VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH A NASAZENÍ SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ VE VÝUKOVÉM STŘEDISKU

DESIGN AND DEPLOYMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM IN EDUCATIONAL CENTER

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. ROMANA KŘÍŽOVÁ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2014

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2013/2014
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Křížová Romana, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh a nasazení systému řízení bezpečnosti informací ve výukovém středisku

v anglickém jazyce:

Design and Deployment of Information Security Management System in Educational Center

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2013/2014.

L.S.

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 30.05.2014

Abstrakt

Diplomová práce se zabývá zabezpečením výukového střediska, ve kterém probíhá výzkum zaměřený na chemický průmysl. První část práce vymezuje teoretické znalosti, na jejichž základě se postupuje v praxi. Praktická část se zabývá zabezpečením objektu jak po technické stránce, tak navrhuje školení manažerů i zaměstnanců a nastavuje příslušná práva. Nezbytnou součástí projektu je také orientační cenová kalkulace. Praktická část navazuje na současnou analýzu stávajícího objektu.

Abstract

This Master´s thesis is focused on the security of Educational center running a research aimed at chemical industry. In the first part the theoretical basis followed in the field are defined. The practical part is based on the security of a property considering the technical aspects as well as the suggestions of the trainings of managers and employees and sets respective permissions. A guide price calculation is also essential this project. The practical part evolves the existing analysis of the property.

Klíčová slova

Management informační bezpečnosti, PDCA model, bezpečnost informací, bezpečnost organizace, metodika školení, nastavení práv

Key words

Information security management, PDCA model, security of information, organization security, methodics of training, setting of permissions

Bibliografická citace

KŘÍŽOVÁ, R. *Návrh a nasazení systému řízení bezpečnosti informací ve výukovém středisku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2014. 101 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne …… …….

Křížová Romana

Poděkování

Ráda bych tímto poděkovala vedoucímu práce Ing. Viktoru Ondrákovi a oponentu Ing. Petru Sedlákovi za poskytnutí odborné pomoci, cenných rad a připomínek nepostradatelných pro vypracování diplomové práce.

Poděkování patří také Petru Vejmělkovi za poskytnutí potřebných informací a podkladů, které mi umožnily zpracovat tuto diplomovou práci.

Obsah

Úvod

Výukové středisko, v němž probíhá výzkum z oblasti chemického průmyslu, se může stát terčem útoku jak zvenčí, tak poškozením ze strany manažerů či zaměstnanců zevnitř. Tento objekt je současně i hotelem pro návštěvníky, kteří nemají s výzkumem či různými školeními nic společného. Ať už úmyslně, nebo neúmyslně, i návštěvníci hotelu mohou narušit daný výzkum. Narušení výzkumu a ztráta informací, které mohou přijít do nepovolaných rukou, mohou způsobit závažné škody a velké ztráty.

V diplomové práci se z těchto důvodů zaměřuji na zabezpečení objektu, jak po technické stránce, kde navrhuji nasazení kamer, bezpečnostních oken, tak po stránce bezpečnosti lidí, kterou zajišťují detektory kouře, plynu a další komponenty. Návrh umístění čteček karet už souvisí se zabezpečením i mimo technologii. Příslušní manažeři či zaměstnanci ve výzkumu budou rozhodovat o nastavení práv jednotlivých osob. Důležitou součástí je manažery i zaměstnance zaškolit. Proto se také v praktické části zabývám návrhem metodiky školení.

Pokud přijdeme s návrhem projektu do výběrového řízení i mimo něj, je nezbytné stanovit orientační cenovou kalkulaci. Tato kalkulace neslouží jen investorovi, ale i dodavateli, který bude mít celkový přehled a navíc rozdělení nákladů na materiál a vykonanou práci.

Cíl práce

Cílem práce je navrhnout zabezpečení výukového střediska zaměřeného na výzkum v chemickém průmyslu ve speciálně vybavených laboratořích. V práci bude řešeno umístění bezpečnostních komponent, nastavení práv, návrh metodiky školení, kvalita hesel a jejich obměna, zákaz vybraných činností a také postihy za jejich nedodržování. Cílem je dodržení předem stanovených požadavků investora, včetně rozpočtu, který bude součástí tohoto řešení.

1. Teoretická východiska řešení

Abychom se v této problematice lépe orientovali a chápali se, je nezbytné si objasnit základní pojmy. V této kapitole vysvětlím k čemu je systém řízení informační bezpečnosti užitečný a pro koho je určen. Na modelu PDCA ukáži, jak se nejdříve ustanoví, následně zavede, provozuje, monitoruje a přezkoumává. Na závěr modelu ISMS popíši, jak jej zlepšujeme a staráme se o jeho údržbu. Objasním rozšířené metodiky, které se zabývají i dalšími aspekty řízení informatiky organizací. O zvýšení celkové důvěryhodnosti dodavatele a o plnění požadavků referenčních norem a specifikací bude popisovat kapitola Certifikace ISMS. Závěrem uvedu přínosy, které nám zavedení a certifikace ISMS přinesou.

Systém řízení informační bezpečnosti

Informační bezpečnost obecně zahrnuje celou řadu problémů a jejich řešení. Příkladem můžeme uvést analýzu rizik zabezpečení sítě, fyzických spojů a serveru, digitální podpis, autentizaci, autorizaci, antivirovou ochranu, zálohování apod. Informační bezpečnost je dnes nezbytnou součástí každého informačního systému ve všech organizacích. (1)

Systém řízení informační bezpečnosti (dále jen ISMS) lze zavést a používat v organizaci s deseti zaměstnanci a stejně tak i ve velkém holdingu s tisíci zaměstnanci. Netýká se pouze průmyslových podniků a privátních organizací, ale také veřejně právních institucí a orgánů státu. (1)

Ve velkých firmách a nadnárodních organizací bývá ISMS popsán detailněji než je tomu u malých a středních firem. Implementace a interpretace jednotlivých doporučení se může lišit např.: počtem uživatelů, rozsahem systému, způsobem zpracování dat, reálných bezpečnostních rizik atd. (1)

Pojem ISMS

ISMS (Information Security Management System) je soubor pravidel a opatření, po jejichž zavedení má úplné a správné informace včas k dispozici ten, kdo je skutečně potřebuje a pouze ten, kdo je k přístupu oprávněn. Zahrnuje část celkového systému řízení organizace, který je založen na přístupu organizace k rizikům činností.

Je zaměřen na ustanovení, zavádění a provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. (1)

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv. Jejich cílem je eliminovat možnou ztrátu nebo poškození tím, že určíme aktiva, která se mají chránit. Zvolíme a řídíme možná rizika bezpečnosti informací, zavedeme opatření s požadovanou úrovní záruk a tak kontrolujeme. (1)

Jedná se o systém, který nejen chrání informace organizace před zneužitím či jejich ztrátou, ale také chrání členy vedení a zaměstnance před nechtěnými prohřešky vůči zákonům České republiky. Největším nebezpečím je člověk, který způsobuje většinu bezpečnostních incidentů. (1)

Každý z nás by si měl být vědom, že se bezpečnost informací nedá zajistit stoprocentně. Mělo by být však provedeno vše, aby byla bezpečnost zajištěna na přijatelnou úroveň za ekonomicky zdůvodnitelné náklady. Zde sehrává nezastupitelnou roli řízení rizik, které se stalo nenahraditelným základem každého ISMS. (1)

1.1. Základní pojmy

Základní pojmy jsou nedílnou součástí pro sjednocení terminologie. Proto se těmito pojmy budeme v této kapitole zabývat.

Systémy řízení (2)

IMS – integrovaný systém řízení (integrated MS) – komplexní řízení v organizaci

EMS – systém řízení vztahu k okolí (environmental MS)

QMS – systém řízení kvality (quality MS)

OHASMS – ochrana a bezpečnost zdraví při práci

PDCA model – Demingův model, pro životní cyklus IMS se zpětnou vazbou (Plan-Do-Check-Act)

IT vs. ICT (2)

IT – informační technologie (Information Technology)

ICT – informační a komunikační technologie (Information and Communication Technology)

ICT (2)

Informace – informaci tvoří v informatice kódována data (kódováním není myšleno kryptování)

Data – jsou „plněním“ informace, kterou vytváří

Přenos dat (digitální komunikace) – přenos digitálních zpráv nebo digitalizovaného analogového signálu pomocí fyzického dvoubodového nebo vícebodového přenosového média, kterým může být metalický či optický kabel nebo bezdrátový přenos

Signál – fyzikální vyjádření informace ve formě změn fyzikální veličiny v čase

Informační systém (IS) – lze chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují

ISO/OSI model – sedmivrstvý referenční komunikační model podle něhož dochází k propojování systémů

Bezpečnost (2)

Bezpečnost organizace – nejvyšší kategorie bezpečnosti, objektu a majetku

Bezpečnost IS/ICT – nižší kategorie, ochrana aktiv jako součásti IS na ICT

Bezpečnost informací – nižší kategorie, obecné shrnutí zásad bezpečné práce s informacemi

Bezpečnostní problematika – důležité pojmy (2)

Aktivum – hmotný a nehmotný majetek, rozdělením (skupinami) aktiv je definován rozsah ISMS a stanovené hodnoty slouží jako základ pro analýzu rizik

Rozdělení aktiv:

- informační aktiva (data, informace)
- hardwarová aktiva (hardware)
- softwarové aktiva (software)
- služby poskytované prostřednictvím IS

Ohodnocení aktiv

1) identifikace
2) nástroje k ohodnocení aktiv
3) stanovení stupnice
   - žádný dopad
   - zanedbatelný dopad
   - potíže a finanční ztráty
   - vážné potíže a velké ztráty
   - existenční potíže
4) hodnocení nákladů v důsledku porušení:
   - důvěrnosti
   - integrity
   - dostupnosti

Výpočet hodnoty aktiva

Součtový algoritmus – nejjednodušší a nejpoužívanější

Výpočet - součet všech hodnot jednotlivých komponent se vydělí počtem daných komponent

Hrozba – jakákoliv událost, kterou může být narušena důvěrnost, integrita a dostupnost aktiva (3)

Zranitelnost – jakékoliv slabé místo aktiva na úrovni fyzické, logické či administrativní bezpečnosti, které může být zneužito hrozbou (3)

Opatření – aktivita, zařízení, technika či postup zabraňující účinku i snižující sílu hrozby

Riziko – pravděpodobnost, že hrozba zneužije zranitelnosti a způsobí narušení integrity, důvěrnosti anebo dostupnosti (3)

Dopad – vzniklá škoda v důsledku hrozby

Integrita – u informací je zajištěna správnost a úplnost

Dostupnost – pro oprávněné uživatele je zajištěna dostupnost informací v okamžiku jejich potřeby

Bezpečnostní mechanizmus – technika pro implementaci bezpečnostní funkce jako celku nebo její části

Bezpečnostní funkce – funkce systému přispívající k jeho bezpečnosti (autentizace, autorizace, aj.)

Autentizace – proces ověření integrity (co víš, co máš, co jsi) (4)

Autorizace – získání přístupu k informacím, funkcím a dalším objektům na základě jeho autentizace, může být založeno na omezeních (4)

Analýza rizik – systematické používání informací pro odhad míry rizika a určení jeho zdrojů

Řízení rizik – koordinace potřebná k řízení a kontrole organizace s ohledem na rizika

Hodnocení rizik – proces analýzy a vyhodnocení rizik

Vyhodnocení rizika – proces porovnávání odhadnutého rizika s danými kritérii pro určení jeho významu

Zvládání rizik – proces výběru a přijímání opatření pro snížení rizika

Akceptace rizika – rozhodnutí přijmout riziko

Prohlášení o aplikovatelnosti – dokument s popisem opatření v ISMS organizaci

Příručka bezpečnosti informací (příručka ISMS) – slouží ke zdokumentování všech bezpečnostních opatření a k objasnění bezpečnostních principů všem uživatelům a manažerům

Míra – je ukazatel (i více ukazatelů) určující informační potřebu

Měření – proces získávání informací o účinnosti ISMS

Záznam – je dokument o dosaženém výsledku či důkaz o činnosti v řízení kvality

Metriky – slouží k měření účinnosti bezpečnosti informací

Audit – nezávislý, systematický a dokumentovaný proces sloužící k objektivnímu hodnocení dle předem stanovených kritérií

Přezkoumání – je určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů

Záznam – dokument, ve kterém jsou uvedeny dosažené výsledky nebo ve kterém se poskytují důkazy o provedených činnostech (5, str. 116)

Neshoda – nesplnění požadavku (5, str. 119)

Náprava – opatření k odstranění neshody (5, str. 119)

Opatření k nápravě – je opatření k odstranění příčiny neshody (5, str. 119)

Preventivní opatření – opatření k odstranění potenciální neshody (5, str. 119)

Bezpečnostní politika – jsou pravidla určující systém řízení, ochrany a distribuce aktiv (5, str. 127)

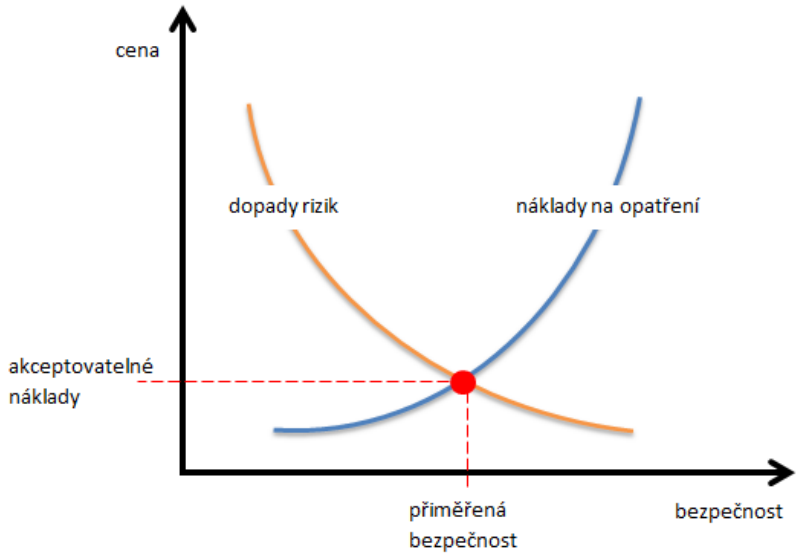
Bezpečnostní událost – identifikovaný stav problému, služby nebo sítě, ukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření (5, str. 149)

Bezpečnostní incident – pojem označující nějakou nestandardní či nepříjemnou bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci (5, str. 150)

