutí.

Po vstupu do oddělení je nalevo umístěno sociální zařízení, napravo od vchodu poté archiv, kde nebudou ukládány utajované informace. Tato místnost bude sloužit pouze pro uložení neutajovaných dokumentů. Místnost nalevo bude sloužit pro uložení zařízení pro zabezpečenou komunikaci LAN. V místnosti na konci oddělení bude počítačové zařízení, na kterém se budou zpracovávat utajované informace stupně důvěrné a vyšší. V celé diplomové práci jsou pod pojmem utajované informace míněno dle zákona 412/2000 Sb., utajované informace stupně důvěrné a vyšší. Vedle této místnosti bude jednací místnost určená pro jednání. Jelikož se počítá, že v jednací místnosti se budou projednávat i zpracované utajované informace, bude se na zabezpečení této místnosti pohlížet stejně, jako na místnosti se zařízením pro zabezpečenou komunikaci a místností na zpracovávání utajovaných informací. Rozložení místností je znázorněno na obrázku 11 a obrázku 12.



Obrázek 11: Rozmístění místností dle požadavků (Zdroj: Vlastní)

Obrázek 12: 3D pohled na rozmístění místností (Zdroj: Vlastní)

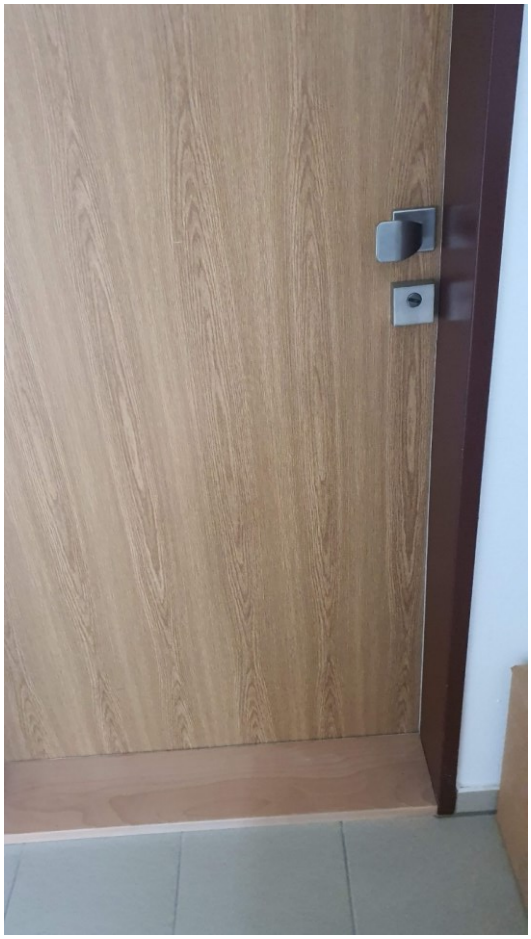
Pro lepší orientaci v dalších popisech budou místnosti označeny následovně:

- chodba bude označena číslem 2.0,
- WC bude označeno číslem 2.1,
- archiv bude označen číslem 2.2,
- místnost zabezpečené komunikace 2.3,
- jednací místnost bude označena číslem 2.4,
- místnost pro zpracování utajovaných informací bude označena číslem 2.5.

6.3 Současný stav zabezpečení

Aktuálně budova neslouží ke zpracovávání utajovaných informací. Její zabezpečení spočívá v čipovém/klíčovém přístupu hlavního vchodu pouze oprávněným osobám. Každá oprávněná osoba má čipovou kartu, která ovládá otevírání hlavních vchodových dveří budovy. Dále je tento vchod napojen na video panel v každém oddělení, kdy je pomocí video panelu tyto dveře možno ovládat na dálku. Vchodové dveře nejsou vybaveny

automatickým zavíráním systémem BRANO. Každé oddělení má vchod do kanceláří oddělen bezpečnostními protipožárními dveřmi s kováním, kde na venkovní straně je umístěna dveřní pevná koule. Jako vstupní dveře do jednotlivých oddělení jsou použity SAPELI Damier – protipožární viz obrázek 13.



Obrázek 13: Vchod do jednotlivých oddělení SAPELI – Damier (Zdroj: Vlastní)

Dveře v interiéru jednotlivých kanceláří jsou dřevěné obložky uchycené na montážní pěnu. Dveře v interiéru jsou z materiálu MDF – dřevovláknitá deska, která má homogenní strukturu s pevnými hranami.

6.4 Vybavení místností

Pro provedení kvalitní identifikace hrozeb je nutno zmínit vybavení jednotlivých místností. Nejdůležitějšími místnostmi z pohledu ochrany utajovaných informací jsou místnosti 2.3, 2.4 a 2.5.

V jednací místnosti bude umístěna velkoplošná TV, kde při zasedání budou na TV zobrazovány důležité informace a to i utajovaného charakteru. V místnosti pro zpracování

utajovaných informací bude umístěna multifunkční tiskárna, skartovací zařízení, monitor LCD, PC skříň, klávesnice, myš a také úschovný objekt.

V místnosti 2.3 bude umístěn modem pro komunikaci s vnějším prostředím v síti Internet.

7 ANALÝZA HROZEB

Pro potřeby diplomové práce byla zvolena metoda pro analýzu hrozeb zvaná PNH. Tato jednoduchá bodová polokvantitativní metoda vychází ze třech složek, kterými jsou pravděpodobnost vzniku (P), závažnost (pravděpodobnost) následků (N) a názoru hodnotitelů (H). Celkové hodnocení hrozby (R) je poté stanoveno součinem jednotlivých činitelů P, N, H.

7.1 Stanovení hodnot

Pravděpodobnost vzniku (P), se kterým může nebezpečí nastat je stanovena dle stupnice 1-5 , kde číslo 5 je největší pravděpodobností, že nebezpečí nastane, viz tabulka 1.

Tabulka 1: P – pravděpodobnost vzniku (Zdroj: Vlastní)

Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Pravděpodobnost následků (N) neboli jejich závažnost, určuje dopad následků na možný únik informací. V tabulce je stanovena hodnota od 1 do 5, kdy 5 znázorňuje nejhorší následek úniku informací. Trvalý únik informací je takový, který určuje možnost úniku informací bez možnosti okamžitého zjištění, viz tabulka 2.

Tabulka 2: N – Pravděpodobnost následků (Zdroj: Vlastní)

Nahodilý únik	1
Nepravděpodobný únik	2
Pravděpodobný únik	3
Velmi pravděpodobný únik	4
Trvalý únik	5

Názor hodnotitelů (H) je zohlednění míry závažnosti ohrožení, čas působení ohrožení, stav technologických zařízení, vliv pracovního prostřední a pracovních podmínek viz tabulka 3.

Tabulka 3: H - Názor hodnotitelů (Zdroj: Vlastní)

Zanedbatelný vliv na míru nebezpečí	1
Malý vliv na míru nebezpečí	2
Větší, nezanedbatelný vliv na míru nebezpečí	3
Velký vliv na míru nebezpečí	4
Velice významný a nepříznivý vliv na míru nebezpečí	5

Celkové hodnocení rizika (R) jak již bylo zmíněno, je dáno součinem výše uvedených hodnot. Míra akceptovatelnosti hrozby je stanovena v Tabulce 4.

Tabulka 4: R - Celkové hodnocení hrozeb (Zdroj: Vlastní)

Rizikový stupeň	**R**	**Míra rizika**
V.	> 100	Nepřijatelná hrozba
IV.	51 – 100	Nežádoucí hrozba
III.	11 – 50	Mírná hrozba
II.	3 – 10	Akceptovatelná hrozba
I.	< 3	Bezvýznamná hrozba

7.2 Identifikace hrozeb

K identifikaci hrozeb bylo nutno tyto hrozby rozdělit do určitých kategorií:

- personální bezpečnost,
- administrativní bezpečnost,
- fyzická bezpečnost,
- bezpečnost informačních a komunikačních zařízení,
- kompromitují vyzařování,
- ostatní hrozby.

Se skupinou odborníků na danou problematiku, byly hrozby identifikovány na základě podrobného studování půdorysu budovy, včetně použitých stavebních materiálů. Dále byly hrozby identifikovány pomocí metody zkoumání a monitorování budovy. Pro potřeby diplomové práce byly identifikovány hrozby spojené s kompromitujícím vyzařováním. Za

zmínku ovšem stojí i ostatní hrozby, které jsou s tímto problémem velmi úzce spjaty. Celkem tedy bylo identifikováno 28 možných hrozeb.

7.2.1 Oblast kompromitujícího vyzařování

V oblasti kompromitujícího vyzařování byla identifikace zaměřena převážně na akustické kompromitující vyzařování a také na optické vyzařování z místností 2.4 a 2.5 do ostatních místností a prostor. Dále bylo zhodnoceno také elektromagnetické vyzařování elektronických zařízení.

Rekonstrukce signálů z vedení elektrického napětí 230V

Zachycení elektromagnetického vyzařování z vedení elektrického napětí 230V.

Rekonstrukce signálů ze zdrojů LAN

Pomocí zachycení dat ze zařízení typu router, mohou být zachyceny zasílané data prostřednictvím internetové sítě.

Použití zařízení na bázi odposlechu

Je zde velkým rizikem vnesení zařízení pro vysílání radiového signálu a tedy odposlechu konverzace.

Akustické vyzařování přes tenké zdivo

Tloušťka a akustické vlastnosti použitého zdiva POROTHERM 24 P +D mezi místnostmi 2.4 a 2.5 a dále tloušťka zdiva POROTHERM 11,5 AKU mezi místnostmi 2.3, 2.1 a 2.0 a také mezi místnostmi 2.4 a 2.2 můžou zapříčinit, že zvuk a projednávané informace budou velmi jednoduše zachyceny zvukovými prostředky cizími nebo neoprávněnými osobami.