Řízení kontinuity organizace (BCM) – je aktivita úzce spojená a podřízená podnikání, která může poskytnout strategický a provozní rámec pro pohled na způsob, jakým organizace poskytuje svoje produkty a služby a jak je přitom odolná proti jejich zničení, narušení nebo ztrátě (5, str. 160)

Systém řízení kontinuity organizace (BCMS) – je řídící proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností organizace, na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty (5, str. 160)

Přiměřená bezpečnost – je velikost úsilí a investic do bezpečnosti IS a musí odpovídat hodnotě aktiv a míře možných rizik. Stanovuje zejména bezpečnostní politika organizace. (2)



Obrázek 1: Přiměřená bezpečnost
Upraveno podle: (2)

Certifikační problematika (2)

Certifikace – potvrzení shody systému řízení na základě norem, zvýšení důvěryhodnosti subjektu

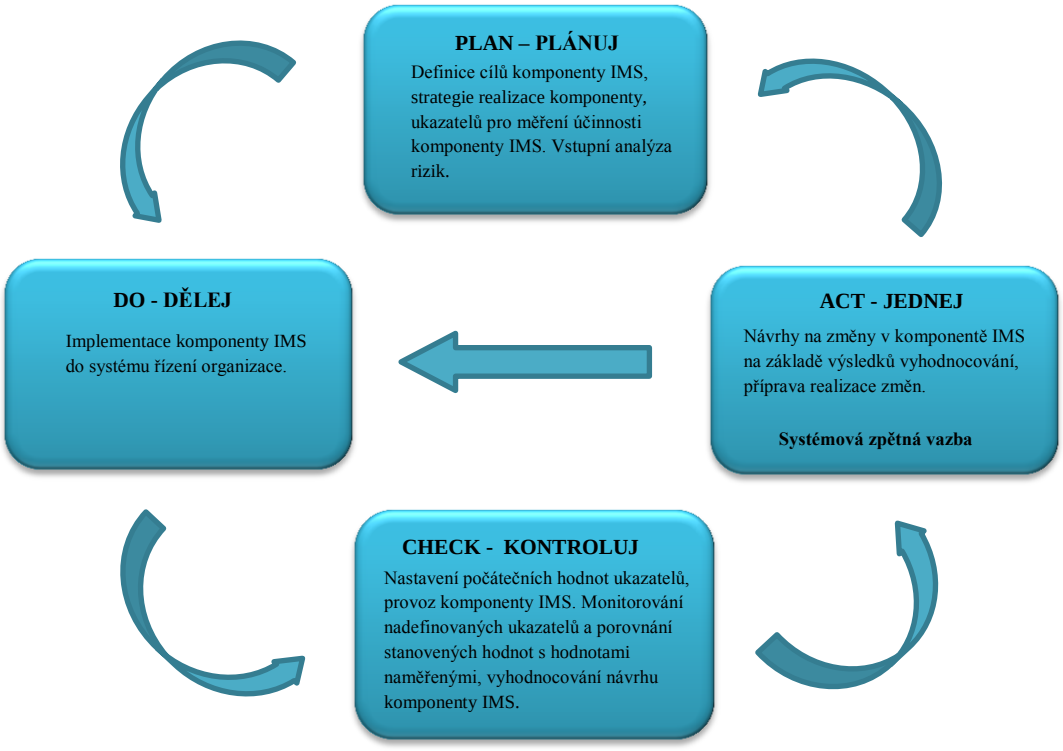
Akreditace – postup pro potvrzení nezávislosti, způsobilosti a objektivity pro činnost

Certifikační orgán – v souladu s normami je třetí strana hodnotící a certifikující systém řízení organizace

1.2. Model ISMS

Systém řízení bezpečnosti informací je založen na modelu (cyklu) PDCA.

Model (cyklus) PDCA = Demingův model (cyklus)



Obrázek 2: Demingův model
Upraveno podle (2)

Na obrázku č. 2 je znázorněn koncept tohoto modelu, který poskytuje schematické vyjádření životního cyklu celého integrovaného systému řízení, nebo jeho komponenty, a zároveň zajišťuje i tzv. zpětnou vazbu. Jde o metodu postupného zlepšování, například kvality výrobků, služeb, procesů, aplikací či dat, probíhající formou opakovaného provádění čtyř základních činností. Součástí modelu je také dokumentace každé jeho etapy jako jedna z klíčových částí celého modelu. (2; 5, str. 85)

Jednotlivé etapy ISMS jsou obsahem norem ISO/IEC 27001 a ISO/IEC 27002. V následujících jednotlivých kapitolách bude vždy zmínka o tom, v jaké normě a její části se daná problematika nachází. (2)

Požadavky normy ISO/IEC 27001 jsou spojeny s naplněním modelu PDCA a všechny jsou závazné, protože společně vytvářejí úplný a smysluplný celek. Zajištění shody s touto normou je podmíněno splněním všech těchto závazných požadavků. (2; 5, str. 85)

Naproti tomu norma ISO/IEC 27002 je souborem postupů a je navržena jako soubor doporučení a jednotlivé požadavky závazné nejsou. (2; 5, str. 85)

1.2.1. Ustavení ISMS

Ustavení ISMS je první etapou, která upřesňuje správné formy řešení bezpečnosti informací. Definuje rozsah ISMS a odsouhlasení Prohlášení o politice ISMS patřící mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. První etapa by měla být ukončena souhlasem vedení se zavedením ISMS podle potřeb organizace, zjištěných při analýze a zvládání rizik ISMS. (2; 5, str. 86)

Ustavení ISMS je možné rozdělit do následujících činností: (2; 5, str. 86)

- určení rozsahu a hranice ISMS podle činností organizace a jejího organizačního uspořádání
- prohlášení o politice ISMS
- pravidla a postupy řízení rizik – součástí kapitoly je identifikace aktiv a rizik ISMS

- Souhlas vedení organizace s navrhovanými zbytkovými riziky, se zavedením ISMS a zpracování Prohlášení o aplikovatelnosti

Etapa „budování“ má zásadní dopady na fungování ISMS během jeho celého životního cyklu. (5, str. 86)

Určení rozsahu a hranice ISMS

Popis určení rozsahu a hranice ISMS podle činností organizace a jejího organizačního uspořádání je obsahem normy ISO/IEC 27001. Nachází se v kapitole 4.2.1 odstavci a. (2)

Prvním úkolem řízení bezpečnosti je určení rozsahu a hranic, ve kterých je ISMS uplatňován, neboť vždy nemusí pokrývat celou organizaci. (5, str. 87)

Z hlediska prosazení ISMS do organizace je možné ke stanovení rozsahu přistupovat dvěma základními způsoby: (5, str. 87)

1) rozsah ISMS je identický s rozsahem celé organizace
2) rozsah ISMS se implementuje na jasně definovanou část organizace

ad 1) V prvním případě spočívá výhoda v tom, že řízení od počátku řeší bezpečnost informací v celé organizaci. Tento přístup však vyžaduje poměrně významné investice z hlediska spotřeby zdrojů i financí, a ne vždy jsou realizovány všechny plánované a očekávané přínosy řízení bezpečnosti. Nalezneme mnoho případů, kdy velikost projektů bývá pro rozvoj společnosti spíše na škodu.

ad 2) Dalším řešením je ISMS implementovat na jasně definovanou část organizace, například na vybranou pobočku, určený organizační celek či informační systém. Nemusí se zde jednat o nejdůležitější část organizace. Lepší volbou je výběr části organizace, která je otevřená a ochotná zavádět smysluplné změny a zlepšení.

Toto řešení spočívá ve významné výhodě, neboť je možné se soustředit na vyšší míru úsilí do zvolené oblasti a v tomto vymezeném rozsahu zvládnout dva úkoly. (5, str. 87)

Prvním a nelehkým úkolem je objasnění účelnosti a potřebnosti zavedení ISMS do části či celé organizace. Neméně lehkým úkolem je pak důsledné zvládnutí všech požadavků ISMS při jejich praktickém prosazování. (5, str. 87)

Zavádění ISMS není o znalostech a schopnostech jednotlivce či omezené skupiny odborníků, ale o schopnosti společně sdílet nabyté znalosti a zkušenosti. Na jejich základě pak úspěšně rozvíjet řízení bezpečnosti pro všechny zúčastněné, včetně liniových manažerů i koncových uživatelů. (5, str. 87)

Rychlejší zavedení ISMS je možné a je vhodné realizovat tak, že zkrátíme dobu cyklu PDCA modelu. Jinými slovy znamená, že v daném období (např. 1 rok) necháme ISMS projít více PDCA cykly (např. dvěma či třemi). Významné urychlení spočívá v tom, že do realizace druhého či třetího PDCA cyklu již promítáme získané zkušenosti. Navíc se během realizace můžeme soustředit na podstatné menší okruhy a tím bude docházet i k lepšímu stanovení priorit dílčích PDCA cyklů. (5, str. 88)

Prohlášení o ISMS

Zpracování politiky ISMS je obsahem normy ISO/IEC 27001. Nalezneme tuto kapitolu 4.2.1 v odstavci b. (2)

Na základě specifických potřeb dané organizace vzniká definice Prohlášení o politice. Je důležité, aby z praktického hlediska politika ISMS: (5, str. 88)

- upřesnila cíle ISMS a definovala základní směr a rámec pro řízení bezpečnosti informací
- zohlednila požadavky, cíle organizace a související zákonné, regulativní a smluvní požadavky
- vytvořila potřebné vazby pro vybudování a údržbu ISMS v organizaci (například zohlednila její strategii, organizační strukturu, používané procesy, apod.)
- stanovila kritéria, podle nichž jsou popisována a hodnocena rizika
- byla vedením organizace schválena

Politika ISMS je důležitý dokument, protože prezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základ pro celý ISMS. Správně definovaná politika ISMS může značně usnadnit budoucí prosazování pravidel a požadavků na bezpečnost informací v organizaci. (5, str. 88)

Pravidla a postupy řízení rizik

Zpracování metodiky hodnocení rizik a určení kritérií pro akceptaci rizik je obsahem normy ISO/IEC 27001 kapitoly 4.2.1 odstavce c. (2)

Identifikace informačních aktiv, identifikace a hodnocení rizik ohrožení informačních aktiv je obsahem normy ISO/IEC 27001 kapitoly 4.2.1 odstavců d – g. (2)

Řízení rizik je pro systematické řízení bezpečnosti informací klíčovým nástrojem. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření. Tato opatření jsou schopna snížit negativní dopady skutečných rizik. Přesná znalost bezpečnostních rizik vede také k účinnému vynaložení úsilí při prosazování bezpečnostních opatření, které přinášejí větší efektivitu. Řízení rizik je základem ISMS, neboť podstatným způsobem ovlivňuje efektivitu celého jeho fungování. (5, str. 90)

Vztahy mezi jednotlivými termíny jsou znázorněny na obrázku č. 3:

Obrázek 3: Uspořádání terminologie řízení rizik
Upraveno podle (5, str. 90)

A) Teorie analýzy a řízení rizik

Analýza a řízení bezpečnostních rizik představují základní nástroj v rukou vrcholového vedení organizace. Vlastní provedení je možné rozlišit dle podrobnosti a hloubky přístupu k jejímu řešení: (5, str. 91)

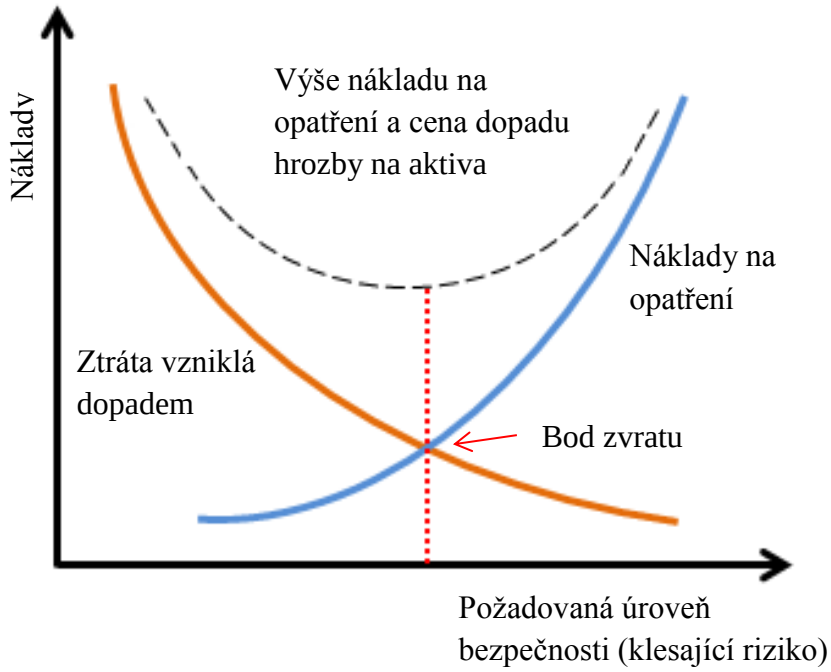
- nic nedělat
- neformální přístup (pragmatická analýza rizik)
- základní přístup
- detailní přístup
- kombinovaný přístup

První varianta „nedělat nic“ říká, že vrcholové vedení by mělo mít na vědomí, že s tímto rozhodnutím budou příslušná rizika plně akceptovat. Neznamená to, že v určitém časovém úseku není toto řešení nejefektivnější. S ohledem na význam informací a složitost IS je tento přístup vhodný pouze pro nově vzniklé společnosti, které ještě v počátcích svého působení nemají příliš co chránit. (5, str. 92)

Neformální přístup spočívá v analýze rizik, která se provádí živelně, bez dokumentace přesných postupů. (5, str. 92)

Základní přístup vyšel z poznatku, že řízení rizik není úplně jednoduchou disciplínou a proto se raději stanoví určité minimální požadavky, které budou vyhovovat většině obecných bezpečnostních potřeb. Od jisté hladiny základní úrovně se dostáváme do situace, kdy se jakýkoliv posun stává velmi nákladným. Je to dáno tím, že nejsme schopni se soustředit na nejslabší článek, ale prohloubení opatření musíme provádět plošně. V tomto okamžiku je pro další rozvoj bezpečnosti informací nezbytné využívat konceptu řízení rizik. Koncept nám dovolí rozpoznat slabší a silnější stránky systému a na jejich základě stanovit přesnější priority pro rozvoj bezpečnosti informací. Jde nám o to, abychom vždy nalezli právě ty nejslabší články, které budeme posilovat tak, aby míra bezpečnosti byla vyvážená a bezpečnost byla ekonomicky zvládnutelná. Ekonomický aspekt je v praxi realizován oceněním jednotlivých aktiv, která jsou východiskem pro stanovení maximálních nákladů na realizaci opatření na jejich ochranu. Na obrázku č. 4 jsou znázorněny vztahy mezi hodnotou aktiva (resp. mezi

ztrátou vzniklou v případě jeho zničení nebo poškození) a náklady na realizaci ochrany aktiva formou opatření. (5, str. 92-93)



Obrázek 4: Bod zvratu
Upraveno podle (2; 5. str. 93)

Detailní přístup udává všechna rizika, která jsou analyzována podrobně podle předem definované a dodržované metodiky. (5, str. 91)

Posledním řešením je přístup kombinovaný, kde jsou některá rizika analyzována podrobně a některá jsou případně při analýze i záměrně opomenuta. (5, str. 91)

Doporučuje se používat kombinace metod analýzy rizik neformální a detailní. Nejprve se však provede počáteční analýza rizik na hrubé úrovni pro všechny systémy IT. U systémů, které budou identifikovány jako významné pro činnost organizace, případně budou vystavené vysokým rizikům, provádíme analýzu podrobnou. (2)

B) Principy řízení rizik

Řízení rizik je komplexním oborem. Snaží se o identifikaci existujících rizik, o vyjádření úrovně jejich působení a o určení optimálních opatření pro snížení těchto rizik na přijatelnou úroveň. (5, str. 94)

Pro efektivní řízení rizik je důležité uplatnit následující principy: (5, str. 94)

- pravidelná aktualizace – na základě nových poznatků z monitorování systému řízení bezpečnosti nebo z externích zdrojů. Provádí se nejméně 1x za rok.
- zlepšení znalostí – proces zlepšování znalostí musí umět reagovat na změny jednak v organizaci a jednak v konceptech práce se znalostmi. Je nutné ukládat získané znalosti a průběžně je spravovat s cílem je sdílet pro další rozvoj systému řízení rizik.
- dokumentace – musí být úplná, splňovat požadavky na konzistenci a obsahovat mechanismy, které umožní určit či zjistit odpovědnosti za provedená rozhodnutí.
- odpovědnost za činnosti – musí být zavedena přímá odpovědnost funkčních útvarů a manažerů za koordinaci a integraci postupů v celé organizaci. Činnosti musí být prokazatelné.
- multidisciplinární přístup – multidisciplinární přístup vychází od mnoha uživatelů s různými názory a pohledy na význam rizika, jeho identifikaci, zvládání a také akceptaci.
- systematické a centralizované řízení – využívá standardizace, úplnosti přístupů, plánování, soudržnosti, využití zkušeností a zlepšování.
- integrovaný proces – potřeba provázat s procesy pro řízení informatiky, řízení bezpečnosti informací, řízení kontinuity organizace atd.

Řízení rizik pracuje s odhady možných dopadů, které mohou být méně či více přesné. Právě vyšší míra nepřesnosti informací o rizicích a vyšší úroveň dynamiky zvyšují význam řízení rizik na úkor tzv. analýzy rizik. (5, str. 94)

C) Nedostatky klasických metod řízení rizik

Klasické metody řízení zdůrazňují analytický charakter řízení. Prováděny jsou relativně složité analytické práce a jejich výsledkem je méně či více přesné vyjádření existujících bezpečnostních rizik. Následně dochází k návrhu vhodných bezpečnostních opatření. Ta mají za úkol existující rizika snížit nebo úplně eliminovat. (5, str. 94-95)

Mezi podstatné nedostatky se řadí relativně dlouhá doba mezi jednotlivými analýzami, která je v rozporu s potřebami zajistit flexibilní fungování informačních a komunikačních technologií. Mezi další nedostatky patří složité interní vazby, které se promítají do výpočtu rizik či do výběru bezpečnostních opatření. (5, str. 95)

Zvládání rizik je zde pojímáno, jako jednorázový akt. Pozornost metod se primárně věnuje detailní analýze rizik. Existují pouze omezené možnosti, jak integrovat do klasických metod řízení rizik externí zdroje informací (například zprávy z auditu, výsledky monitorování atd.) (5, str. 95)

D) Moderní přístupy k řízení rizik

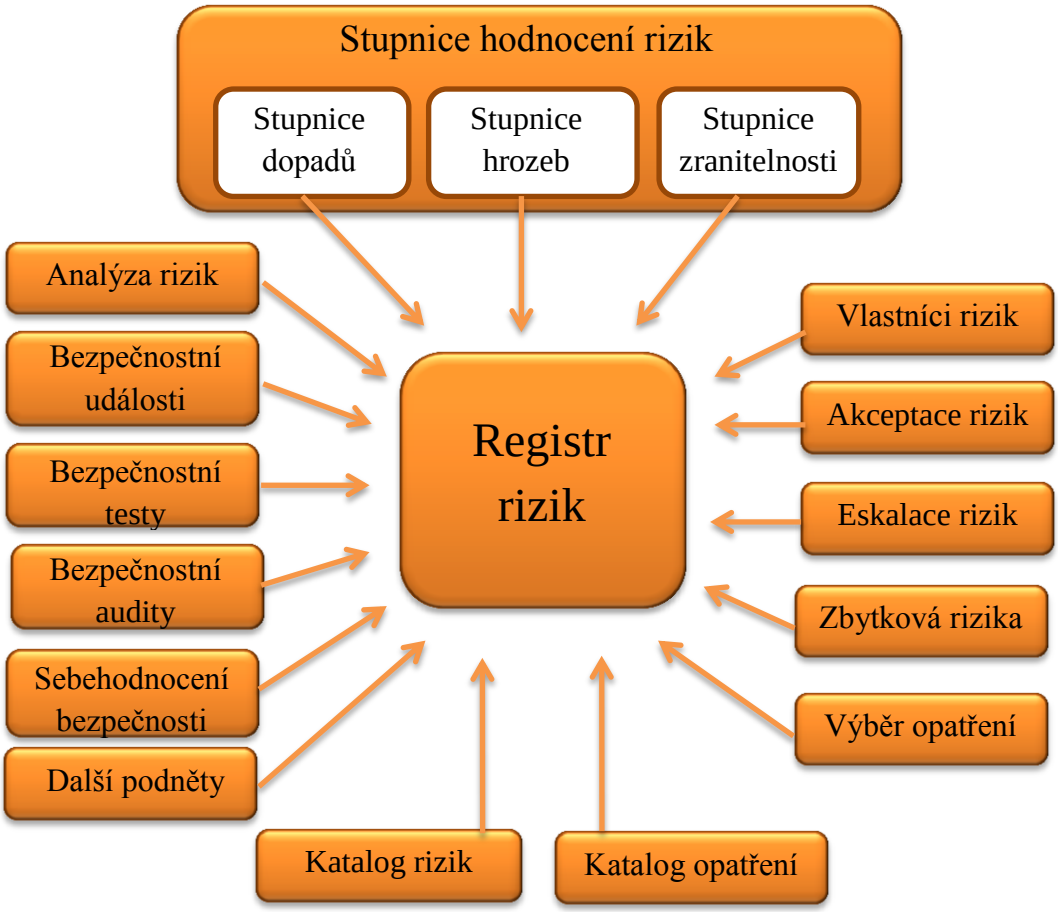
Se zvyšujícími se potřebami jsou rozvíjeny metody pro analýzu a zvládání rizik. Od dříve využívaných jednorázových analýz je snahou aplikovat analýzy při každodenním řízení bezpečnosti informací. Základním prvkem moderních přístupů je vybudování tzv. registru rizik, kam jsou ukládány informace o všech bezpečnostních rizicích a následné údržbě. Cílem je zjištěná rizika nejdříve identifikovat, následně ohodnotit, určit odpovědnost a sledovat postup zvládání rizika v čase. (5, str. 95)

Zmiňované moderní přístupy dovolují především neustále kontrolovat aktuální situaci kolem bezpečnostních rizik a rychle zpracovávat nově zjištěná rizika, což vede ke snadnějšímu prosazování a vyšší efektivitě. (5, str. 95)

Při aplikaci moderních metod řízení rizik je potřeba si ujasnit následující hlediska: (5, str. 96)

- **Jednoduché hodnocení rizik** – například doporučení organizace Bank Information Technology Secretariat. Riziko se počítá jednoduše jako prostý součin možných dopadů, pravděpodobnosti výskytů dopadů a pravděpodobné účinnosti provedených opatření.
- **Definice struktury pro řízení rizik** – snahou je jednoznačně určit odpovědnosti související s řízením rizik, definovat pravidla pro rozhodování, způsoby komunikace, způsoby vykazování atd. Cílem je provázat metodu řízení rizik s konkrétním prostředím informačních a komunikačních systémů.

- **Využití různých zdrojů vstupních informací** – zobrazení na obrázku č. 5 s názvem *Postavení registru rizik*. Cílem je připravit podmínky pro využití širokého spektra vstupních informačních zdrojů.



Obrázek 5 : Postavení registru rizik
Upraveno podle (5, str. 96)

Řízení rizik se zde neopírá pouze o náročné analytické postupy, ale mezi vstupy jsou zahrnuty i méně náročné zdroje informací. Dochází tak k těsnějšímu propojení metody řízení rizik s procesem řízení bezpečnosti informací. V případě moderního pojetí je vhodné využívat metody, které dovolují identifikovat a popsat bezpečnostní rizika, jež jsou specifická pro dané prostředí. Takovou metodou je například metoda FRAP (Faciliated Risk Analysis Process), jejíž snahou je otevřená komunikace mezi oběma stranami. Přispívá tak ke sblížení představ i zlepšení vzájemné výměny informací a často vede k odhalení doposud skrytých bezpečnostních rizik. (5, str. 96-97)

E) *Jak na účinné řízení rizik?*

Promítáme-li teoretické poznatky do praxe, musíme být obezřetní vůči některým doporučením. Musíme si v prvé řadě uvědomit, že popis rizik by měl pomoci při přijímání důležitých rozhodnutí a to i často nad rámec ISMS. (5, str. 97)

Aby tato rozhodnutí mohla být plněna odpovědně, řízení rizik by mělo splňovat tři zásady. Dodržování se osvědčuje v případech, kdy je řízení rizik v organizaci, nebo její části novinkou. Pro odborníky se mohou některá rizika omezení posunout. Vždy však na vrub srozumitelnosti výsledků. Níže zmiňované tři zásady vychází především z praktických zkušeností: (5, str. 97)

- **Rizikové scénáře by měly být voleny způsobem, aby byly pro danou organizaci jedinečnými.** Význam spočívá v tom, že není vhodné pracovat pouze s obecně definovanými hrozbami. Lepší srozumitelnost mají rizikové scénáře, neboť přesně vyjadřují konkrétní situaci organizace.
- **Rozsah rizikových scénářů, se kterými se pracuje, by měl být v desítkách rizik.** Na základě zkušeností lze konstatovat limit přibližně 35-50 rizik, či rizikových scénářů. Ideálním případem je práce s 20-30 riziky, nebo rizikovými scénáři. V případě přesahování počtu limitů je potřeba rizika strukturovat.
- **Vždy musíme okomentovat hodnoty, kterých jsme dosáhly při stanovení rizik.** Získáváme tak možnost ohodnocení rizik dále rozvíjet. Komentáře ukazují zkušenosti a jejich použití je nositelem úspěchu.

F) *Určení metody pro hodnocení rizik*

Cíl spočívá v rozhodnutí organizace nejen o samotné metodě pro hodnocení rizik. Je také nutné definovat potřebné stupnice pro vyjádření veličin potřebných pro řízení rizik. Nejdůležitější je definovat stupnice pro stanovení: (5, str. 98)

- míry integrity aktiv
- míry dostupnosti aktiv
- míry důvěrnosti aktiv
- míry škod a dopadů

- pravděpodobnosti uplatnění hrozby
- pravděpodobnost zranitelnosti
- stupnice pro vyjádření rizik a hladiny přijatelnosti rizika

Výše zmiňované míry pravděpodobnosti a stupnice nám dovolují určovat skutečnou výši hodnot jednotlivých parametrů rizik a usnadňují rozhodovací procesy související s řízením rizik. Metoda, kterou si stanovíme, by měla usnadňovat rozhodování při analýze, zvládání a hodnocení rizik. (5, str. 98)

G) *Ohodnocení aktiv ISMS*

Ohodnocení aktiv probíhá v několika základních krocích, které jsou následovné: (2)

1) identifikace aktiv – včetně jeho vlastníka
2) nástroje k ohodnocení aktiv – SW prostředky k ohodnocení aktiv (např.: metodika CRAMM)
3) stanovení stupnice a hodnotících kritérií, příkladem můžeme uvést:

Tabulka 1: Příklad stupnice a hodnotících kritérií aktiv
Upraveno podle (2)

Bezvýznamné riziko	Žádný dopad	1	
Akceptovatelné riziko	Zanedbatelný dopad	2	
Nízké riziko	Potíže a finanční ztráta	3	
Nežádoucí riziko	Vážné potíže a velká finanční ztráta	4	
Nepřijatelné riziko	Existenční potíže	5	

4) hodnocení nákladů v důsledku porušení (3 základní kritéria):
   - důvěrnost
   - integrita
   - dostupnost

Stanovené hodnoty nám slouží jako základ pro analýzu rizik. (2)

H) *Identifikace a analýza rizik ISMS*

Začínáme identifikací hrozeb, které mohou negativně ovlivnit skupinu aktiv. Pro rozšíření povědomí o těchto hrozbách je možné nalézt tyto hrozby v katalogu, který je veřejně dostupný např.: v ISO/IEC 27005 či BS 779-3. (5, str. 99)

Při práci s hrozbami se definují různé scénáře rizika. Tyto scénáře vyjadřují situace, které mohou nastat s tím, že jsou odhadovány možné dopady těchto situací, pravděpodobnost takové situace a pravděpodobnost, že existující bezpečnostní opatření jsou odolné vůči hrozbám. (5, str. 99)

S ohledem na hodnotu aktiva se určí výše dopadu a následná výše škody, kterou by hrozba mohla organizaci způsobit. Na základě obecných zkušeností se uplatní pravděpodobnost, s jakou by se mohl scénář uplatnit. Další a poslední proměnnou je míra zranitelnosti, kde se na základě existujících bezpečnostních opatření určuje míra jejich účinnosti vůči definovanému scénáři. Vyjádření všech hodnot spojených se scénářem rizika dovoluje jednoduché stanovení míry rizika daného scénáře. (5, str. 99)

Je možné na základě porovnání určit hlavní slabiny daného ISMS. To znamená, vyhledat nejrizikovější scénáře. (5, str. 99)

I) *Zvládání rizik ISMS*

Na základě zjištěných bezpečnostních potřeb a určení priorit je nyní nutné vybrat vhodná bezpečnostní opatření umožňující zjištěná rizika eliminovat. Pro zvládání rizik se nejčastěji používá katalog opatření. Katalog opatření je definovaný normou ISO/IEC 27002, nalezneme jej v 5. kapitole. Je možné doplňovat opatření i nad rámec těchto doporučení. (5, str. 100)