Akustické vyzařování do prvního nadzemního podlaží

Akustické vlastnosti stropu mohou zapříčinit přenos zvuku do 1. nadzemního podlaží a tím zapříčinit akustický únik informací.

Akustické vyzařování do třetího nadzemního podlaží

Akustické vlastnosti stropu mohou zapříčinit přenos zvuku do 3. nadzemního podlaží a tím zapříčinit akustický únik informací.

Vizuální vyzařování přes okna místnosti na zpracování utajovaných informací

Okno v místnosti 2.5 může být zneužito ke sledování promítaného obrazu na informačních a komunikačních zařízeních, které jsou v této místnosti použity. Hrozí zde tedy vizuální kompromitující vyzařování.

Vizuální vyzařování přes okna jednací místnosti

Okna v místnosti 2.4 mohou být zneužita ke sledování promítaného obrazu na informačních a komunikačních zařízeních, které jsou v této místnosti použity. Hrozí zde tedy vizuální kompromitující vyzařování.

Akustické vyzařování přes okna místnosti pro zpracování utajovaných informací

Pomocí směrových antén mohou být odposlouchávány konverzace, ve kterých se projednávají utajované informace.

Akustické vyzařování přes okna v jednací místnosti

Pomocí směrových antén mohou být odposlouchávány konverzace, ve kterých se projednávají utajované informace.

Akustické vyzařování mezi budovami

Akustické vlastnosti použitého zdiva POROTHERM 40Si P10 mohou zapříčinit prostup zvuku z místnosti 2.5 a místnosti 2.3.

Elektromagnetické vyzařování počítačových komponent

U těchto zařízení hrozí vysílání elektromagnetických vln, které mohou být zachyceny a následně rekonstruovány. Jsou zde myšleny všechny periferní zařízení jako klávesnice, myš, LCD monitor, multifunkční zařízení a PC skříň.

Elektromagnetické vyzařování LCD TV v místnosti 2.4

U tohoto zařízení hrozí vysílání elektromagnetických vln, které mohu být zachyceny a následně rekonstruovány.

7.2.2 Oblast fyzické bezpečnosti

V oblasti fyzické bezpečnosti byly identifikovány hrozby v použitém stavebním materiálu, použitém vybavení dveří a oken budovy. Dále pak bylo zkoumáno možné násilné vniknutí do budovy.

Násilný vstup přes vchodové dveře

Přes necertifikované vstupní dveře a necertifikovanou zámkovou vložku dveří může do oddělení násilně vstoupit osoba, která má v úmyslu získat utajované informace. Stejná situace platí u použitých dveří do místností. Tyto dveře nejsou bezpečnostními dveřmi.

Násilný vstup přes okna

Při použitých oknech od výrobce Montplast je možnosti násilného vniknutí rozbitím okna případně pro zkušeného člověka je možné vniknutí přes použité kování okna.

Vstup přes terasu

Jelikož budova disponuje terasou v každém poschodí, vzniká zde nebezpečí násilného vstupu ze střechy budovy na terasu objektu a dalším násilným vniknutím až do oddělení.

7.2.3 Bezpečnost informačních a komunikačních systémů

V oblasti bezpečnosti informačních a komunikačních systémů se identifikace hrozeb zaměřila na možný únik dat přes počítačové zařízení a přenosná zařízení pro záznam zvuku, fotografií nebo videa.

Pořizování zvukových záznamů

Při vnesení elektronických zařízení umožňující nahrávání zvuku vzniká nebezpečí nahrávání projednávaných informací.

Pořizování fotografií/videa

Při vnesení elektronických zařízení umožňující pořizování zvukových a audiovizuálních nahrávek hrozí nebezpečí pořizování těchto záznamů.

Antivirová ochrana informačních zařízení

Zařízení připojeno do globální sítě internet může být napadeno nebezpečným softwarem.

Získání dat z nezabezpečené sítě LAN

Při odesílání dat z informačního zařízení, ve kterém se zpracovávají a odesílají tyto informace, mohou být informace (či jednotlivé data) úmyslně zachyceny přes nezabezpečené zařízení, jakými jsou například switch, modem nebo router.

7.2.4 Personální bezpečnost

V oblasti personální bezpečnosti byly identifikovány hrozby, které se týkají vstupů do místností neoprávněnými osobami.

Neoprávněný vstup do oddělení

Do oddělení mohou vstupovat pouze osoby s platným osvědčením fyzické osoby.

Neoprávněný vstup do místnosti zabezpečené komunikace

Do místnosti, kde bude umístěno zařízení pro zabezpečenou komunikaci, mohou mít přístup pouze osoby, které mají certifikát/oprávnění s tímto zařízením manipulovat.

Neoprávněný vstup do místnosti ke zpracování utajovaných informací

Do místnosti ke zpracování utajovaných informací, mohou mít přístup pouze osoby, které se mohou seznamovat s těmito zpracovávanými informacemi.

Neoprávněný vstup do jednací místnosti

Do jednací místnosti mohou vstupovat pouze osoby, které mají platné osvědčení daného stupně projednávané informace.

7.2.5 Administrativní bezpečnost

Nekontrolované vstupy do místností

V oddělení není aktuálně zpracován seznam osob, které jsou oprávněny vstupovat do utajovaných místností, a které se mohou přímo podílet na zpracování utajovaných informací.

Evakuační plán

Pro případnou evakuaci osob by měl v budově být zpracován evakuační plán. Plán aktuálně v budově není zpracován.

7.2.6 Ostatní hrozby

Požár v budově nebo místnosti

V případě požáru budovy nebo místnosti, je hrozba vstupu neoprávněné osoby do utajovaných místností.

Vytopení budovy

V případě vytopení budovy nebo 3. nadzemního podlaží, je hrozba zničení informačních a komunikačních zařízení.

7.3 Hodnocení hrozeb

V této kapitole budou jednotlivé identifikované hrozby bodově ohodnoceny a dle Tabulky 4 bude určeno celkové hodnocení rizika. Pro potřeby diplomové práce bude nejdůležitější hodnocení hrozeb z oblasti kompromitujícího vyzařování. Ostatní hrozby budou hodnoceny menší mírou rizika a ošetřeny pouze ty nejzávažnější. Všechny analyzované hrozby musí být určitým způsobem ošetřeny, jelikož by budova s těmito hrozbami nemohla být užívána ke zpracování UI. Výpočet hrozeb bude proveden součinem stanovených hodnot P x N x H. Hodnocení hrozeb je dle kategorií rozdělen v tabulkách 5-10.

Tabulka 5: Hodnocení hrozeb kompromitujícího vyzařování (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Míra hrozby
Rekonstrukce signálů z vedení elektrického napětí 230V	4	5	5	**100**	Nežádoucí hrozba
Rekonstrukce signálů ze zdrojů LAN	4	5	5	**100**	Nežádoucí hrozba
Použití zařízení na bázi odposlechu	5	5	5	**125**	Nepřijatelná hrozba
Akustické vyzařování přes tenké zdivo	5	5	5	**125**	Nepřijatelná hrozba
Akustické vyzařování do prvního nadzemního podlaží	5	5	5	**125**	Nepřijatelná hrozba
Akustické vyzařování do třetího nadzemního podlaží	5	5	5	**125**	Nepřijatelná hrozba
Vizuální vyzařování přes okna místnosti na zpracování utajovaných informací	5	5	5	**125**	Nepřijatelná hrozba
Vizuální vyzařování přes okna jednací místnosti	5	5	5	**125**	Nepřijatelná hrozba
Akustické vyzařování přes okna místnosti pro zpracování utajovaných informací	4	5	5	**100**	Nežádoucí hrozba
Akustické vyzařování přes okna v jednací místnosti	4	5	5	**100**	Nežádoucí hrozba
Akustické vyzařování mezi budovami	3	2	3	**18**	Mírná hrozba

Identifikovaná hrozba	P	N	H	R	Míra hrozby
Elektromagnetické vyzařování počítačových komponent	5	5	5	**125**	Nepřijatelná hrozba
Elektromagnetické vyzařování LCD TV v místnosti 2.4	5	5	4	**100**	Nežádoucí hrozba

Tabulka 6: Hodnocení hrozeb oblasti fyzické bezpečnosti (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Nežádoucí hrozba
Násilný vstup přes vchodové dveře	4	4	4	**64**	Nežádoucí hrozba
Násilný vstup přes okna	5	3	4	**60**	Nežádoucí hrozba
Vstup přes terasu	5	3	4	**60**	Nežádoucí hrozba

Tabulka 7: Hodnocení hrozeb v oblasti bezpečnosti informačních a komunikačních systémů (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Míra rizika
Pořizování zvukových záznamů	5	4	4	**100**	Nežádoucí hrozba
Pořizování fotografií/videa	5	5	4	**100**	Nežádoucí hrozba
Antivirová ochrana informačních zařízení	5	5	4	**100**	Nežádoucí hrozba
Získání dat z nezabezpečené sítě LAN	5	5	5	**125**	Nepřijatelná hrozba

Tabulka 8: Hodnocení hrozeb z oblasti personální bezpečnosti (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Míra rizika
Neoprávněný vstup do oddělení	4	3	4	**48**	Mírná hrozba
Neoprávněný vstup do místnosti zabezpečené komunikace	4	4	5	**100**	Nežádoucí hrozba
Neoprávněný vstup do místnosti ke zpracování utajovaných informací	4	4	5	**100**	Nežádoucí hrozba
Neoprávněný vstup do jednací místnosti	4	4	5	**100**	Nežádoucí hrozba

Tabulka 9: Hodnocení hrozeb z oblasti administrativní bezpečnosti (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Míra rizika
Nekontrolované vstupy do místností	4	3	3	**36**	Mírná hrozba
Evakuační plán	2	2	3	**12**	Mírná hrozba

Tabulka 10: Hodnocení ostatních hrozeb (Zdroj: Vlastní)

Identifikovaná hrozba	P	N	H	R	Míra rizika
Požár v budově nebo místnosti	3	2	3	**18**	Mírná hrozba
Vytopení budovy	3	2	3	**18**	Mírná hrozba

Z tabulek 5-10 můžeme pozorovat, že z 28 hrozeb vychází 8 hrozeb jako nepřijatelných. Každá z identifikovaných hrozeb má však velký vliv na únik utajovaných informaci.

8 OŠETŘENÍ HROZEB

V této kapitole praktické části budou ošetřeny identifikované hrozby v oblasti kompromitujícího vyzařování a ochrany utajovaných informací místností 2.3, 2.4 a 2.5. Bude postupováno od nepřijatelných hrozeb, až po mírné hrozby.

8.1 Použití zařízení na bázi odposlechu

Pokud bude zařízení pro odposlech umístěno přímo v místnosti, jedinou možnou ochranou je pravidelná prohlídka místnosti. Dále je potřeba řízeného vstupu do místností, kde budou vstupovat pouze oprávněné osoby. Tím můžeme eliminovat, že neoprávněná osoba umístí odposlech do jedné z místností 2.5, 2.4, 2.3. V případě, že by tato situace mohla nastat, je jednoduchým řešením pravidelná kontrola místností detektory analogových a digitálních bezdrátových odposlechů. Osoby, které využívají zmíněné místnosti, by dle směrnice v nepravidelných intervalech kontrolovali místnosti detektorem odposlechu, případně i detektorem bezdrátových kamer. Příklady těchto zařízení jsou uvedeny na obrázku 14, na kterém je zobrazen detektor odposlechu a detektor kamer.

Obrázek 14: Vlevo detektor odposlechů vpravo detektor kamer (Spyshop, 2021b; Spyshop 2021a)

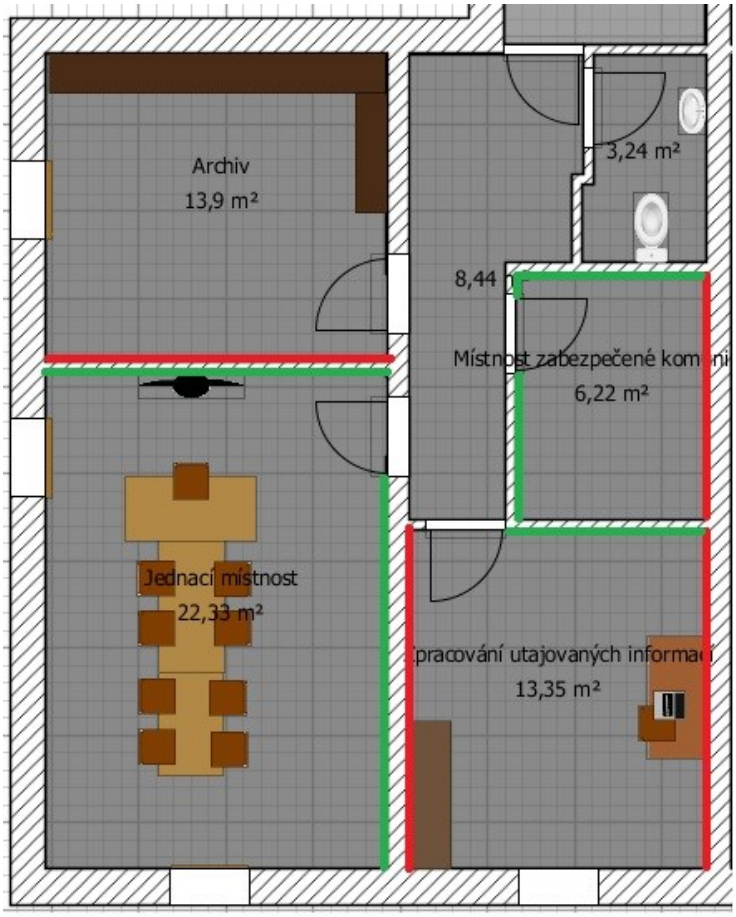
Zařízení zobrazeny na obrázku 14, by proti neoprávněné manipulaci byly uloženy v uzamykatelné bezpečnostní skříni, která je umístěna v místnosti 2.5.

8.2 Akustické vyzařování přes tenké zdivo

V domě je použito zdivo POROTHERM 24 P +D mez místnostmi 2.4 a 2.5. Nejnebezpečnější varianta pro akustické vyzařování jsou stěny POROTHERM 11,5 AKU v místnosti 2.3, které z hlediska odhlučnění nejsou dostatečná a dle pozorování propouští i mluvené slovo. Pokud by v místnosti byl použit zesilovač zvuku, případně zařízení na podobném principu, bylo by možné mluvené slovo celkem snadno zachytit. V tomto případě se nejedná pouze o mluvené slovo, ale dle některých výzkumů je velkým rizikem také akustické vyzařování klávesnice, kdy může být analyzován zvuk stisku jednotlivých kláves a poté může být dekódováno, která klávesa byla stisknuta. Ošetření tohoto rizika je problematické z hlediska stavebních úprav. V dnešní době je na trhu mnoho odhlučňovacích panelů. Tato hrozba bude ošetřena stavebními úpravami. Místnosti, které obsahují okna, musí dodržet směrnici, ve které bude uvedeno, že v případě projednávání nebo zpracovávání utajovaných informací, musí tato okna být v uzavřeném stavu, jelikož přes otevřené okno je velká hrozba úniku utajovaných informací vlivem akustického vyzařování.

Dle pozorování a zkoumání budovy můžeme dle půdorysu vidět, že je pro odhlučnění stěn možno využít zhruba 10cm dalšího materiálu, aby bylo možné otevírat dveře. Ovšem odhlučnit místnost můžeme z obou stran, tudíž je možno využít i širší skladby odhlučňovacího materiálu. Jelikož bude v kapitole 8.7 využito principu stíněné komory, bude nezbytné použité materiály zakrýt.

Nejlepším řešením je použití sádrokartonové stěny. Jelikož přenos hluku nezáleží pouze na tloušťce použitého materiálu, ale zvuk se nese i konstrukcí. Z důvodu použití klasické konstrukce pro ukotvení sádrokartonových desek, bude cela konstrukce podlepena tlumící páskou na sádrokarton, aby nedocházelo k přenosu zvuku pomocí konstrukce. Výplň mezi konstrukcí bude minerální vata. Systém konstrukce bude použit dle obrázku 15, na kterém je zeleně vyznačeno, ve které části bude osazena konstrukce minerální vaty a sádrokartonu.



Obrázek 15: Vyznačení odhlučnění místností (Zdroj: Vlastní)

Obrázek 16: Vlevo akustické desky a vpravo použití minerální vaty (Notami, ©2017a; Notami, ©2017b)

Jelikož při ochraně utajovaných informací je důležité některé komponenty naddimenzovat, budou místnosti odhlučněny z více stran. Zde již vhledem k tloušťce případné konstrukce a nedostatku místa bude použito akustických desek, které budou lepeny přímo na stěnu. Tyto stěny jsou na obrázku 15 zobrazeny červeně.

8.3 Akustické vyzařování do prvního nadzemního podlaží

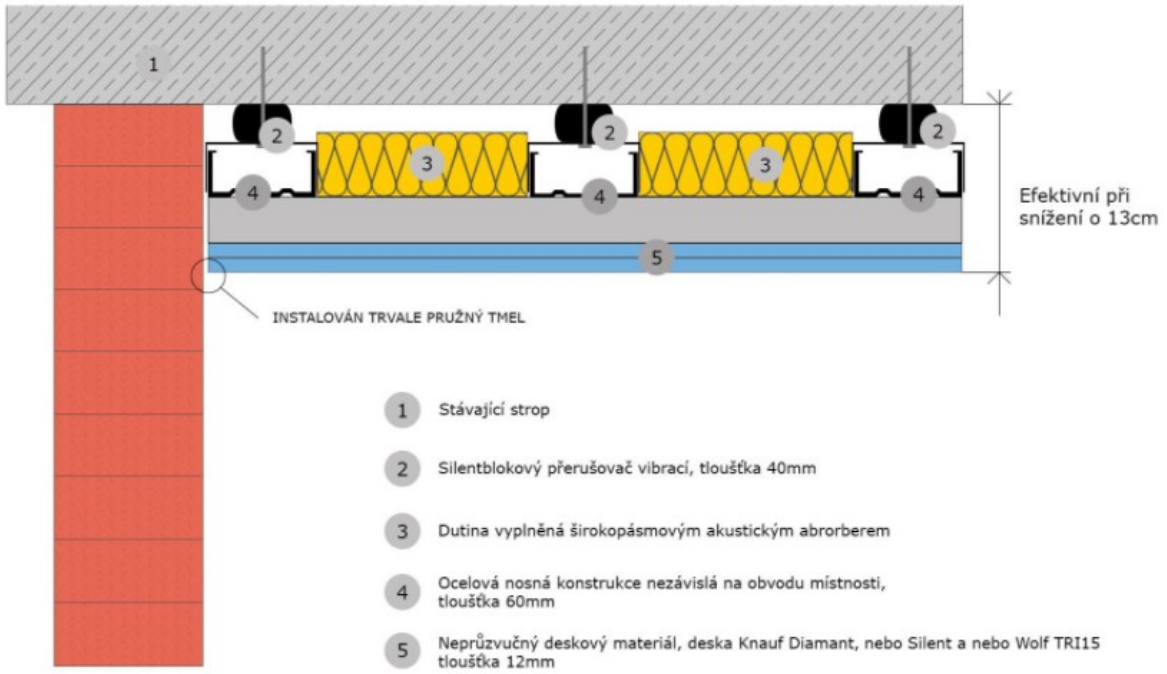
Stejný případ jako v předchozí kapitole nastává u přenosu zvuku do přízemí. Nejjednodušší způsob odhlučnění je z oddělení v přízemí. Zde ovšem nastává problém v použití stíněné komory, která bude použita v kapitole 8.7. V tomto případě bude potřeba odhlučnit přímo podlahy v celém oddělení, abychom se vyvarovali různým výškám podlah v místnostech. V celém oddělení bude zachována současná skladba podlahy, kde se pouze strhne pohledový podklad z linolea. Na odhlučnění bude použito akustické pěny, viz obrázek 17.