J) *Zpráva o hodnocení rizik*

Na závěr by měl být celý postup řízení rizik zdokumentován. (5, str. 100)

Souhlas vedení organizace s navrhovanými zbytkovými riziky, se zavedením ISMS a zpracování prohlášení o aplikovatelnosti

Zpracování prohlášení o aplikovatelnosti dle přílohy A normy ISO/IEC 27001 a jeho schválení vedením organizace je obsahem právě této normy. Nachází se v kapitole 4.2.1 v odstavcích h-j. (2)

Je zapotřebí, aby vedení organizace odsouhlasilo návrh bezpečnostních opatření. Tím by se vedení organizace mělo vyjádřit i k tomu, zda jsou existující zbytková rizika pro chod organizace přijatelná či nikoliv. (5, str. 100)

Dojde-li k tomu, že výsledky řízení rizik nepovedou k požadované úrovni bezpečnosti, dle požadavků vedení, je možné včas upravit návrh bezpečnostních opatření. (5, str. 100)

Souhlas vedení organizace se zbytkovými bezpečnostními riziky pak představuje souhlas s určitou mírou rizika při ochraně informací v organizaci. (5, str. 101)

Povinným dokumentem organizace je prohlášení o aplikovatelnosti popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná na ISMS organizace. Jinými slovy musí tento dokument obsahovat cíle opatření a jednotlivá bezpečnostní opatření, která byla pro daný ISMS vybrána na pokrytí existujících bezpečnostních rizik. Zmíněný dokument obsahuje i velmi důležitou zpětnou vazbu. Díky tomu jsme schopni jednoduše kontrolovat, zda došlo k pokrytí všech identifikovaných rizik příslušnými bezpečnostními opatřeními. (5, str. 101)

Zkušenost z tvorby prohlášení o aplikovatelnosti také ukazuje možnost využití tohoto dokumentu na systematický popis ISMS. Do prohlášení se v těchto případech doplňují informace a údaje, které jdou nad rámec požadavků normy. Velmi užitečné je do prohlášení o aplikovatelnosti doplnit i vazby na bezpečnostní dokumentaci. Jednoznačně identifikovat, ve které dokumentaci se daná opatření definují či řeší. (5, str. 102)

1.2.2. Zavádění a provoz ISMS

Zmíněná etapa životního cyklu ISMS se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v etapě Ustavení ISMS. Důležitou částí je příprava dílčích plánů. Zde se upřesňují termíny, zodpovědné osoby atd. Všechna bezpečnostní opatření by měla být zdokumentována v tzv. Příručce bezpečnosti informací, která slouží ke zdokumentování všech bezpečnostních opatření a k objasnění bezpečnostních principů všem uživatelům a manažerům. (2; 5, str. 104)

V normě ISO/IEC 27001 4.2.2 a, b, f, g nalezneme doporučení ke zpracování plánu zvládání rizik. (2)

Zpracování dokumentace postupů provádění opatření ISMS se nachází v normě ISO/IEC 27001, kapitole 4.2.2 a odstavcích c, d, e, h. (2)

Navržení záznamů k prokázání provozu ISMS doporučuje norma ISO/IEC 27001 v kapitole 4.3.3. (2)

Plán zvládání rizik

Plán zvládání rizik popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovené cíle a priority těchto činností ISMS, omezující faktory a potřebné zdroje. Tím se stává velice důležitým dokumentem. Podstatné je též určení osobní zodpovědnosti za jednotlivé naplánované činnosti. (5, str. 104)

Do plánu zvládání rizik je z praktického hlediska vhodné zapracovat činnosti, které vedou k potřebnému snižování bezpečnostních rizik. Tyto činnosti mohou být postiženy výčtem dílčích aktivit či množinou projektů, které souvisí se snižováním rizik. Do plánu je nepochybně vhodné také zapracovat požadavky, které jsou dány normou ISO/IEC 27001. (5, str. 105)

Při realizaci plánu by měly být shromažďovány podklady v podobě záznamů o těchto činnostech. (5, str. 105)

Příručka bezpečnosti informací

Při tvorbě bezpečnostní dokumentace je zapotřebí rozlišovat tři úrovně. (5, str. 105)

Na nejvyšší úrovni jsou především dokumenty, které si vyžaduje systém řízení bezpečnosti a které jsou s ohledem na požadavky ISMS povinné. Těmto dokumentům je často podřízena i jejich forma a mají své specifické místo. Za povinné požadavky můžeme považovat například rozsah a politiku ISMS, zprávu o hodnocení rizik, prohlášení o aplikovatelnosti a mnoho dalších. (5 , str. 105)

K podpoře prosazování ISMS slouží druhá úroveň dokumentace. Vždy by měla být přizpůsobena konkrétnímu ISMS. V tomto případě nejčastěji hovoříme o příručce bezpečnosti informací. Při tvorbě příručky je důležité vymezit dílčí procesy a postupy, které zajišťují efektivní prosazování jednotlivých bezpečnostních opatření. Je tedy podstatné definovat kdo, co, jak, kdy kde má chránit. (5, str. 105)

Nejnižší úroveň zaznamenává tzv. pracovní postupy. Pracovní postupy by měly podrobně vysvětlovat úkony k naplnění dílčích procesů. Tuto úroveň je možné řešit odkazem na příslušnou dokumentaci. (5, str. 105)

Prvotním cílem je předání dokumentace cílovým skupinám. Není však vhodné do jednoho dokumentu kombinovat více cílových skupin. (5, str. 105-106)

Prohlubování bezpečnostního povědomí

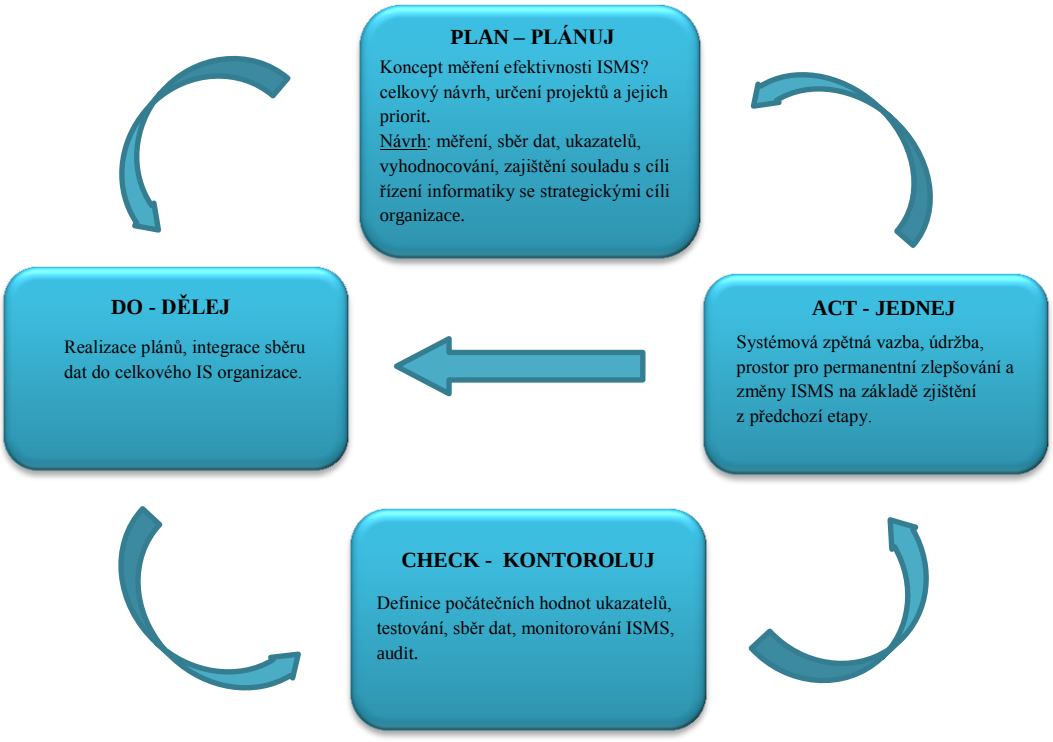
Prohlubování bezpečnostního povědomí je složitým úkolem a vyžaduje velkého úsilí. Za tímto pojmem se ukrývá promítnutí všech definovaných pravidel a postupů do skutečného chování všech zodpovědných uživatelů a manažerů. Tento proces je nekonečný, neboť neustále dochází k rozvoji systému bezpečnosti řízení informací. (5, str. 106)

Do podvědomí uživatelů je nezbytné se dostat, jinak nám nebudou platné ani nejmodernější systémy, dokud uživatelé nebudou ochotni přistoupit k bezpečnosti od základu, například dostatečně silným heslem, které nebude ležet na papíře u jejich počítače, či si nebudou sdělovat citlivé informace sobě navzájem. (5, str. 106)

Tyto situace je potřeba omezit. V nejlepším případě jim zamezit, a proto je nutné všem pracovníkům vysvětlovat bezpečnostní principy, pravidla a seznamovat je s bezpečnostními riziky, které mohou mít až existenční následky pro organizaci. Proto jsou organizována také školení, která se na tuto problematiku zaměřují. Nejslabším článkem v pomyslném řetězci ISMS vždy bude lidský činitel a jeho nepředvídatelné projevy. (5, str. 106)

Měření účinnosti ISMS

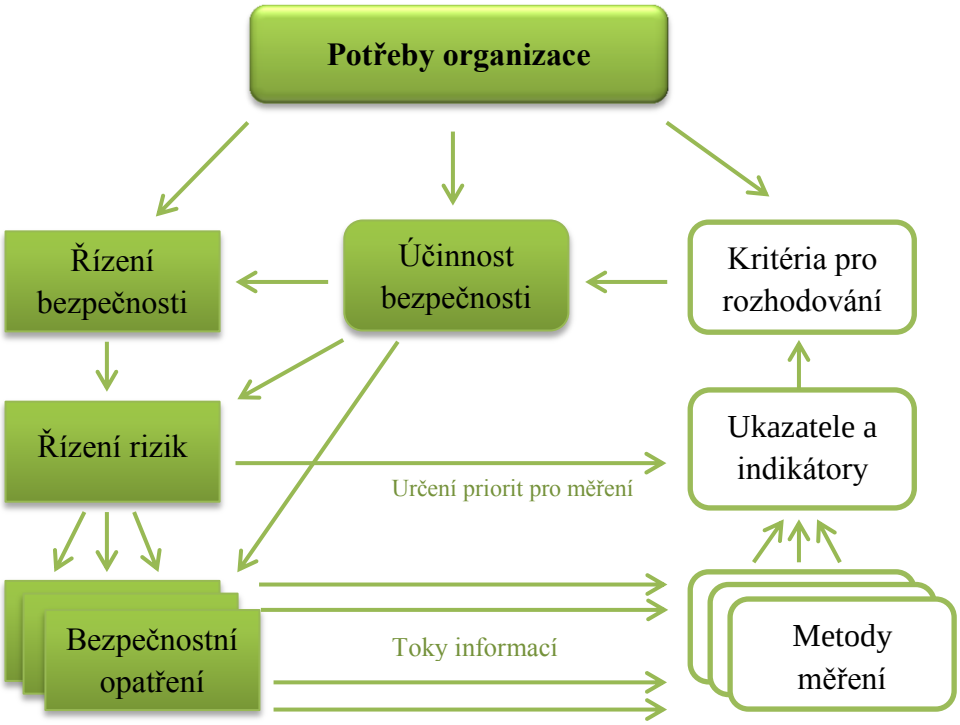
Prosazování efektivního řízení bezpečnosti je spojeno s měřením účinnosti aplikovaných bezpečnostních opatření. Je potřeba definovat a pravidelně sledovat objektivní údaje o skutečném fungování systému řízení bezpečnosti, na základě kterých je vhodné provádět všechna důležitá rozhodnutí. Tento proces není jednoduchý a je nutné jej mít na zřeteli již v okamžiku návrhu celého ISMS, neboť velmi podstatné kroky pro měření efektivnosti a jejího vyhodnocení jsou již součástí první etapy životního cyklu. Obrázek č. 6 znázorňuje, čemu se jednotlivé etapy životního cyklu věnují pro řízení účinnosti ISMS. (5, str. 106-107)



Obrázek 6: Použití modelu PDCA pro řízení účinnosti ISMS
Upraveno podle (5)

Účinnost bezpečnosti informací – rozsah bezpečnosti informací naplňující cíle organizace. Zda daný proces probíhá správně a zda opatření jsou správně implementována. (2)

K měření účinnosti bezpečnosti informací slouží metriky, které dělíme na implementační, výkonnostní a dopadové. (2)



Obrázek 7: Měření účinnosti ISMS a jeho zpětná vazba
Upraveno podle (5, str. 109)

Schéma fungování bezpečnostních ukazatelů účinnosti je znázorněno na obrázku č. 7. Popis obrázku č. 7 začněme od řízení rizik. Je základem nejen pro celé řízení bezpečnosti, ale také určuje priority pro její měření. Dále je zřejmé, že musí být nastaveny vhodné metody měření, které pomocí ukazatelů podporují rozhodovací proces. Vše s vazbou na strategické cíle organizace a její potřeby. (5, str. 109)

Problémem měření účinnosti je sestavení určitého konkrétního systému ukazatelů včetně stanovení jejich výchozích hodnot pro spuštění monitorovacího systému. Dále zajištění odpovídajícího sběru dat pro jejich pravidelné zjišťování.