Obrázek 17: Akustická pěna (Akustická pěna, 2021)

Tato pěna je lisována z kousků polyuretanové pěny, která zapříčiní snížení hluku vyzařovaného do přízemí.

8.4 Akustické vyzařování do třetího nadzemního podlaží

Stejně jako do přízemí, je riziko úniku hluku do patra nad oddělením přes stropy. Vzhledem k instalaci stínících panelů, bude potřeba tyto panely zakrýt. Jako jednoduchý a účinný systém se jeví instalace sádrokartonového podhledu. Použito bude klasické sádrokartonové konstrukce a výplně akustickým absorbérem. Tato konstrukce je znázorněna na obrázku 18.



Obrázek 18: Odhlučnění stropu (Gutta, 2015)

Tato konstrukce bude uchycena na silentblocích, které zabraňují otřesům z patra. Místo klasické sádrokartonové desky bude použito neprůzvučného materiálu Wolf TRI15 s tloušťkou 12mm, který dle výrobce sníží neprůzvučnost až o 36dB (Ciurshop, 2021).

8.5 Vizuální vyzařování přes okna místnosti na zpracování utajovaných informací

Přes okno této místnosti může případný útočník pouze vizuálním vyzařováním zachytit obraz na monitoru počítače. Možností ochrany máme několik, a i když se zazdít okno může jevit, jako nejjednodušší není tomu tak vždy. V případě zazdění okna sice zamezíme tomu, že případný útočník uvidí na display monitoru, ale vyvstanou nám další problémy hlavně s větráním oddělení. V tomto případě jsou dalšími možnostmi použití vnitřních obyčejných žaluzií a pro případné nepovolené vniknutí v době, kdy se zpracovávají utajované informace důvěrné a vyšší použití venkovních bezpečnostních rolet. Tím zůstane okno zachováno a může být použito pro případné větrání, ale zároveň ochráníme informace před jejich únikem. Samozřejmě jakékoliv okno je menší překážkou vůči fyzické ochraně, proto je možná také varianta zavedení ventilace do celého oddělení. V tomto případě je ale také hrozba úniku dat kompromitujícím vyzařováním naindukováním na vlnovod-kovové ventilační potrubí. Vzhledem k zachování rázu budovy a menší hrozbou oproti ventilaci,

bude použita varianta s žaluziemi jak vnitřními tak venkovními. Venkovní žaluzie budou umístěny na rám okna s postranními vodícími lištami v zateplení domu. To zajistí, že venkovní žaluzie budou pevně držet na svém místě, viz obrázek 19. Rolety budou poháněny elektrickými motorky, kde tlačítko pro ovládání bude umístěno v místnosti. V případě že zaměstnanci budovu opustí, musí být ve směrnicích uvedeno, že tyto žaluzie z důvodu bezpečnosti budou zatažené. Dále bude ve směrnici uvedeno, že v případě projednávání UI bude zakázáno otevírat okna, větrání bude zajištěno mimo dobu projednávání UI.

Obrázek 19: Montáž venkovních žaluzií na rám okna s ovládáním (Almma, 2020)

Vzhledem k tomu, že v tabulce hodnocení hrozeb vyšly hrozby akustického vyzařování přes okna jednací místnosti a okna místnosti pro zpracování utajovaných informací jako nežádoucí, řešení pomocí venkovních bezpečnostních žaluzií řeší i tyto dvě rizika, jelikož venkovní žaluzie snižují hluk, který vychází jak ven, tak dovnitř.

8.6 Vizuální vyzařování přes okna jednací místnosti

Stejně jako v kapitole 8.5, je nebezpečné vizuální vyzařování přes okna této místnosti. Ještě větší hrozbou je potom větší terasové okno, které slouží i jako vstup na tuto terasu. Z okna této místnosti lze také pozorovat vedlejší budovu, která slouží k jiným účelům,, cizí společnosti. Z tohoto důvodu je zde velmi velké riziko kompromitace dat vlivem vizuálního vyzařování. Abychom zachovali stejné podmínky jako v kapitole 8.5 (větrání), použijeme

zde stejný způsob zabezpečení. Vnitřní žaluzie na okně místnosti a také na balkonových dvoukřídlích dveřích. Dále budou použity venkovní bezpečnostní žaluzie stejně jako v kapitole 8.5.

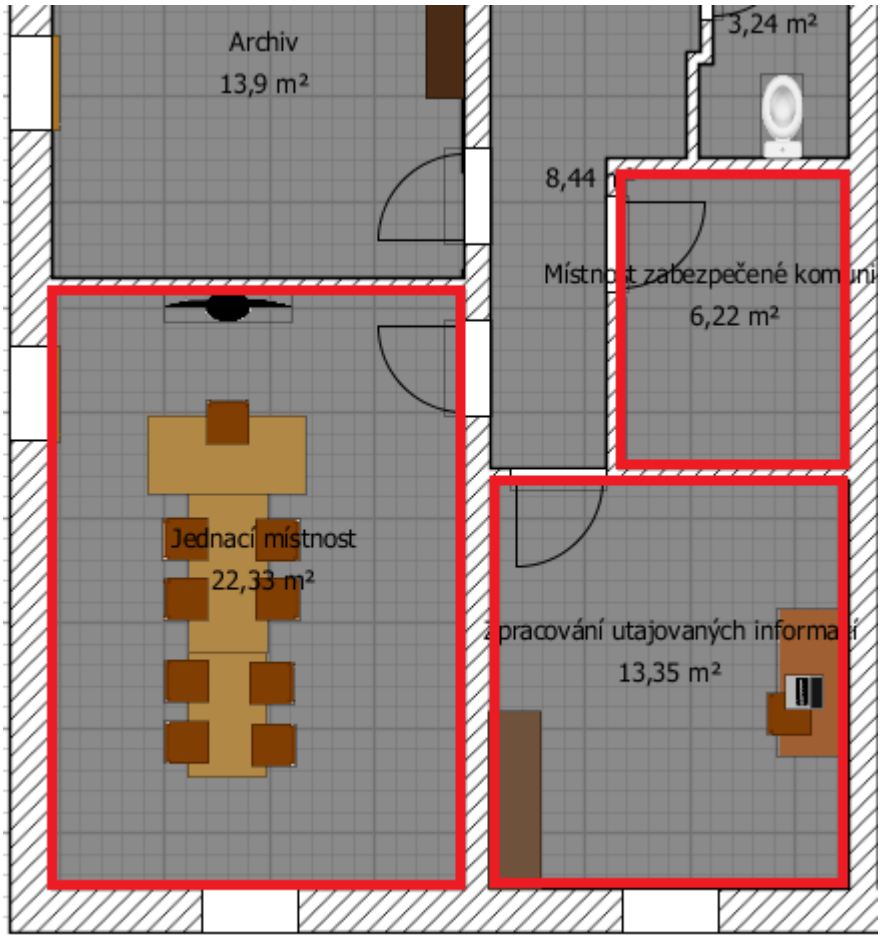
8.7 Elektromagnetické vyzařování počítačových komponent

Velkou hrozbou v oblasti kompromitujícího vyzařování je elektromagnetické vyzařování počítačových komponent. Metod pro ochranu před touto hrozbou je několik. Nejspolehlivější ochranou je stavba stíněné klece. Existuje mnoho firem, které se této problematice věnují. Po pečlivém prostudování všech možných variant, se jako nejlepší varianta jeví řešení pomocí letovaných stínících panelů, které mají tloušťku pouhých 0,3mm. Tyto panely tedy nezabírají mnoho místa a dají se lehce stavebně překrýt minerální vatou a sádrokartonovou stěnou, kdy stejný systém byl použit v kapitole 8.2.

Obrázek 20: Stínící panely (Mudroch Labs s.r.o., 2021a)

Dle výrobce tyto panely zabraňují jak kompromitujícímu vyzařování, tak místnost chrání proti úniku informací pomocí odposlechů. Jako nejslabší článek ve vytvoření stíněné komory se jeví pouze okno. Vzhledem k funkčnosti stíněné komory se tento článek musí do konstrukce zahrnout také. Vzhledem k tomu, že okna kvůli architektonickému rázu musí být zachována, bude použito skleněné dvojsklo s metalickou síťkou mezi skly. Pokud ovšem bude okno otevřené, místnost ztrácí funkci stíněné komory. Je proto nezbytné, aby ve směrnicích bylo uvedeno, že v případě zpracovávání nebo projednávání utajovaných informací musí být okna v zavřeném stavu. Dveře místnosti musí být speciálně upraveny pro stínící komoru. Tyto dveře musí splňovat kompaktní vodivý kontakt po obvodu dveří.

Pokud již vezmeme v potaz, že se dveře budou měnit, osadí se dveře režimovým vstupem na zadávání hesla do místností 2.3, 2.4 a 2.5 (Techniserv, 2008).



Obrázek 21: Červeně znázorněna stínící komora (Zdroj: Vlastní)

Dalším řešením v oblasti elektromagnetického vyzařování počítačových (a vlastně veškerých elektronických komponent), je použití tempestovaných počítačových sestav. Tyto komponenty jsou měřeny a testovány ve speciálních laboratořích a vyzařují co nejméně elektromagnetických vln. Pokud spojíme stínící komoru s tempestovanou sestavou snížíme hrozbu úniku utajovaných dat na minimum. Variant jakou sestavu použít je několik. Od počítačů typu all in one (jedná se o počítač spojený s obrazovkou do jednoho celku), tak si můžeme poskládat sestavu zvlášť z jednotlivých komponent. U počítačových sestav je vzhledem ke spojení do jednoho celku problematická výměna jednotlivých komponent. Abychom zachovali dostupnost informací, bude pro potřeby diplomové práce použit výběr jednotlivých komponent zvlášť. Do místnosti pro zpracování utajovaných informací bude použit stolní počítač značky Dell Precision T3620 spolu s 24“ LCD monitorem Dell U241. Obě zařízení splňují požadavky NSTISSAM TEMPEST/1 -92, úroveň I; CID09/15A,

úroveň I; a SDIP-27 úroveň A. Jako periferní zařízení byly vybrány klávesnice a myš Emcon SST TEMPEST USB viz obrázek 22. Obě tyto zařízení splňují požadavky na co nejmenší elektromagnetické vyzařování. Do Stanice se připojují pomocí USB portu (APItech, 2021b; APItech, 2021c; APItech, 2021d).

Obrázek 22: Vybraná tempestovaná sestava (APItech, 2021b; APItech, 2021c; APItech, 2021d)

Obrázek 23: Tiskárna HP 577 Laserjet MFP (APItech, 2021a)

Dalším zařízením, které může vyzařovat elektromagnetické vyzařování je tiskárna. Ta z bezpečnostních důvodů bude připojena pouze lokálně do portu USB. Jedním z produktů splňující normy pro tempestovaná sestavy je tiskárna Emcon and SST TEMPEST HP 577 Laserjet MFP, která je zobrazena na obrázku 23 (APItech, a2021).

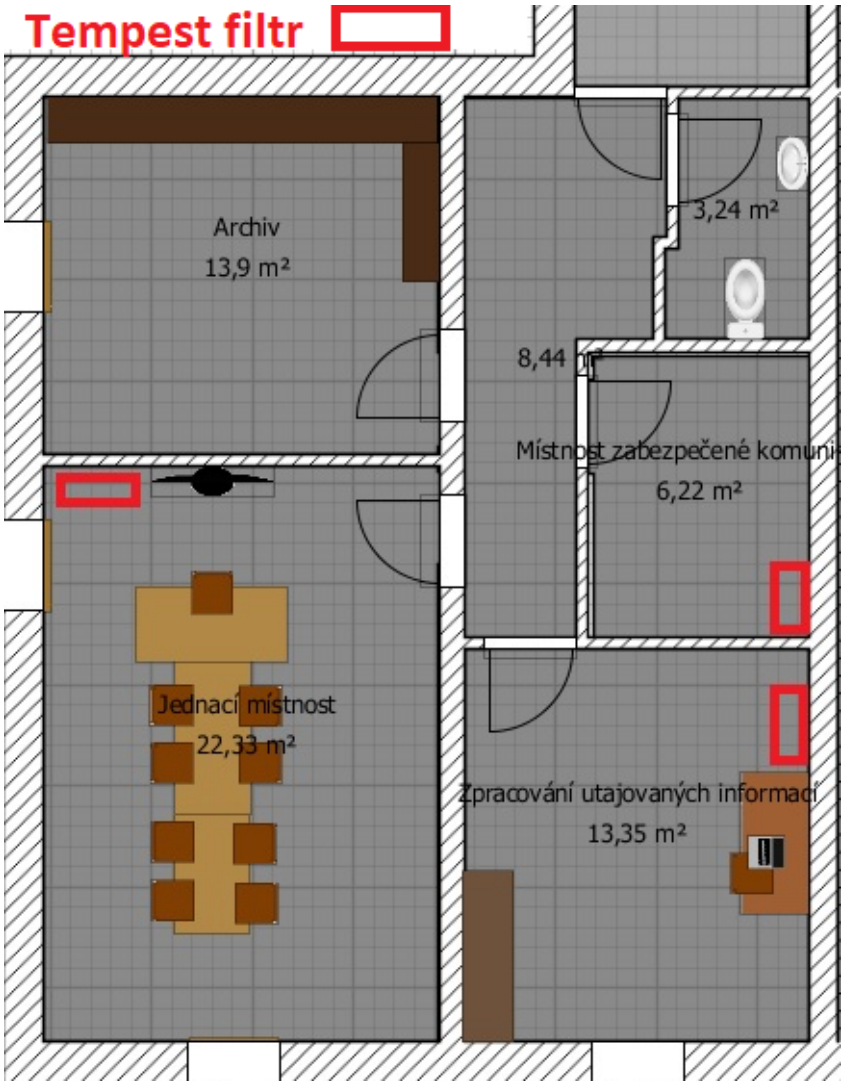
8.8 Získání dat z nezabezpečené sítě LAN

Hrozbou, která přímo nesouvisí s kompromitujícím vyzařováním, ale je neméně důležitá je rekonstrukce ze signálů po LAN kabelech. Před fyzickým napojením je kabel ochráněn tím, že je instalován přímo ve stěně, tudíž není možné se k němu bez povšimnutí dostat a napojit se na komunikaci například pomocí wiretappingu. Jediné riziko je při přímém přenosu těchto dat do sítě internet. Ochranou proti takovému získání dat je zabráněno zařízením zabezpečené komunikace, které bude umístěno v místnosti 2.3. Přesný typ zabezpečení nelze z bezpečnostních důvodů uvádět. Toto zařízení musí obsluhovat pouze osoba, která splňuje podmínky personální bezpečnosti a současně musí být dodrženy podmínky fyzické bezpečnosti. Abychom zabránili úniku informací vlivem kompromitujícího vyzařování z kabelu LAN do například datové nebo rozvodné sítě, musíme dodržet určité vzdálenosti při vedení kabelů ve stěně. Obecně vzato je nejlepším způsobem vést elektrické kabely a kabely LAN vždy od sebe vzdáleně. Například kabely LAN můžeme vést ve stěně při zemi a elektřinu u stropu. Tímto způsobem vyřešíme dvě hrozby vycházející z analýzy hrozeb a to hrozbu rekonstrukce signálů ze zdrojů LAN, která byla hodnocena stupněm nežádoucí, ale také hrozbu získání dat z nezabezpečené sítě LAN v oblasti bezpečnosti informačních a komunikačních systémů, která byla hodnocena stupněm nepřijatelná hrozba.

8.9 Rekonstrukce signálů z vedení elektrického napětí 230V

Kompromitující vyzařování se šíří všemi možnými cestami. Nejohroženější cestou šíření kompromitujícího vyzařování v budovách je vedení elektrického napětí 230V, ke kterému jsou připojeny veškeré komunikační a informační systémy, které zpracovávají, případně předávají utajované informace. Kromě toho, že LAN kabely v budově povedou vzdáleně od vedení elektrického napětí 230V musí být toto napětí ochráněno proti kompromitujícímu vyzařování. Nejčastějším opatřením je použití síťových filtrů. Nejjednodušší řešení pro použití v budově je použití TEMPEST vysokofrekvenčních filtrů zapojených do zásuvky viz obrázek 24. Do tohoto filtru je poté zapojeno určité zařízení nakládající s UI. Jednotlivé rozmístění filtrů bude dle obrázku 25.

Obrázek 24: Příklad TEMPEST VF filtru (MPE, 2021)



Obrázek 25: Rozmístění TEMPEST VF filtrů (Zdroj: Vlastní)

Pro zajištění bezpečnosti bude filtr umístěn v místnostech 2.5, 2.4 a 2.3. V místnosti 2.5 bude do filtru zapojena počítačová sestava spolu s tiskárnou.

8.10 Elektromagnetické vyzařování LCD TV v místnosti 2.4

U hrozby elektromagnetického vyzařování elektronických zařízení jako je LCD TV umístěna v místnosti 2.4, je hrozba snížena pomocí instalace letovaných stínících panelů a vsazení skleněného dvojskla s metalickou síťkou mezi skly. Dále je také možno odstínit samostatné kabely televize. Jelikož televize nebude napojena přímo na anténu, nehrozí zde hrozba úniku dat tímto způsobem. K připojení elektronických dokumentů promítaných na televizi bude sloužit port USB ze strany televize. V tomto případě lze USB port televize chránit pomocí rozbočovače, který splňuje podmínky pro nízké elektromagnetické vyzařování. K televizi bude připojen rozbočovač SI-Model 2181/2 viz obrázek 26, který může fungovat na větší vzdálenosti pomocí optického kabelu.