Použití vybraných ukazatelů závisí především na konkrétních podmínkách organizací, na možnostech sběru dat, které jsou nezbytné pro jejich výpočty a vyhodnocování. Ve světové praxi můžeme naleznout mnoho doporučení a zkušeností. (5, str. 110)

Řízení provozu, zdrojů, dokumentace a záznamů ISMS

V této fázi nestačí pouze postupovat dle dohodnutých pravidel, ale je potřeba shromažďovat podklady, které jsou nezbytné pro další fázi, která se zabývá monitorováním. Je důležité vytvářet záznamy o jednotlivých provedených úkonech ISMS, ve kterých se objeví základní informace například o termínech, identifikaci, apod. (5, str. 116)

Z pohledu řízení zdrojů je nezbytné sledovat, zda jsou potřeby ISMS pokryty odpovídajícím množstvím odborných zdrojů, jako jsou lidské, finanční, technické atd. a efektivně řídit použití těchto zdrojů pro účinné fungování ISMS. (5, str. 116)

Provozním požadavkem je definice postupů a opatření. Je nutné využívat nástrojů, které jsou schopny odhalovat včas bezpečnostní slabiny a incidenty. Na tyto události pak upozornit příslušné pracovníky organizace. Tito pracovníci zajistí prošetření a zaznamenají průběh i výsledky šetření. (5, str. 117)

1.2.3. Monitorování a přezkoumání ISMS

Norma ISO/IEC 27991 4,2.3, 6 se zabývá zpracováním metodiky k provádění interních auditů a měření účinnosti opatření ISMS. (2)

Proškolení interních auditorů a provedení interního auditu ISMS nalezneme v normě ISO/IEC 27001 6, 8.2. (2)

Zpracování a přezkoumání ISMS vedením doporučuje norma ISO/IEC 27001 7.2, 7.3. (2)

Hlavním úkolem etapy zavádění ISMS je zajistit účinnou zpětnou vazbu. Mělo by proto dojít k prověření všech aplikovaných bezpečnostních opatření a jejich

důsledků na ISMS. Vlastní ověření začíná u přímé kontroly odpovědných osob, a to ze strany jejich nadřízených, či bezpečnostním manažerem. Důležité je také nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů. Cílem všech použitých zpětných vazeb je připravit dostatek podkladů o skutečném fungování ISMS a jejich následnému předložení za účelem přezkoumání. Během této části se provádí následující: (5, str. 117)

- monitorování a ověřování účinnosti prosazení bezpečnostních opatření
- provedení interních auditů
- příprava zprávy o stavu ISMS

Provádění kontrol ISMS

Základní zpětnou vazbou je provádění kontrol ze stran všech osob, které mají jakoukoliv odpovědnost za fungování ISMS. Tyto osoby by měly dohlížet na to, zda dochází ke splnění všech bezpečnostních požadavků a zda bezpečnostní opatření spadající do jejich kompetencí naplňují očekávání, která byla do nich vkládána při jejich zavádění. (5, str. 117)

Součástí kontrol je včasná detekce chyb, úspěšných i neúspěšných pokusů o narušení bezpečnosti, či schopnost sledování bezpečnostních událostí a včasné detekce bezpečnostních incidentů. Dále sem patří i vyhodnocení měření účinnosti ISMS a aplikovaných bezpečnostních opatření. Výsledky měření jsou podstatným podnětem pro další významnou kontrolní činnost. Takovou činností je na mysli přehodnocení výsledků ohodnocení rizik na základě zkušeností z praktického fungování ISMS. Tyto aktivity jsou promítány do aktualizace příslušných dokumentů a plánů. (5, str. 117)

Interní audity ISMS

Provádění interních auditů je kritickým prvkem zpětné vazby. Interní audity zajišťují nezávislý pohled na fungování ISMS a měly by svoje zaměření rovnoměrně rozložit na celý rozsah. Samozřejmě při zvážení cílů, priorit a rizikových oblastí ISMS.

Audity by měly prověřovat dva aspekty, které spolu úzce souvisí. Prvním z nich je dodržování pravidel a druhým aspektem auditu, je prověření fungování jednotlivých bezpečnostních opatření. (5, str. 118)

Přezkoumání ISMS vedením organizace

Při monitorování získáme podněty a připomínky, které jsou důležitými informacemi a slouží pro objektivní a účinné přezkoumání ISMS. Přezkoumání ISMS by mělo probíhat pravidelně, nejméně 1x za rok. Není ale výjimkou, když probíhá častěji. Bývá to především u nově zavedených ISMS, kde je potřeba častějšího přehodnocení. (5, str. 118)

Mezi vstupy pro přezkoumání ISMS patří všechny podstatné informace za hodnocené období. Hlavní pozornost by měla být věnována následujícímu: (5, str. 118-119)

- výsledkům provedených auditů ISMS
- zpětné vazbě od zainteresovaných uživatelů a třetích stran
- výsledkům měření účinnosti ISMS
- změnám, které ovlivňují ISMS
- existujícím slabinám a hrozbám, které mohly být při analýze rizik podceněny
- získaným doporučením pro další zlepšování ISMS

Na základě těchto podnětů dochází k posouzení slabých a silných stránek, což vyjadřuje SWOT analýza. K důležitým výstupům SWOT analýzy patří: (5, str. 119)

- zlepšení účinnosti ISMS
- aktualizace ohodnocení rizik a souvisejících plánů pro zvládání rizik
- plánovaná náročnost ISMS na zdroje (lidské, technologické, finanční, aj.)
- nezbytné úpravy procesů, pravidel a postupů

Díky zprávě o stavu ISMS, která by měla být orientována hlavně na budoucnost, je s vedením organizace možné uzavřít „dohodu“ o prohlubování bezpečnosti. ISMS zpráva dovoluje manažerům definovat cíle pro další období a žádat vedení organizace o přidělení příslušných zdrojů na naplnění cílů, které jsou ve zprávě uvedeny. (5, str. 119)

1.2.4. Údržba a zlepšování ISMS

Poslední etapou celého cyklu ISMS je jeho udržování a zlepšování. Tato fáze by měla přispívat ke sběru podnětů, zlepšování a k nápravě všech nedostatků (neshod), které se v ISMS vyskytují. (5, str. 119)

V průběhu této části je nezbytné: (5, str. 119)

- provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků
- zavádět identifikované možnosti zlepšení ISMS (především na základě přehodnocení vedením)

Soustavné zlepšování ISMS

Dokonalé systémy v praxi v podstatě neexistují. Proto je důležité do každého systému zapracovat zpětnou vazbu. Zpětná vazba by měla fungovat tak, že na jedné straně bude získávat podněty a na straně druhé odhalovat nedostatky, jejich příčiny a bude vhodným způsobem na tyto podněty reagovat. (5, str. 120)

Podstatným prvkem zlepšování je využití zpětné vazby. Je žádoucí, aby se zlepšování ISMS opíralo o zkušenosti. Nápady pocházející z praxe jsou nenahraditelné, a proto by jim měla být věnována velká pozornost. (5, str. 120)

U všech podnětů je potřebné vždy zvážit přímé i nepřímé dopady. Pro rozvoj ISMS je také potřebné motivovat pracovníky, aby sdíleli své zkušenosti s tímto spojené a otevřeně navrhovali, co je vhodné a žádoucí na chodu ISMS v organizaci zlepšit. (5, str. 120)

Odstraňování nedostatků ISMS

Pro odstraňování nedostatků ISMS jsou dvě formy opatření: (5, str. 120)

- opatření k nápravě – v tomto případě se již nedostatek projevil a je potřeba jej vhodným způsobem napravit.
- preventivní opatření – je proaktivní formou řešení nedostatků ISMS. Vychází z toho, že se zjištěný nedostatek ještě neprojevil, ale další odklad jeho řešení by mohl vést k tomu, že se v budoucnu nějaká negativní událost objeví a způsobí vážnější problémy.

K odstraňování nedostatků patří v prvé řadě objasnění příčin. Je důležité se podívat na souvislosti, aby se opatření realizovala tak, že se omezí možnosti opakování daného nedostatku. (5, str. 120-121)

Praktické zkušenosti ukazují, že často podceňovanou příčinou nedostatků je nedostatečná znalost požadavků, kterou ISMS vyžaduje. Nedostatečná znalost je však jako příčina uváděna jen výjimečně. Snad je to proto, že nikdo nechce přiznat svoje chyby. (5, str. 121)

1.3. Metodiky a knihovna ITIL

V této kapitole se budeme zabývat metodikami, které se kromě oblasti řízení bezpečnosti zabývají i dalšími aspekty řízení informatiky organizací. Metodika je podrobný popis celkové činnosti. V metodikách je uplatňován klasický PDCA cyklus. Dále zde bude popsána knihovna ITIL, poskytující ucelený soubor pro řízení služeb IT. (2; 5, str. 42)

1.3.1. Metodika COBIT

Vychází ze skutečnosti, aby podnik mohl dosahovat svých cílů, vznáší business požadavky, které generují požadavky na IT zdroje, jež jsou zapojeny do IT procesů přinášející businessu požadovanou službu a informace. (2)

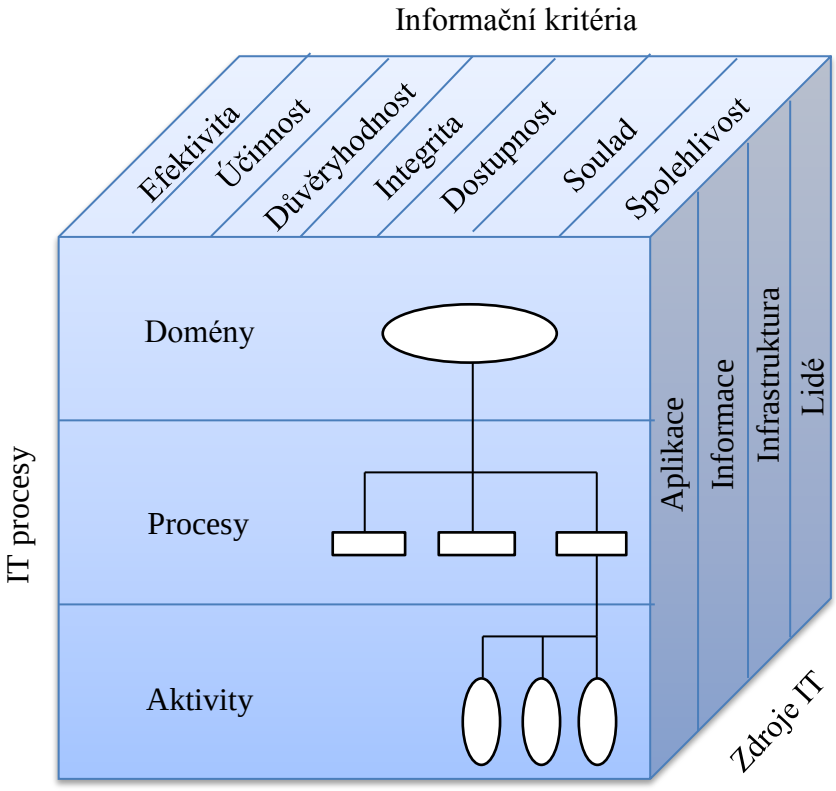
Je považována za soubor těch nejlepších praktik pro řízení informatiky, které by měly umožnit dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik. (2)

Cílem metodiky COBIT je propojení principů obecného řízení organizace s pravidly, která jsou uplatňována v prostředí IT. (2)

S touto metodikou se velice dobře pracuje a člověk se v ní rychle orientuje, neboť vše je vyvedeno v přehledné tabelární formě s pevně danou strukturou. (2)

PDCA cyklus pro metodiku COBIT: (2)

- PLAN – odpovídá plánování a organizaci
- DO – je zastoupena doménou Akvizice a implementace + Poskytování a podpora
- Fázím CHECK a ACT – odpovídá doména Monitorování a vyhodnocování



Obrázek 8: COBIT kostka
Upraveno podle (2; 5, str. 43)

COBIT je komplexnější než ITIL. Následující 3 komponenty využívá COBIT kostka, která je uvedena na obrázku č. 8 (2)

- informační kritéria (osa x)
- IT procesy (osa y)
- zdroje IT (osa z)

COBIT kostka přehledně znázorňuje vzájemné prolínání IT procesů, zdrojů informatiky a požadavků na informační kritéria. Ukazuje základní koncepci metodiky: zdroje informatiky jsou řízeny procesy tak, aby bylo dosaženo stanovených cílů, které odpovídají strategickým požadavkům. (5, str. 43)

Informační kritéria COBIT

Efektivita – požadavky na včasné doručování relevantních informací ve správném, konzistentním a použitelném tvaru (2)

Účinnost – požadavky na zpracování informací nejekonomičtějším a nejproduktivnějším způsobem prostřednictvím optimálního využívání zdrojů informatiky (2)

Důvěryhodnost – požadavky zahrnující ochrany důležitých informací proti neautorizovanému použití (prozrazení) (2)

Integrita – požadavky týkající se přesnosti a kompletnosti informace ve vztahu k požadavkům podnikání a jeho očekáváním (2)

Dostupnost – požadavky týkající se dostupnosti informace pro podnikání a týkající se také ochrany potřebných zdrojů (2)

Soulad – požadavky týkající se udržování souladu se zákony, směrnicemi, regulacemi a kontraktačními podmínkami, které se týkají procesů podnikání (hlavních podnikových procesů) (2)

Spolehlivost – požadavky vztahující se k přínosu informace pro rozhodování manažerů (2)

IT zdroje COBIT (aplikace, informace, infrastruktura a lidé)

Odpovídá obecnému členění aktiv na: (2)

- aktiva SW
- aktiva HW
- Data
- IT služby

IT procesy COBIT

Existují 4 základní domény: (2)

- plánování a organizace
- akvizice a implementace
- dodávka a podpora
- sledování a hodnocení

Procesy jsou spravovány v rámci každé domény. Procesů označovaných jako „High Level Control Objectives“ je 34. (2)

Aktivity neboli detailní kontrolní cíle tvoří každý proces. (2)

Struktura IT procesů vytváří v COBIT tzv. smyčku, která odpovídá základním prvkům životního cyklu informačních systémů. (2)

1.3.2. Metodika CRAMM

CRAMM metodika vznikla jako zkratka: CCTA Risk Analysis and Management Method. Je to metodika a soubor softwarových nástrojů pro zavádění a podporu systému řízení bezpečnosti informací pro provádění identifikace a ohodnocení aktiv, analýzy rizik informačních systémů a sítí. Slouží k návrhu bezpečnostních opatření, určování havarijních požadavků na IS a k návrhům na řešení havarijních situací. (2)

Tato metodika obsahuje velmi rozsáhlou databázi (knihovnu) opatření, která zahrnuje bezpečnostní opatření na pokrytí rizik. (2)

Rozlišujeme: (2)

- CRAMM Expert
- CRAMM Express

CRAMM Expert je detailní analýza, která se dělí na 3 fáze s následujícím cílem a obsahem: (2)

- fáze 1 – identifikace aktiv a vytvoření modelů aktiv, na základě interview s vybranými respondenty stanovení hodnoty aktiv (určení možných dopadů na provoz a cíle organizace při jejich ohrožení)
- fáze 2 – identifikace hrozeb a zranitelností systému a určení jejich úrovně, výpočet míry rizika
- fáze 3 – návrh opatření na pokrytí zjištěných rizik a identifikace jejich stavu, zpracování podkladů pro implementaci opatření doporučených k realizaci

Jestliže provádíme hodnocení rizik pomocí metodiky CRAMM Expert, je nutné detailně popsat celý systém, ohodnotit jednotlivá identifikovaná aktiva a následně hrozby a zranitelnosti. Tyto činnosti jsou vykonávány v rámci samostatného projektu, neboť množství informací je značné. Délka samostatného projektu se zpravidla počítá v jednotkách měsíců. (2)

CRAMM Express je analýza, která umožňuje provést analýzu rizik celého systému v průběhu několika hodin. Přitom zůstávají původní zásady metodiky nedotčeny. Ze tří kategorií se generují pouze opatření první. (2)

Postup: (2)

- zjištění hodnoty dat pomocí vodítek hodnocení
- rychlé hodnocení hrozeb a zranitelností
- stanovení míry rizika a výčet opatření

Expresní analýzu můžeme také použít jako rychlou variantu na začátku projektu. Snadno převedeme všechny informace do CRAMM Expert, abychom pokračovali v detailní analýze. (2)

CRAMM a výběr opatření

Základním výstupem 3. fáze expertní analýzy je výběr opatření. Zdrojem je databáze (knihovna) opatření, kde jsou tato bezpečnostní opatření rozdělena do 5 hlavních oblastí: (2)

- IT bezpečnost
- Komunikační bezpečnost
- Personální bezpečnost
- Administrativní bezpečnost
- Fyzická bezpečnost

1.3.3. Knihovna ITIL

ITIL poskytuje ucelený soubor pro řízení služeb IT (od roku 2007 platná V3). (2)

Celková koncepce je podřízena životnímu cyklu služeb IT ve formě: (2)

- strategie služeb – představuje propojení aktivit organizace se strategií v oblasti informatiky. Obsahuje definice služeb, typů poskytovatelů služeb a strategii návrhu, vývoje a poskytování služeb, strategii ITSM a plánování přidané hodnoty, IT Governance.
- návrh služeb – obsahuje včetně insourcingu, outsourcingu a sdílených služeb také návrhy služeb IT a architektury IS v organizaci v celém životním cyklu.
- implementace služeb – zahrnuje návody na implementaci služeb do reálného prostředí (například řízení změn, verzí, modely služeb, návrhy kontrol pro uvádění služeb do provozu atd.).
- provoz služeb – podpora správy služeb v produktivním prostředí, řešení poruch, problémů apod.