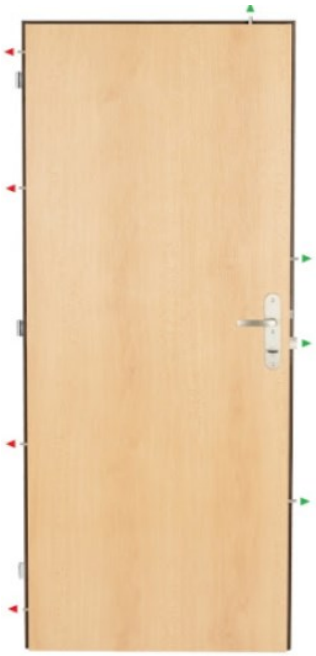
Obrázek 26: SI-Model 2181/2 (Cordsen Engineering, 2021)

Toto zařízení disponuje čtyřmi USB porty. Do zařízení, se kterým bude počítač komunikovat, se rozbočovač zapojí pomocí přípojky USB - typ B. Zařízení bude umístěno na hlavním pracovním stole místnosti. Optický kabel bude vedený v lištách po okraji místnosti (Cordsen Engineering, 2021).

8.11 Násilný vstup přes vchodové dveře

Jelikož aktuálně použité vchodové dveře SAPELI jsou pouze ohnivzdorné a mají pouze obyčejné kování, je nutné tyto dveře vyměnit, aby se zabránilo vstupu do oddělení nepovolaným osobám. Je vhodné použít bezpečnostní dveře, které splňují požadavky pro ochranu od NBÚ a jsou certifikovány dle platných norem NBÚ. Pro vstup do oddělení

budou zvoleny bezpečnostní dveře, které mohou po úpravách od výrobce splňovat normy pro stupeň utajení přísně tajné. Do oddělení budou instalovány dveře od společnosti Sherlock typ Securido Exkluzív viz obrázek 27. Tyto bezpečnostní dveře po úpravách od výrobce mohou splňovat normu na utajení stupně přísně tajné.



Obrázek 27: Sherlock typ Securido Exkluzív (4Lock, 2021)

Dveře budou osazeny nerezovým prahem a vsazeny do ocelové zárubně. Dveře také obsahují bezpečnostní vložku ISEO R6 a vícebodové uzamykání ukryté ve dveřích.

8.12 Násilný vstup přes okna

Některé okna budovy jsou již ze svého stavebního hlediska chráněny proti neoprávněnému vniknutí, jelikož se oddělení nachází ve druhém podlaží. Přes okno v místnosti 2.4 je téměř nereálné násilně vniknout do oddělení vzhledem k jeho výšce. Násilný vstup přes okna všech místností už ovšem omezují opatření v kapitolách 8.5, 8.7 a 8.13, kde byly použity opatření v podobě venkovních bezpečnostních žaluzií a speciálních oken zamezujícím kompromitujícímu elektromagnetickému vyzařování.

8.13 Vstup přes terasu

Pro jakoukoliv budovu, která slouží k podobným účelům je nebezpečí vniku ze střechy zvýšena, pokud je zde umístěn předsunutý balkon/terasa. Abychom zamezili jednoduchému přístupu případného útočníka ze střechy budovy na terasu oddělení a jeho následným

jednoduchým vniknutím přes okna či dveře do oddělení můžeme na tuto terasu nainstalovat jednoduchou ocelovou konstrukci se střechou a případným mřížováním po celé jeho ploše, viz obrázek 28.

Obrázek 28: Návrh střechy terasy s případným zamřížováním (Zdroj: Vlastní)

Instalací zastřešení a mříží, zamezíme jednoduchému přístupu na terasu a také omezíme viditelnost do oken místností.

8.14 Pořizování zvukových záznamů, fotografií/videa

Abychom zabránili používání mobilních telefonů a jiných zařízení umožňující nahrávání zvuku, videa, případně fotografií, je nutné zřídit úložné schránky pro jakoukoliv návštěvu, která do oddělené vstoupí. Tato návštěva bude povinna uzamknout do připravených schránek veškerá elektronická zařízení, kterými jsou i chytré hodinky. Vždy pokud opustí zabezpečené oddělení, mohou své zařízení ze schránek vyjmout. Tím se zamezí vnášení zařízení do zabezpečeného oddělení a nechtěnému vynášení utajovaných informací.

8.15 Antivirová ochrana informačních zařízení

Každé počítačové zařízení potřebuje určitou ochranu ať už v podobě firewall tak i antivirovou ochranu. Jelikož bude veškerá komunikace z oddělení chráněna zařízením zabezpečené komunikace, není potřeba tak velké antivirové ochrany. Pro potřeby antivirové ochrany je zvolen antivirový program od společnosti McAfee. Je ovšem potřeba chránit zařízení před útoky a viry, které se nacházejí mimo internet. Uživatel může přinést vir přímo

na flash disku. Proto antivirus disponuje kontrolou zařízení po jeho zapojení. Jelikož není potřeba v uživatelském rozhraní instalovat jakékoliv soubory ale pouze zpracovávat textové a jiné dokumenty je antivirus nastavený tak, aby detekoval jakýkoliv spustitelný soubor na flash disku a tuto hrozbu okamžitě zastavil a uložil do antivirové truhly. Po každém takovém incidentu, kdy antivirus detekuje hrozbu je nutné výpočetní zařízení zkontrolovat a důkladně vyhledat veškeré možné hrozby.

8.16 Neoprávněný vstup do místnosti se zařízením zabezpečené komunikace

Jak již bylo zmíněno v kapitole 8.8, do místnosti se zařízením zabezpečené komunikace mohou vstupovat pouze osoby, které splňují podmínky personální a fyzické bezpečnosti. Další hrozbou spjatou s neoprávněným vstupem je velmi jednoduchý přístup do těchto místností. Aktuálně jsou v místnostech osazeny obyčejné interiérové dveře. Místo aktuálních dveří a jejich rámů budou osazeny kovové zárubně a bezpečnostní interiérové dveře společně s elektronickým přístupem na kód, který budou znát jen oprávnění uživatelé. Tento kód se bude v náhodném časovém horizontu měnit. Dále by tyto dveře měli být osazeny alarmem, aby se zamezilo tomu, že dveře do místnosti zůstanou otevřené.. V případě toho, že oprávněná osoba dveře za sebou nezavře, po zhruba 20s od jejich otevření se spustí hlasitý alarm. V případě že bychom tento problém řešili pouze automatickým zavíracím systémem Brano, je zde velká hrozba lidského selhání.

8.17 Neoprávněný vstup do místnosti ke zpracování utajovaných informací

Pro oprávněný vstup do místnosti pro zpracování utajovaných informací bude vytvořen seznam osob, které mohou do místnosti vstupovat samostatně a také seznam osob, které mohou vstupovat do místnosti s doprovodem. Musíme také rozdělit situace, kdy je riziko, že se návštěva seznámí s utajovanou informací a kdy je tomuto riziku zamezeno. V případě, že například bude v místnosti vše uloženo v trezoru a informační zařízení bude ve vypnutém stavu, není tudíž k dispozici žádná utajovaná informace, se kterou by se mohla neoprávněná osoba seznámit. Tyto případné kompromitující materiály budou uloženy vždy po skončení prací v trezoru.

Obrázek 29: Trezor BST-418 (JPkontakt, 2021)

V místnosti pro zpracování utajovaných informací bude uložen trezor BST-418 s bezpečnostní třídou II, pro stupeň utajení až přísně tajné. Stejně jako v místnosti se zařízením zabezpečené komunikace bude tato místnost osazena kovovými zárubněmi a bezpečnostními interiérovými dveřmi s elektronickým zámkem a alarmem.

8.18 Neoprávněný vstup do jednací místnosti

Stejně jako v případě místnosti pro zpracování utajovaných informací je velmi důležité ochránit projednávané informace před jejich vyzrazení neoprávněným osobám. Jelikož se v této místnosti nenachází zařízení pro ukládání utajovaných informací, v případě, že se zde tyto informace neprojednávají je velmi malé riziko, jejich vyzrazení. V případě, že se zde budou projednávat utajované informace a budou promítané i na LCD TV, která je umístěna v tomto oddělení, hrozba vyzrazení UI stoupá. Proto je nutné zde také instalovat stejně jako v kapitole 8.16 bezpečnostní interiérové dveře s elektronickým zámkem a také z důvodu bezpečnosti i alarm, aby se zabránilo tomu, že dveře zůstanou otevřené.