- průběžné zlepšování služeb – přispívá ke zlepšování zavedených existujících služeb.

ITIL (IT Infrastructure Library) nám dává doporučení co a kdy dělat nejen při provozu, ale i údržbě IT služeb. Neříká jak to dělat, ale říká co a kdy. Jedná se o Framework postavený na nejlepších zkušenostech z praxe. Je nezávislý na platformě, a protože je to „rámec“, jsou výstupy všech dodavatelů v celém odvětví kompatibilní a univerzálně použitelné (školení, SW nástroje i konzultační služby). Je detailní než COBIT. (2)

Pro ITIL je klíčový proaktivní přístup. Reaktivní pouze reaguje na události, jež nastaly, zatímco proaktivní se zabývá detekcí a řešením možných problémů, potřebných změn v ICT infrastruktuře, které by mohly v budoucnu vyvolat incidenty, či přinést problémy. (2)

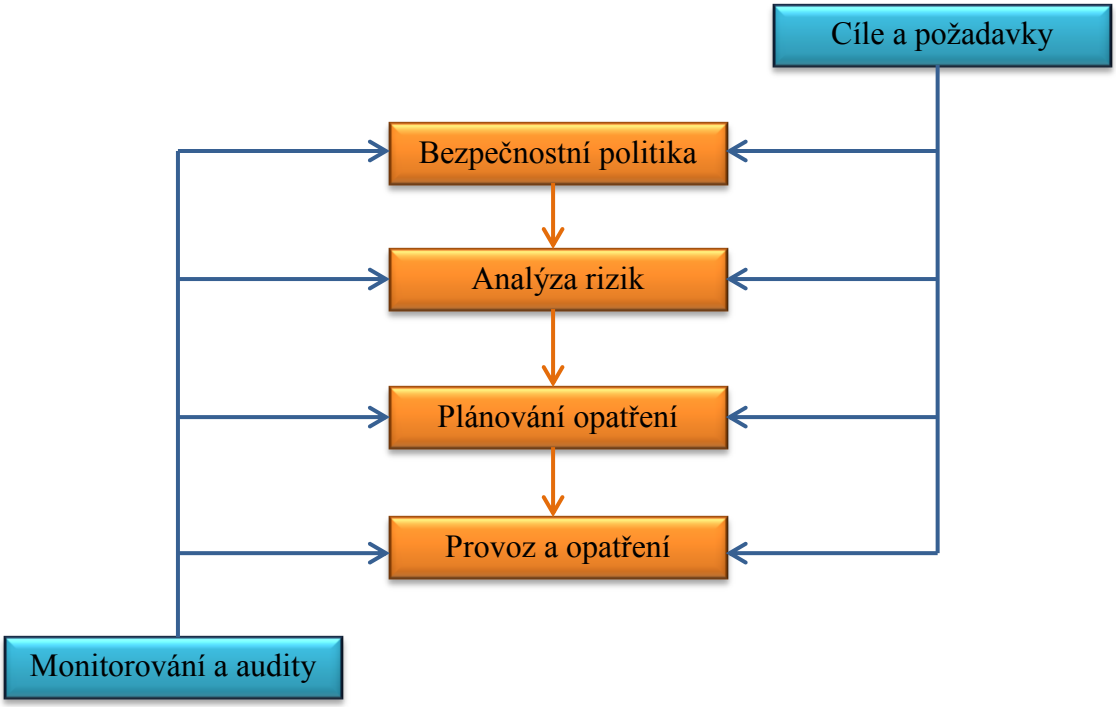
Obsahem ITIL je: (2)

- definování procesů potřebných pro zajištění ITSM
- zásady pro implementaci procesů ITSM

ITIL neřeší: (2)

- projektovou metodiku implementace ITSM
- konkrétní podobu organizační struktury
- podobu a obsah pracovních procedur
- způsob obsazení rolí konkrétními pracovními pozicemi

Základní procesy řízení bezpečnosti informací podle ITIL jsou zobrazeny na obrázku č. 9.



Obrázek 9: Základní procesy řízení bezpečnosti informací podle ITIL
Upraveno podle (2)

1.4. Certifikace systému řízení bezpečnosti informací

Cílem a smyslem certifikace je nezávislé posouzení systému řízení dané organizace nebo její části, s ohledem na požadavky, které jsou definované příslušnou certifikační normou. V případě systému řízení bezpečnosti informací je touto normou ISO/IEC 27001. (5, str. 179)

Certifikace versus akreditace

Certifikaci může provádět pouze oprávněná instituce, tzv. certifikační orgán, který byl pro tuto činnost akreditován. V tomto případě se akreditací rozumí prověření odborné úrovně a fungování certifikačního orgánu. (5, str. 179)

Certifikace potvrzuje shodu zavedeného, zlepšovaného a udržovaného systému řízení na základě plnění požadavků referenčních norem a specifikací. Proto se přesněji uvádí, že se jedná o Certifikaci shody. Certifikace systémů následně znamená zvýšení jejich důvěryhodnosti dodavatele výrobků či poskytovatele služeb. (5, str. 179)

Akreditace je postup pro potvrzení objektivity, nezávislosti a odborné způsobilosti subjektu pro vykonávání definovaných činností. Na tomto základě vydává prověřený orgán osvědčení o akreditaci. (5, str. 179)

Certifikační orgán ISMS je třetí strana. Hodnotí a certifikuje ISMS organizace s ohledem na vydané normy ISMS a další dokumenty, které jsou vyžadované systémem řízení. (5, str. 180)

Pro auditory a certifikační orgány platí velmi přísná pravidla, aby se zabránilo konfliktu zájmů. Zmíněná pravidla zakazují certifikačním orgánům poskytovat jakékoliv poradenství, které by vedlo ve prospěch certifikované organizace. Pokud certifikační orgány pořádají školení, musí být prováděna na obecné bázi. (5, str. 180)

Průběh certifikace ISMS

Průběh certifikace probíhá v po sobě jdoucích několika krocích.

Prvním krokem je potřeba zajistit obchodní vztah mezi certifikačním orgánem i danou organizací. Na organizaci je, aby si zvolila certifikační orgán, který jí nejvíce vyhovuje. Při utváření tohoto vztahu je potřeba respektovat pravidla a postupovat podle nich tak, jak je certifikační orgán definuje. Součástí bývá i vyplnění dotazníku, pomocí něhož certifikační orgán stanoví potřebný rozsah certifikačního auditu. Před provedením vlastního certifikačního auditu se může organizace dohodnout na provedení tzv. předcertifikačního auditu, který slouží k provedení nanečisto. V tomto případě se postupuje podle certifikačních pravidel, ale zjištění auditorů jsou nezávazná a slouží organizaci jako podněty ke zlepšování ISMS. Provedení předauditu nejsou povinná, ale jsou často žádaná. Dochází zde ke vzájemnému poznání organizace, která se uchází o certifikaci. (5, str. 181)

Druhým krokem je vlastní certifikace, což je provedení certifikačního auditu, který se skládá ze dvou fází.

V první fázi je hlavním cílem posouzení dokumentace konkrétního ISMS, zda plně odpovídá požadavkům certifikační normy. V tomto případě to je ISO/IEC 27001. Do jisté míry můžeme první fázi považovat za posouzení fáze plánování v rámci PDCA cyklu modelu ISMS. Tým certifikačních auditorů se zároveň seznamuje s organizací a připravuje si plán pro druhou fázi auditu. (5, str. 181)

Druhá fáze je rozhodující, neboť certifikační auditoři se věnují nalezení shody mezi definovanými požadavky normy, vyjádřenými především dokumentací organizace a schopností organizace všechny tyto požadavky, při zachování vlastní funkčnosti dodržet. Základem bývá předložení potřebných dokladů a věrohodných důkazů, že definované požadavky jsou skutečně v praxi prosazeny a splňovány. Výstupem druhé fáze je doporučení auditního týmu, zda by měl být daný ISMS certifikován či nikoliv. (5, str. 181)

O vlastní certifikaci pak rozhoduje nezávislá osoba (nejčastěji se jedná o tzv. certifikační radu). V případě, že rada rozhodne o vydání příslušného certifikátu, je doba platnosti 3 roky. (5, str. 181-182)

Údržba a obnova certifikátu

Certifikační orgán musí po vydání certifikátu provádět pravidelné dozorové audity, které musí být prováděny nejméně s ročním intervalem. V případě zjištěných nedostatků mohou auditoři doporučit pozastavení či ukončení platnosti vydaného certifikátu. Za každé 3 roky se musí provést tzv. recertifikace. To znamená, že musí proběhnout rozsáhlejší audit, který postihne celý rozsah ISMS. Šíře recertifikačního auditu je srovnatelná s druhou fází. (5, str. 182)

1.5. Přínosy zavedení a certifikace ISMS

Zavedení systému řízení informační bezpečnosti může organizaci pomoci řešit problémy týkající se bezpečnosti ICT. Je přímou cestou jak k dosažení stanovené úrovně bezpečnosti informačních technologií, tak k účinnému a efektivnímu nakládání s informacemi v rámci celé organizace. (6, str. 103)

ISMS představuje dokumentovaný systém řízení, který se stává nedílnou součástí všech procesů organizace, neboť v sobě zahrnuje management, politiku, organizaci a pravidelné přezkoumávání. (6, str. 103)

ISMS začínají využívat všechny organizace bez ohledu na svoji velikost či obor, pro něž jsou informace a informační technologie klíčovou součástí všech procesů, nebo které spravují citlivá data svých klientů. Zároveň mají potřebu efektivně a komplexně zajistit jejich bezpečnost. Jeho zavedení se stává strategickým rozhodnutím vedením organizace. (6, str. 103)

Přínosy jsou následující: (6, str. 104)

- stanovení cílů a požadavků na kontinuální zlepšování zaručuje dlouhodobě efektivní řízení nákladů
- bezpečnost informací se stane integrální částí celého systému řízení organizace
- stanovení bezpečnostní strategie a odpovědností
- přechod k bezpečnosti řízené a komplexní (od nesystémového a neuceleného bezpečnosti informací)
- efektivní řízení investic vkládaných do bezpečnosti
- přehled a inventura vlastních aktiv, klasifikace a jejich ocenění
- identifikace hrozeb v oblasti bezpečnosti informací, eliminace anebo snížení rizik v této oblasti
- snížení nebo řízené odstranění rizik v oblasti IS
- zvýšení povědomí a odpovědnosti zaměstnanců
- zavedení systémového a systematického přístupu při používání IT/IS
- naplnění legislativních požadavků
- trvalé monitorování a zlepšování ISMS
- zvýšení důvěryhodnosti organizace
- konkurenční výhoda, kultivace image a firemní kultury organizace
- snížení rizik souvisejících s nedostupností informací a služeb, únikem nebo neoprávněným přístupem k informacím
- stanovení optimálního poměru mezi investicemi do bezpečnosti a dosaženou úrovní zabezpečení informačních aktiv organizace

- vypracování dokumentace pro ISMS
- zavedení systému průběžného sledování a hodnocení aktuálně dosažené úrovně informační bezpečnosti
- identifikace a vynucení dodržování legislativních a smluvních požadavků
- soulad s legislativními a právními předpisy
- ochrana zaměstnanců před trestní odpovědností podle § 180 trestního zákoníku č. 40/2009 Sb. ze dne 8. ledna 2009
- úspora nákladů souvisejících s odstraňováním následků bezpečnostních incidentů
- organizací veřejné správy řeší požadavky implementace IS veřejné správy podle zák. č. 365/2000 Sb., resp. 517/2002 Sb.
- vyhledávání slabých míst organizace, optimální rozložení nákladů na zvýšení bezpečnosti informací a jejich minimalizace

Při činnostech, jako zvládnutí stále většího množství zpracovávaných informací, automatizace jejich zpracování, globalizace i rostoucí objem výměny informací, vliv nových vyhlášek a zákonů, je nutné: (6, str. 105)

- zajistit včasnou dostupnost
- zamezit nechtěné modifikaci
- zabránit zneužití
- vyloučit možnost ztráty

Zaměstnanci odpovídají za bezpečnost informací svých pracovišť i zákazníků. (6, str. 105)

1.6. Organizace zabývající se bezpečností informací

Celosvětové (nadnárodní) normativní organizace

ISO (International Organization for Standardization) – zabývá se tvorbou, aktualizací a harmonizací mezinárodních norem ISO a jiných druhů dokumentů.