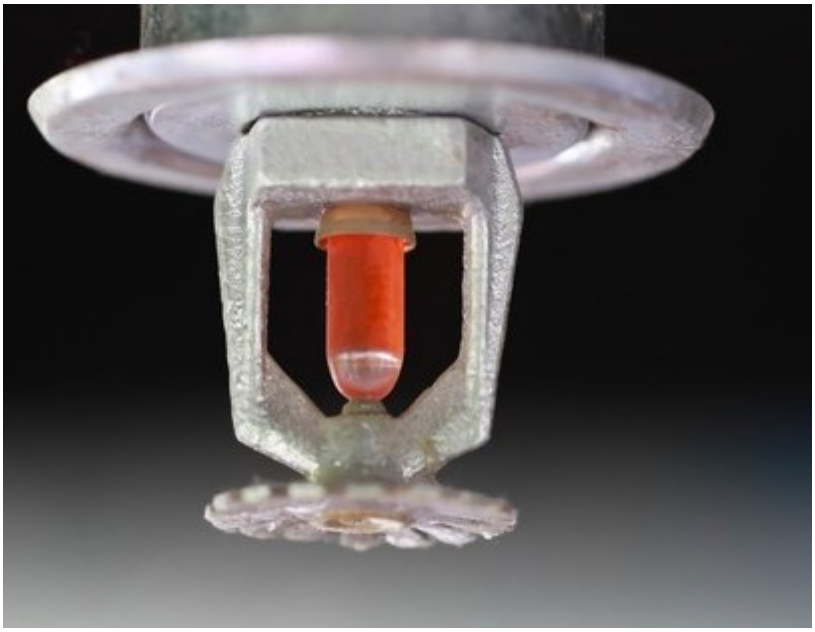
8.19 Mírné hrozby

U všech mírných hrozeb byla hrozba snížena v průběhu ošetření nežádoucích a nepřijatelných hrozeb. Neoprávněnému vstupu do oddělení bylo zabráněno instalací bezpečnostních dveří Sherlock typ Securido Exkluzív. Pokud i tak neoprávněná osoba vstoupí do oddělení, je hrozba, že se seznámí s utajovanou informací velmi nízká, jelikož místnosti, kde se utajované informace nacházejí, jsou zabezpečeny zvlášť. Při nekontrolovaném vstupu do jednotlivých místností musí být sepsán dokument, který bude umístěn u vstupu do oddělení a ve kterém budou uvedena jména oprávněných osob. Dále zde musí být umístěna také kniha vstupu pro případné návštěvy, kde se každá návštěva musí zapsat včetně času příchodu a odchodu a svého identifikačního čísla například rodného čísla, či osobního čísla zaměstnance.

V případě hrozby v podobě evakuačního plánu, musí být plán sepsán i pro toto oddělení zvlášť, jelikož není možné opustit oddělení bez provedení bezpečnostních opatření pro ochranu utajovaných informací. V evakuačním plánu pro oddělení musí být uveden postup pro rychlé, ale i bezpečné opuštění budovy.

- Ukončit práci na zařízení a uložit veškeré kompromitující dokumenty a zařízení pro ukládání kompromitujících dokumentů uložit do úschovného zařízení.
- Vypnout veškerá zařízení pro zpracování utajovaných informací.
- Uzavřít a uzamknout všechny místnosti, ve kterých se zpracovávají utajované informace.
- Provést veškerá opatření dle směrnic pro zařízení zabezpečené komunikace.
- Uzavřít a uzamknout místnost 2.3.
- Uzavřít a uzamknout oddělení a opustit budovu.

Pokud do oddělení vnikne požár, je nejmenší riziko nechat oddělení kontrolovaně vyhořet. Není možné sem vpustit hasičské jednotky, protože je zde riziko seznámení se s utajovanou informací. Proto celé oddělení musí být vybaveno požárními detektory a automatickým hasicím zařízením, které bude instalováno při úpravách stropu proti akustickému kompromitujícímu vyzařování. Automatické hasicí zařízení je znázorněno na obrázku 30.



Obrázek 30: Stabilní hasicí zařízení (Tzb-info, 2019)

V případě vytopení budovy je hrozba úniku utajovaných informací pouze mírná. V případě, že by zařízení bylo zničeno vodou, je nepravděpodobné, že by se někdo seznámil s utajovanou informací. Toto zařízení ovšem musí být odborně zničeno, jelikož pevný disk pořád uchovává utajované informace. V případě že bude zařízení zničeno částečně, je možné tyto komponenty zaměnit za stejné. Pokud bude zničeno oddělení, je nutné po stavebních úpravách provést novou certifikaci.

ZÁVĚR

Cílem diplomové práce bylo přiblížit problematiku kompromitujícího vyzařování na vybraném typu objektu v zastavěné oblasti, analyzovat hrozby pro tento objekt a navrhnout řešení těchto hrozeb. Pro tento příklad byla vybrána náhodná budova, která se nachází v hustší zástavbě okolních budov. V teoretické části byla popsána problematika v oblasti kompromitujícího vyzařování z hlediska legislativy české ale i zahraniční. Dále byly v teoretické části popsány principy odposlechu a nebezpečí spojené s kompromitujícím vyzařování.

V praktické části byla provedena analýza hrozeb pro zjištění současných hrozeb pro budovu, ve které se budou zpracovávat a projednávat utajované informace důvěrné a vyšší dle zákona 412/2005 sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. Analýza hrozeb byla provedena na základě podrobného zkoumání a pozorování budovy z hlediska použitých stavebních materiálů a stavebních prvků.

Z analýzy hrozeb vyplývá 28 možných hrozeb, z nichž 8 bylo hodnoceno jako nepřijatelné a jejich ošetření muselo být provedeno okamžitě, 14 hrozeb bylo nežádoucích a 6 hrozeb bylo mírných. V praktické části proto bylo při ošetření hrozeb postupováno od nepřijatelných hrozeb až po mírné hrozby, jelikož v ochraně utajovaných informací je každá hrozba, která může zapříčinit únik utajovaných informací nebezpečná. Zavedením opatření v oblasti kompromitujího vyzařování se tyto hrozby snížili na přijatelné a budova může projít certifikačním řízením pro zpracování utajovaných informací.

Některé z uvedených opatření se mohou jevit jako naddimenzovaná. Je to z toho důvodu, že budova by mohla být pro budoucí použití certifikována na vyšší stupeň utajení bez velkých stavebních úprav. Tyto návrhy byly konzultovány s odborníky na danou problematiku.

Cílem praktické části bylo přiblížit problematiku kompromitujícího vyzařování, provést analýzu hrozeb a navrhnout opatření pro jejich snížení. Tyto cíle diplomové práce byly splněny, jelikož všechny hrozby, které byly analyzovány, byly na základě zavedených opatření zmírněny.

SEZNAM POUŽITÉ LITERATURY

AC/35-D/2000-REV8: DIRECTIVE ON PERSONNEL SECURITY, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2000-REV8. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

AC/35-D/2001-REV3: DIRECTIVE ON PHYSICAL SECURITY, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2001-REV3. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

AC/35-D/2002-REV5: *DIRECTIVE ON THE SECURITY OF NATO CLASSIFIED INFORMATION*, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2002-REV5. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

AC/35-D/2003-REV5: DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2003-REV5. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

AC/35-D/2004-REV3: Primary Directive on CIS Security, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2004-REV3. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

AC/35-D/2005-REV3: MANAGEMENT DIRECTIVE ON CIS SECURITY, 2020. In: . SECURITY COMMITTEE, ročník 2020, AC/35-D/2005-REV3. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

Akustická pěna: Jak na odhlučnění podlahy [online], 2021. Praha: akusticka-pena [cit. 2021-03-22]. Dostupné z: https://www.akusticka-pena.cz/poradime-vam/jak-na-odhlucneni-podlahy/

Almma: Bezpečnostní rolety [online], 2020. Plzeň: Xcreative [cit. 2021-03-22]. Dostupné z: https://www.almma.cz/produkty/venkovni-rolety/bezpecnostni-rolety/

APItech: Emcon and SST TEMPEST Medium Sized Commercial MFP [online], 2021a. apitech [cit. 2021-03-22]. Dostupné z: https://www.apitech.com/products/secure-systems-information-assurance/tempest-desktop/printers/hp577-laser-a4/

APItech: Emcon and SST TEMPEST Mini Tower [online], 2021b. apitech [cit. 2021-03-22]. Dostupné z: https://www.apitech.com/products/secure-systems-information-assurance/tempest-desktop/pcs-computers/emconsst-brand-tempest-sc3620tf/

APItech: Emcon and SST TEMPEST USB Keyboard [online], 2021c. apitech [cit. 2021-03-22]. Dostupné z: https://www.apitech.com/products/secure-systems-information-assurance/tempest-desktop/accessories/tempest-usb-keyboard/

APItech: Emcon and SST TEMPEST 24" High Resolution [online], 2021d. apitech [cit. 2021-03-22]. Dostupné z: https://www.apitech.com/products/secure-systems-information-assurance/tempest-desktop/monitors/tempest-24-widescreen-lcd-flat-panel-display/

Autocont: Ochrana dat před únikem a krádeží [online], 2021. Ostrava: Autocont [cit. 2021-03-22]. Dostupné z: https://www.autocont.cz/portfolio/kyberneticka-bezpecnost/ochrana-dat-pred-unikem-a-kradezi

BALOGH, Bc. Petr, 2018. *Ochrana informací před jejich únikem vlivem kompromitujícího vyzařování*. Ostrava. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Ing. Jana Pupíková, Ph.D.

Ciurshop: WOLF PhoneStar TRI 15 mm [online], 2021. CIUR [cit. 2021-03-22]. Dostupné z: http://www.ciurshop.cz/WOLF.0247-WOLF-PhoneStar-TRI-15-mm-vysoce-ucinna-akusticka-deska.html

CNET: How a spy type microburst transmitter works AKA cell phone [online], 2021. A RED VENTURES COMPANY [cit. 2021-03-22]. Dostupné z: https://www.cnet.com/forums/discussions/how-a-spy-type-microburst-transmitter-works-aka-cell-phone/

Cordsen Engineering: TEMPEST Media Converter [online], 2021. Seligenstadt, Germany: Yougrids [cit. 2021-03-22]. Dostupné z: https://www.cordsen.com/index.php/de/component/content/article/36-tempest/tempest-level-b/media-converter-b/99-media-converter-si-model-21812

ČESKO, 2005a. *Vyhláška č. 523/2005 Sb.: Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými*

informacemi a o certifikaci stínicích komor. In: . Praha, ročník 2005, částka 179, číslo 523. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-523?citace=1

ČESKO, 2005b. *Vyhláška 525/2005 Sb.: o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací*. In: . Praha, ročník 2005, částka 179, číslo 525. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1086-vyhlaska-c-5252005/

ČESKO, 2005c. *Vyhláška č. 528/2005 Sb. Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků*. In: . Praha, ročník 2005, částka 179, číslo 528. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-528

ČESKO, 2011. *Vyhláška č. 432/2011 Sb.: o zajištění kryptografické ochrany utajovaných informací*. In: . Praha, ročník 2011, číslo 432. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1084-vyhlaska-c-4322011/

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

Dynamicscience: R-1550B TEMPEST TEST RECEIVER [online], 2021. Chatsworth, USA: Dynamic Sciences [cit. 2021-03-22]. Dostupné z: http://www.dynamicsciences.com/r-1550b-tempest-test-receiver/

EO Security: EO Security [online], 2021. https://eo-security.cz/odposlouchavaci-zarizeni/ [cit. 2021-03-22]. Dostupné z: https://eo-security.cz/odposlouchavaci-zarizeni/

G. KUHN, Marcus, 2003. *Compromising emanations: eavesdropping risks of computer displays*. Number 577. Cambridge: University of Cambridge. ISSN 1476-2986.