Do dokumentů řadíme například: TS – technické specifikace, TR – technické zprávy, TTA – dohody o technických trendech apod. (5, str. 224)

IEC (International Electrotechnical Comission) – připravuje a vydává mezinárodní normy z oblasti elektronických, elektrotechnických a jim příbuzných (elektřina, magnetismus, telekomunikace, multimédia, elektromagnetismus, elektroakustika, výroba a distribuce energií, terminologie, měření, navrhování a také bezpečnost). (2)

ITU (International Telecommunications Union) – spadá do hierarchie OSN. Normalizační aktivity ITU nyní obrací svůj zájem na stavební prvky objevující se v globální informační infrastruktuře a k tvorbě vyspělých multimediálních systémů, které využívají slučování hlasových, datových, zvukových a video signálů. (2)

Evropské normativní organizace

CEN (Comité Européen Normalisation) – CEN v současnosti přispívá k dosažení cílů Evropské unie při vybudování evropského ekonomického prostoru. Cílem je tvorba technických norem, které podporují volný obchod, bezpečnost zákazníků a pracovníků, interoperabilitu sítí, ochranu životního prostředí a rozšiřování vědeckých a výzkumných programů. (2; 5, str. 221)

CENELEC (Comité Européen de Normalisation Eléctrotechnique) – v nedávné době založila sektor ICT, kam přesunula normalizační aktivity související s oblastí informačních a komunikačních technologií. (2)

ETSI (European Telecommunications Standards Institute) – institut telekomunikačních norem. Vytváří globálně použitelné normy pro oblasti informačních a komunikačních technologií včetně pevných, mobilních, rádiových, internetových a konvergentních technologií. (5, str. 221)

Národní normativní organizace: (2)

- ANSI (American National Standards Institute)
- BSI (British Standard Institute)
- DIN (Deutches Institut für Normung)

– ČSNI (Český normalizační institut) – zřízen jako státní příspěvková organizace. V současné době patří mezi organizace podřízené Ministerstvu průmyslu a obchodu.

1.7. Řada norem ISO/IEC 27000

V poslední době je snahou harmonizovat přístupy a vzájemně provázat vydávané normy. Pokusy o vyšší míru harmonizace začaly přinášet hmatatelné výsledky. Nejvíce je to patrné v přístupu k normám, které definují pravidla pro systémy řízení bezpečnosti informací. Na jaře roku 2005 organizace ISO ohlásila zavedení nové řady norem ISO 27000, které vychází z modelu PDCA. (5, str. 78)

- ISO/IEC 27000 – základy (přehled) a slovník
- ISO/IEC 27001 – požadavky
- ISO/IEC 27002 – soubor postupů
- ISO/IEC 27003 – návod pro implementaci
- ISO/IEC 27004 – metriky a měření účinnosti opatření
- ISO/IEC 27005 – management rizik
- ISO/IEC 27006 – požadavky na místa provádějící audit a certifikaci
- ISO/IEC 27007 – směrnice pro audit
- ISO/IEC 27008 – doporučení auditorům ISMS (2)

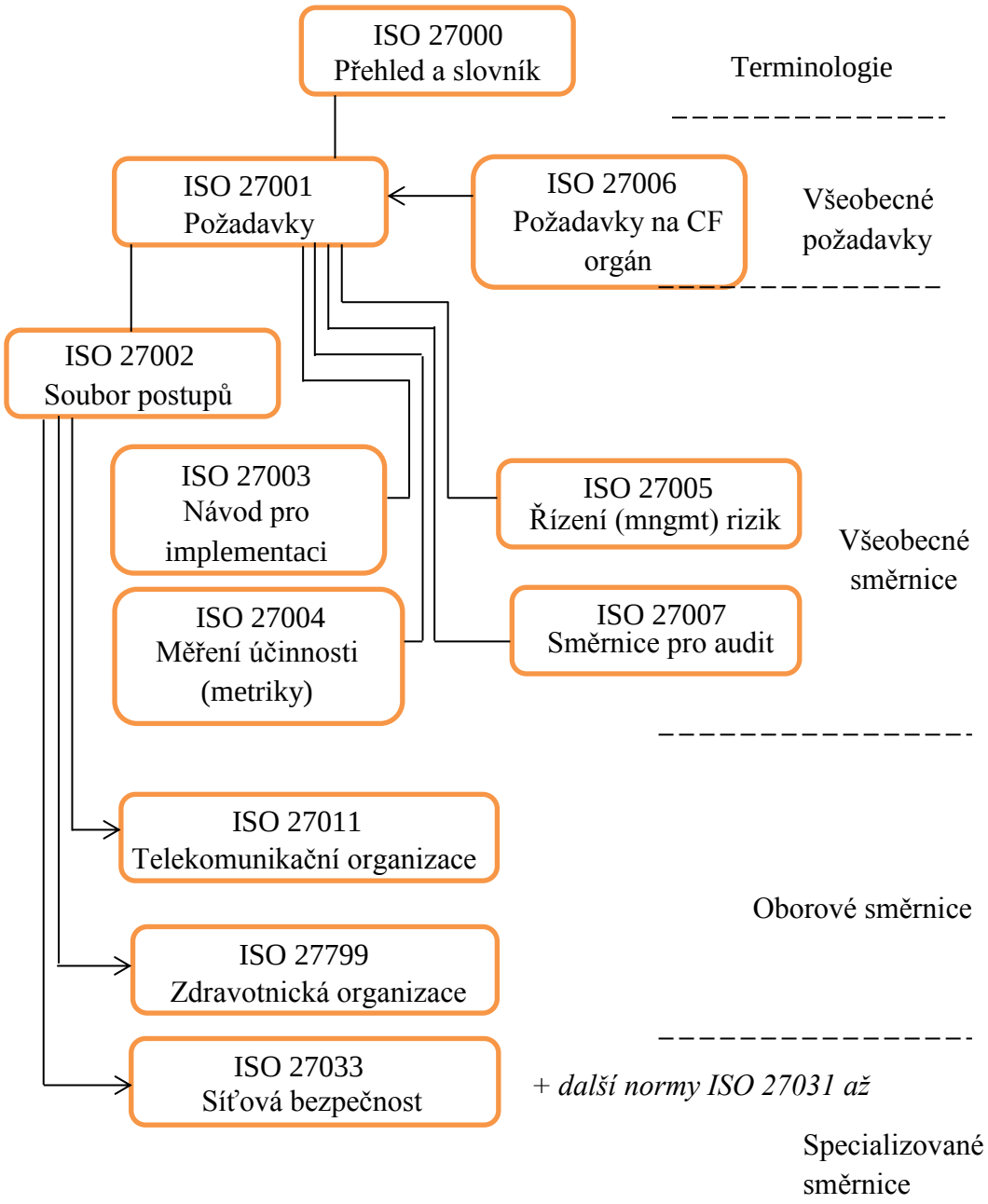
Požadavky a doporučení základních norem jsou další skupinou norem řady 27000 rozšiřovány, podle potřeb a specifických podmínek, v různých odvětvích lidských činností. Jedná se o následující normy: (5, str. 81)

- ISO/IEC 27010 – řízení bezpečnosti informací pro komunikace mezi organizacemi
- ISO/IEC 27011:2008 – směrnice řízení bezpečnosti informací pro telekomunikace
- ISO/IEC 27799:2008 – systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

- ISO/IEC 27013 – směrnice pro společné nasazení ISO/IEC 20000-1 a ISO/IEC 27001
- ISO/IEC 27014 – rámec pro governance bezpečnosti informací
- ISO/IEC 27015 – směrnice řízení bezpečnosti informací pro finanční služby (vydání plánováno na rok 2013)
- ISO/IEC TR 27016 – řízení bezpečnosti informací – organizační ekonomika organizací (vydání plánováno na rok 2013)

Do řady ISO/IEC 27000 jsou zařazovány normy, které se snaží upřesnit doporučení a doplnit podstatné informace pro různé oblasti řízení bezpečnosti informací. Do této skupiny patří normy: (5, str. 82)

- ISO/IEC 27031:2011 – specifikace pro připravenost ICT na kontinuitu organizace
- ISO/IEC 27032 – směrnice pro kybernetickou bezpečnost
- ISO/IEC 27033 – bezpečnost sítí IT (vydání v letech 2009-2013)
- ISO/IEC 27034 – bezpečnost aplikací (vydání plánováno v letech 2011-2014)
- ISO/IEC 27035:2011 – řízení incidentů bezpečnosti informací
- ISO/IEC 27036 – bezpečnost informací pro dodavatelské vztahy (vydání plánováno na rok 2013)
- ISO/IEC 27037 – směrnice pro určování, sbírání nebo získávání a ochranu digitálních důkazů
- ISO/IEC 27038 – směrnice pro vedení digitálních záznamů (vydání plánováno na rok 2013)
- ISO/IEC 27039 – výběr, nasazení a provoz systémů pro detekci a prevenci průniku (vydání plánováno na rok 2013)
- ISO/IEC 27040 – bezpečnost uložení dat (vydání plánováno na rok 2014)



Obrázek 10: Přehled norem ISO 27000
Upraveno podle (2)

1.8. Fyzická bezpečnost a bezpečnost prostředí

Oblasti fyzické bezpečnosti a bezpečnosti prostředí tvoří skupiny: zabezpečené oblasti a bezpečnost prostředí. Zabezpečené oblasti se snaží chránit prostředí organizace jako celek. Naproti tomu bezpečnost zařízení obsahuje opatření, která chrání jednotlivé

prvky infrastruktury ICT. Pouze náležitou kombinací opatření z obou skupin dosáhneme pro organizaci efektivních výsledků.(5, str. 141)

Pro ochranu zabezpečených oblastí je určeno 6 bezpečnostních opatření: (5, str. 141)

- *fyzický bezpečnostní perimetr* – definován zdmi, ploty, mřížemi, signalizací vniknutí či pohybu atd.
- *kontrola fyzického vstupu* – cílem je sledovat osoby, které se v zabezpečeném prostoru pohybují. Součástí je například označení osob, identifikace a doprovázení návštěv apod.
- *zabezpečení místností a prostředků* – tam, kde je potřeba zvláštní ochrana kanceláří, místností a prostředků, ve kterých se nachází citlivé informace nebo jsou kritické s ohledem na fungování organizace.
- *vnější hrozby a vliv prostředí* – za tyto hrozby považujeme například požár, vodu, prach, výbuchy, zemětřesení atd.
- *práce v zabezpečených oblastech* – pro osoby pracující v těchto zabezpečených oblastech je žádoucí určit pravidla. Mělo by pro ně platit omezení pohybu na nezbytně nutnou dobu. Nezbytností je zákaz práce bez dohledu a používání v těchto prostorech různá záznamová zařízení.
- *veřejný přístup* – veřejné prostory by měly být kontrolovány recepcí, která zajistí doprovod návštěv. Prostory pro vykládku a nakládku by měly zajistit přinejmenším provedení vizuální kontroly příchozího materiálu. Ideálním řešením je vybalení všech zásilek v určeném prostoru a jejich další distribuce bez obalů a podobného materiálu. Tím se snižuje riziko, že by se do kritických prostor mohl dostat nežádoucí materiál. U těchto prostor je samozřejmostí omezit prostor na určené osoby.

Bezpečnost zařízení se opírá o následující bezpečnostní opatření: (5, str. 141)

- *umístění zařízení v odpovídajícím prostředí* – doporučuje umísťovat zařízení tak, aby byla zajištěna fyzická bezpečnost. Snahou je minimalizovat fyzický přístup k nim, také omezit možnosti neoprávněného sledování informací na monitoru či zajištění odpovídajících bezpečných provozních podmínek.

- *dodávky energie* – opatření věnující se ochraně podpůrných zařízení (např.: UPS). Některá zařízení mohou být závislá na dodávce chladícího média, jako je například voda.
- *údržba a zařízení* – pro prohloubení spolehlivosti.
- *mazání a likvidace paměťových médií* – důležité, aby na paměťových nosičích nezůstávala uchována data i po jejich vyřazení. Pro spolehlivé smazání dat v podstatě existují 3 metody:
    - *mazání dat pomocí speciálních nástrojů*
    - *mazání elektromagnetickým impulzem*
    - *fyzická likvidace (mechanicky, požárem, atd.)*

1.9. Fáze řešení bezpečnosti IS

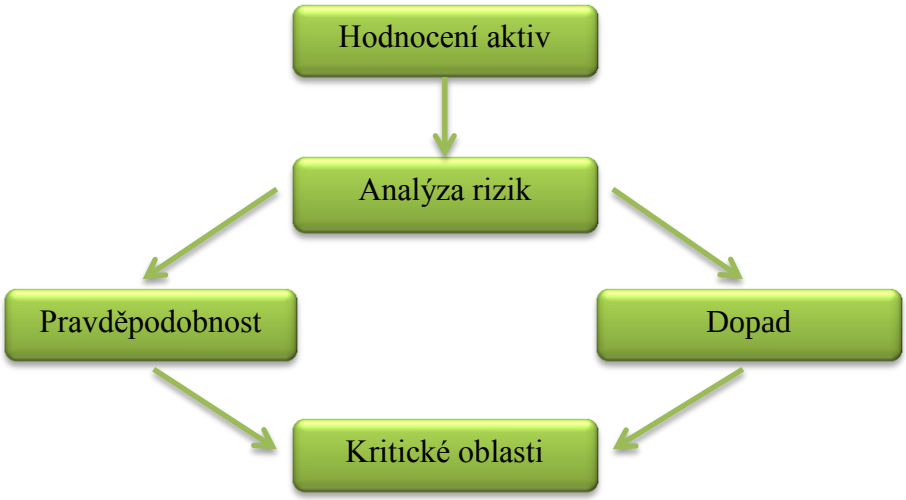
V této kapitole bude vysvětlen termín bezpečnostní politiky, dále se podíváme na její obsah, druhy a typy, základní principy, výhody a přínosy, které přináší a zároveň na problematiku a nedostatky při její realizaci. Důležitou součástí procesu je identifikace, analýza, vyhodnocení rizik a jejich dopadů. K tomu nám slouží analýza rizik. Existuje několik přístupů, ale také i problémů a chyb, které se při analýze rizik mohou vyskytnout. Konkrétní požadavky v konkrétních oblastech pak představuje bezpečnostní projekt, z něhož plynou dva výstupy. Závěrem je potřeba se zmínit o udržování a zlepšování, které slouží ke zlepšení nedostatků.