Gutta: Guttasilent akustické desky AMB [online], 2015. Kladno: Gutta [cit. 2021-03-22]. Dostupné z: https://www.guttashop.cz/guttasilent-akusticke-desky-amb-.8137/?vid=17532&utm_source=google&utm_medium=search&utm_campaign=nanaku&gclid=Cj0KCQiApY6BBhCsARIsAOI_Gjb1K-kTiwY0lkQJs2uC2FN-chxL_wpfR8S4rrptDmt0EDKL_J4wd68aAi5ZEALw_wcB

Hackinglab: Wiretapping [online], 2019. © AEC [cit. 2021-03-22]. Dostupné z: https://hackinglab.cz/blog/wiretapping/

HISTORY OF CODENAME: TEMPEST [online], 2020. Germany: Interelektronix [cit. 2021-02-09]. Dostupné z: https://www.interelectronix.com/history-of-codename-tempest.html

Info Safe: Kontrola radiovým scannerem [online], 2020. Infosafe [cit. 2021-03-22]. Dostupné z: https://www.infosafe.cz/kontrola-radiovym-scannerem

JPKONTAKT: BST - 418 TREZOR SKŘÍŇOVÝ [online], 2021. Pardubice: JP-Kontakt [cit. 2021-03-22]. Dostupné z: https://www.jp-kontakt.cz/Trezory/Trezorove-archivacni-skrine/BST-418-trezor-skrinovy-1790x800x600-mm-bezpecnostni-trida-II-_d6387350_10899.aspx

MAISNER, Martin, 2015. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 978-807-4788-178.

Mapy Google [online], 2011. Mountain View: Google [cit. 2021-03-22]. Dostupné z: https://www.google.cz/maps

MPE: TEMPEST Pluggable Filters [online], 2021. Liverpool: MPE [cit. 2021-03-22]. Dostupné z: https://www.mpe.co.uk/products/tempest-pluggable-filters/

Mudroch Labs s.r.o.: Bezpečnostní rolety [online], 2021a. Praha: Mudroch LABS [cit. 2021-03-22]. Dostupné z: https://www.mudrochlabs.sk/faradayovy-stinene-anechoickych-mistnosti-komory/

Mudroch Labs s.r.o.: Ochrana proti odposlechu, odposlouchávací zařízení v praxi [online], 2021b. Mudroch LABS [cit. 2021-03-22]. Dostupné z: http://www.triangulace.cz/ochrana-proti-odposlechu-odposlouchavaci-zarizeni-v-praxi/

Národní bezpečnostní úřad: O nás [online], 2021. Praha: NBÚ [cit. 2021-03-22]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

NÚKIB: O NÚKIB [online], 2021. Praha: NÚKIB [cit. 2021-03-22]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

Notami: Akustická izolace – odhlučnění stěny [online], 2017a. Praha: © Noitami [cit. 2021-03-22]. Dostupné z: http://www.noitami.cz/odhlucneni/odhlucneni-steny-pricky-zdi/

Notami: Odhlučnění stropu proti běžným hlukům – akusticky neprůzvučný podhled [online], 2017b. Praha: © Noitami [cit. 2021-03-22]. Dostupné z: http://www.noitami.cz/odhlucneni/odhlucneni-stropu-podhledu/

SOSelectronic: Proč potřebujeme síťový filtr a jak jej správně umístit? [online], 2021. SOS electronic [cit. 2021-03-22]. Dostupné z: https://www.soselectronic.cz/articles/schurter/proc-potrebujeme-sitovy-filtr-a-jak-jej-spravne-umistit-2261

SpyShop: Detektor analogových a digitálních bezdrátových odposlechů Protect 1206i [online], 2021a. Praha: Paweł Wujcikowski [cit. 2021-03-22]. Dostupné z: https://www.spyshop24.cz/detektor-analogovych-a-digitalnich-bezdratovych-odposlechu-protect-1206i-290.html

SpyShop: Detektor bezdrátových kamer a odposlechů SH-065 [online], 2021b. Praha: Paweł Wujcikowski [cit. 2021-03-22]. Dostupné z: https://www.spyshop24.cz/detektor-bezdratovych-kamer-a-odposlechu-sh-065-291.html

SpyShop: Laserový mikrofon Spectra Laser M pro profesionály a orgány činné v trestním řízení [online], 2021c. Praha: Paweł Wujcikowski [cit. 2021-03-22]. Dostupné z: https://www.spyshop24.cz/laserovy-mikrofon-spectra-laser-m-pro-profesionaly-a-organy-cinne-v-trestnim-rizeni-457.html

Techniserv: TRENDY V ELEKTROMAGNETICKÉM STÍNĚNÍ [online], 2008. Praha: Techniserv [cit. 2021-03-22]. Dostupné z: https://docplayer.cz/6041053-Trendy-v-elektromagnetickem-stineni.html

Topspy: GSM odposlech - špionážní štěnice TopSpy G10 [online], 2020. Praha: Butta Trade [cit. 2021-03-22]. Dostupné z: https://topspy.cz/produkt/gsm-odposlech-spionazni-stenice-topspy-g10

Tzb-info: Stabilní hasicí zařízení v ochraně budov před požárem [online], 2019. Topinfo [cit. 2021-03-22]. Dostupné z: https://www.tzb-info.cz/pozarni-bezpecnost-staveb/19047-stabilni-hasici-zarizeni-v-ochrane-budov-pred-pozarem-cast-1

VUAGNOUX, Martin a Sylvain PASINI, 2009. *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*. USENIX security symposium.

Webopedia: Tempest [online], 2020. Webopedia Staff [cit. 2021-03-22]. Dostupné z: https://www.webopedia.com/definitions/tempest/

WHITMAN, Michael E. a Herbert J. MATTORD, 2017. *Management Of Information Security*. Fifth Edition. Boston, USA: Cengage Learning. ISBN 978-1-305-50125-6.

4LOCK: Bezpečnostní dveře Securido Exkluzív [online], 2021. Praha: Insion [cit. 2021-03-22]. Dostupné z: https://4lock.cz/bezpecnostni-dvere-securido-r-exkluziv

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AKU	Akustický
apod.	a podobně
BTS	Base Transceiver Station
C.I.A.	Confidentiality, integrity, availability
cm	centimetr
CRT	Cathode Ray Tube
č.	Číslo
dB	Decibel
DVI	Digital Visual Interface
EMC	Elektromagnetic Compatibility
FM	Frekvenční modulace
Gbit/s	Gigabit za sekundu
GPS	Global Positioning System
GSM	Groupe Spécial Module
H	Názor hodnotitelů
HP	Hewlett Packard
HW	Hardware
IEC	Mezinárodní elektrotechnická komise
IMSI	International mobile subscriber identity
Inc.	Incorporated
ISO	International Organization for Standardization
LAN	Local Area Network
LCD	Liquid Crystal Display
m	Metr
mm	Milimetr

MDF	Medium density fibreboard
MFP	Multifunction Printer
N	Pravděpodobnost následků
NATO	North Atlantic Treaty Organization
NBÚ	Národní bezpečností úřad
NÚKIB	Národní úřad pro kybernetickou bezpečnost
Obr.	Obrázek
Odst.	Odstavec
OSB	Oriented strand board
P	Pravděpodobnost vzniku
PC	Personal computer
Písm.	Písmena
R	Celkové hodnocení hrozeb
REV	Revize
RF	Rádiové frekvence
Sb.	Sbírky
Si	Tepelně izolační vlastnost
SIM	Subscriber identity module
STP	Shielded Twisted Pair
SW	Software
TV	Television
UEBA	User and Entity Behavioral Analyse
UI	Utajované informace
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
V	Volt

VF	Vysokofrekvenční
VGA	Video Graphics Array
VPN	Virtual private network
WC	Water Closet
WI-FI	Wireless Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: 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: T00[redacted]/20[redacted]

Bezpečnostní dveře A[redacted] se zvýšenou bezpečností

typ [redacted]

(Název a typové označení technického prostředku)

Výrobce: [redacted] - Bezpečnostné dvere[redacted]

Sídlo: [redacted]

832 21 Bratislava

IČ: 35757094

Držitel: A[redacted] Bezpečnostní dveře [redacted]

Sídlo: Vojtěšská 1

110 00 Praha 1

IČ: [redacted]

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: 16.1.2011

Datum vydání certifikátu: 7.8.2008

Náměstek ředitele
Národního bezpečnostního úřadu

Ing. Jaroslav ŠMID

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

011789

Přílohy 1/1

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