1.9.1. Analýza rizik

S rizikem je spojená každá aktivita organizace a toto riziko je definováno jako nebezpečí, že určitá událost nebo akce negativně ovlivní schopnost organizace dosahovat svých cílů a naplnit svoji strategii. Míra rizika je dána pravděpodobností a velikostí negativního dopadu, s jakou riziko nastane. (7, str. 68)

Aby organizace přežila, musí určitá rizika přijmout a do jisté míry řídit. Analýzu rizik provádíme, abychom zjistili jaká rizika, a hrozby naši organizaci ohrožují. Cílem analýzy rizik je rizika identifikovat a kvantifikovat. Tím budeme moci rozhodnout, zda je přijmeme či nikoliv. (7, str. 68)

Na základě analýzy budeme schopni rozhodovat, které kontrolní mechanismy jsou nezbytné a které naopak nadbytečné. Vzhledem k neustálému vývoji IS je potřeba analýzy rizik aktualizovat. Většinou se aktualizují její jednotlivé části při každé významné změně IS, nebo při zjištění nové hrozby. Naopak celková analýza rizik by měla být aktualizována podle velikosti organizace a její závislosti na informačních technologiích. (7, str. 68-69)

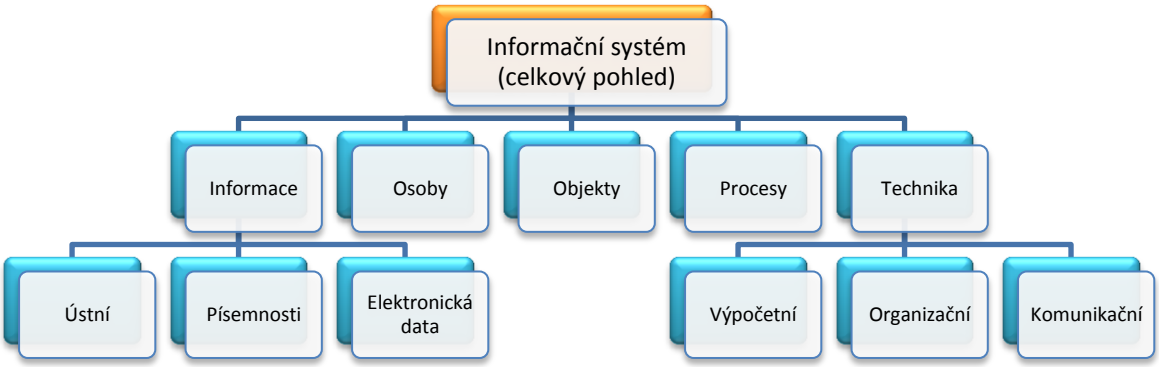


Obrázek 11: Analýza rizik
Upraveno podle (7, str. 68)

Analýza rizik je klíčovou aktivitou v procesu řešení bezpečnosti. Musí poskytnout odpovědi na následující otázky: (7, str. 69)

- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?
- Co se stane, když nebudou informace chráněny?

Typickým výstupem je dokument obsahující popis systému a výsledky analýzy, zjištěné zranitelnosti, úroveň hrozeb, úroveň stávajících ochranných opatření a distribuce výsledných rizik. Obrázek č. 12 znázorňuje možný rozsah analýzy rizik. (7, str. 69)



Obrázek 12: Rozsah analýzy rizik
Upraveno podle (7, str. 69)

Poněvadž je provedení podrobné analýzy pro rozsáhlé IS časově velmi náročné a protože informační rizika, která hrozí některým organizacím, nejsou až tak vysoká, aby provedení analýzy rizik vyžadovala, existuje několik přístupů, které jsou uvedeny v kapitole 1.2.1., v pravidlech a postupech řízní rizik. (7, str. 69)

Analýza rizik je důležitou a náročnou součástí procesu řešení. Řada organizací se na tuto činnost specializuje. Mají své ověřené postupy a užívají různé softwarové nástroje a metodiky jako je například CRAMM. Výsledky těchto analýz jsou velice citlivým dokumentem, neboť obsahují podrobné informace o kritických místech v organizaci. (7, str. 70)

V procesu řízení rizik je analýza rizik naprosto klíčovým krokem. Jedná se o komplexní proces, který je schopen sehrát klíčovou roli v budoucím období existence organizace. Z tohoto důvodu je vhodné uvést některé problémy a chyby, které se při analýze rizik mohou vyskytnout. Jedná se o níže uvedené problémy: (7, str. 70)

- **Plošné zavádění ochranných opatření** – Analýza rizik není prováděna a ochranná opatření jsou zaváděna dle některého standardu. Tento postup nezaručí dostatečnou ochranu informačního systému společnosti a navíc vede k nadměrným výdajům.
- **Malé využití analýzy rizik** – Provádí se analýza rizik. Výsledky zde nejsou použity při klasifikaci dat, bezpečnostních standardů ani tvorbě bezpečnostní

politiky. Do implementace všech opatření není zaručena dostatečná ochrana IS společnosti.

- **Neúplná analýza rizik** – V tomto případě se zahájí detailní analýza rizik, ale nedokončí se. Jestliže k tomuto dojde, je nezbytné, aby se zbytek systému podrobil alespoň základní či neformální analýze.
- **Analýza rizik není aktualizována** – Je provedena podrobná analýza rizik. Tento stav není udržován ani aktualizován. Problém spočívá v tom, že investice byly využity neefektivně. Při potřebě aktualizací se bude muset postupovat znovu od začátku.
- **Subjektivní výběr protiopatření** – Protiopatření vybírá správce sítě bez jakéhokoliv vztahu k analýze rizik. Protiopatření jsou vybírána na základě jeho znalostí a preferencí. Plynou z toho závažná rizika, neboť společnost může vynakládat vysoké částky a i přes to nebudou rizika pokrývána podle své důležitosti a současně řada klíčových protiopatření nemusí být vůbec implementována.

1.9.2. Bezpečnostní politika

Termín „bezpečnostní politika organizace“ se objevuje ve všech přístupech řešení informační bezpečnosti. Jedná se o klíčový bezpečnostní dokument schválený vrcholovým vedením organizace. Tento dokument je závazný pro celou organizaci a organizace v něm deklaruje své základní cíle v oblasti informační bezpečnosti. Pokud organizace přichází do styku s utajovanými skutečnostmi, je definována zákonem (Zákon č. 412/2005 Sb.). Dokument zajišťuje, aby byl dopředu vyřešen případný konflikt mezi bezpečnostními cíli a zájmy organizace, ke kterému by mohlo dojít. (7, str. 55)

Bezpečnostní politika v sobě zahrnuje souhrn norem, pravidel a praktik definujících způsob správy, ochrany a distribuce citlivé informace a jiných aktiv v rámci činnosti organizace. Neexistuje absolutně bezpečný systém. V případě, že analyzujeme IS z hlediska potřeb jeho zabezpečení, rozpoznáváme: (7, str. 55)

- objekt informačního systému (pasivní entita) – obsahuje nebo přijímá informace. Je zpřístupňován subjekty IS udělováním práv přístupu subjektům.

- subjekt informačního systému (aktivní entita) – například osoba, proces nebo zařízení činné na základě příkazu uživatele. Je autorizovatelný, oprávněný k získání informace z objektu, vydávání příkazů ovlivňujících udělení práv přístupu k objektu, změnu stavu objektu atd.

Z hlediska informační bezpečnosti je dokument zabývající se bezpečnostní politikou základní. Mělo by se jednat o dokument písemný, který by odpovídal na následující otázky: (7, str. 56)

- co chceme chránit
- proč budeme chránit
- jak budeme chránit
- jak ověříme, že objekt je opravdu chráněný
- co uděláme, když nastane havárie systému

Hlavní cíle bezpečnostní politiky jsou: (7, str. 56)

- definovat hlavní cíle při ochraně informací
- určit pravomoci a odpovědnosti
- stanovit způsob jak bezpečnost řešit

Má-li organizace přijatou celkovou bezpečnostní politiku, bude se jednat o rozpracování obecných zásad v oblasti informační bezpečnosti. (7, str. 56)

Aby bezpečnostní politika mohla plnit svůj účel, musí: (7, str. 56)

- mít písemnou formu
- být známá všem, koho se týká
- být závazná v celé organizaci (platit pro všechny úseky, zaměstnance, vedoucí)
- být schválena na úrovni vrcholového vedení

Jakákoliv jiná interpretace bezpečností politiky je zavádějící a vede k nezdaru. (7, str. 56)

1.9.2.1. Obsah a druhy bezpečnostní politiky

Bezpečnostní politika organizace bývá strukturována do časových rovin. Doporučení vypracování dokumentu je v následujících úrovních: (7, str. 56-57)

- **Celková bezpečnostní politika** – prezentuje globální popis cílů organizace, jejího IS a zabezpečení. Jedná se o dokument pro časový horizont 5-10 let.
- **Systémová bezpečnostní politika** – prezentuje popis jak chránit, distribuovat a organizovat aktiva IS, včetně popisu konkrétních bezpečnostních cílů, ohrožení zjištěná analýzou rizik a bezpečnostních opatření. Systémová bezpečnostní politika v sobě zahrnuje:
  - technickou, fyzickou, personální a komunikační bezpečnostní politiku. Pokud si rozsah a význam v dané oblasti IS vyžaduje, mohou být vypracovány jako samostatné bezpečnostní politiky.
  - specifikaci funkcí prosazujících bezpečnost. Stanovují autentizaci, autorizaci, klasifikaci dat, audit, atd.
  - specifikaci síly bezpečnostních mechanizmů. Určující způsoby k implementování funkcí k prosazení bezpečnosti.
  - ohodnocení úrovně bezpečnosti (bezpečnostní audit).
- **Detailní systémová (technická) bezpečnostní politika** – Existují dva přístupy k formulaci politiky. Volba závisí spíše na kultuře řízení a struktuře interní předpisové základny než na velikosti a charakteru organizace.
  - **Stručná politika** – rozsah 3-5 stran. Obsahuje pouze základní zásady označované jako „high-level-policy“. Hodí se tam, kde má střední management dostatek pravomocí vydat závazné interní předpisy nebo standardy.
  - **Detailní politika** – rozsah řádově desítek stran. Obsahují jednotlivá bezpečnostní opatření platná pro celou organizaci a jsou společná všem IS organizace. Je nezbytná tam, kde je uplatňován hierarchický model řízení a cokoliv závazného pro celou organizaci může vydat pouze vedoucí.

Občas je výhodné tyto dva přístupy spojit. Jestliže se systém informační bezpečnosti v organizaci teprve zavádí a je-li cílem schválení detailní politiky vrcholovým vedením, může být doporučení následující: (7, str. 57)

1) schválit stručnou politiku
2) v klidu připravit a během 1-2 let schválit detailní politiku

Tyto dva kroky usnadňují, jsou rychlejší a osvědčené. (7, str. 57)

Některé prameny doporučují v politice uvádět také zdroje, ze kterých politika vychází – smluvní, legislativní, závěry rizikových analýz včetně ocenění aktiv atd. Záleží však na formě zpracování, není na tom nic špatného. Tato ustanovení mají totiž obvykle popisný a vysvětlovací charakter. Uživatele však příliš nezajímají a mají obvykle spíše rušivý charakter. Je přitom potřeba dávat pozor, aby se zbytečně nešířily zneužitelné informace o hrozbách a zranitelnosti IS. (7, str. 58)

Obrázek 13: Schéma vazeb druhů bezpečnostních politik organizace
Upraveno podle (7, str. 59)

1.9.2.2. Výhody a přínosy bezpečnostní politiky organizace

- Pro IS přináší rozpracované principy řízení informační bezpečnosti.
- Konkrétní zdokumentovaná pravidla pro efektivní správu IS má odborný personál, který spravuje IS organizace.
- Když je bezpečnost analyzována a vyřešena na velmi podrobné úrovní, sníží se zranitelnost IS organizace.
- Definují se specifické požadavky na chování vnějších subjektů IS. Včetně základních vzorových smluv pro zajištění bezpečnosti komunikačních a informačních technologií.
- Pro práci s informačním systémem budou znát všichni zaměstnanci konkrétní povinnosti a odpovědnosti.
- Vážný zájem organizace zabývat se informační bezpečností (plyne z vypracování studie).
- Zvyšuje kredit společnosti u spolupracujících organizací a obchodních partnerů. Je vypracována dle norem a standardů a je kompatibilní s dokumentací ISO v organizaci.
- Pohled zvenčí často odhalí a pojmenuje chyby, o nichž se ví, ale nemluví se o nich.
- Komplexní přístup ukáže i na vazby uvnitř společnosti a její fungování. (7, str. 59)

Bezpečnostní politika se liší pro každou konkrétní entitu (např.: firmu, státní organizaci, obchodní organizaci apod.) Je sestavována na základě analýzy, která se skládá z analýzy aktiv, hrozeb a rizik. (7, str. 60)

1.9.2.3. Typy bezpečnostních politik organizace

Variant přístupů k zabezpečení IT je více. Některé přístupy jsou zajímavé nákladově, jiné dosaženou transparentností či odolností proti útoku výjimečné síly. Doporučená varianta by měla vždy vzejít z oponované a závazně přijaté bezpečnostní politiky organizace a bezpečnostní politiky IT organizace. A to při respektování

výsledku analýzy rizik IS. Na základě požadované úrovně zabezpečení rozpoznáváme čtyři obecné typy: (7, str. 60-61)

- **Promiskuitní bezpečnostní politika** – neomezující politika. Každý může dělat i to, co by dělat správně neměl. Obvykle jsou IS s promiskuitní bezpečnostní politikou provozně nenákladné. Zaručují minimální nebo vůbec žádnou zabezpečenost (nenutí povinně používat ani hesla). Důvodem k používání této politiky může být ekonomicky nenákladné řešení. Potřebná úroveň bezpečnosti může být zajišťována prostředky mimo komunikační a informační technologie.
- **Liberální bezpečnostní politika** – až na věci explicitně zakázané je povoleno vše. Tato politika se používá v prostředích, ve kterých se hrozby považují za málo až průměrně závažné a nepominutelným požadavkem je i nízká ekonomická náročnost řešení bezpečnosti. Zaručuje však větší zabezpečení než politika promiskuitní.
- **Opatrná (racionální) bezpečnostní politika** – zakazuje dělat vše, co není explicitně povoleno. Tato politika je nákladnější na zavedení, ale zaručuje vyšší míru bezpečnosti. Aplikace vesměs požaduje provedení klasifikace objektů a subjektů podle jejich schopností a citlivosti. Je opřena o zásadu povinného řízení přístupu založeného na rolích. Tyto role vystupují jako subjekty při styku s IS organizace. Obvykle je počáteční bezpečnostní politikou při zavádění firewallů.
- **Paranoidní bezpečnostní politika** – zakazuje dělat vše, co je potenciálně nebezpečné. Tedy i to, co by nemuselo být explicitně zakazováno. Tato politika zaručuje nejvyšší stupeň ochrany. Vede k maximální izolaci systému. Pro organizace je také užitečná, např. databázový systém zpracovávající vysoce důvěrné informace lze fyzicky i technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů. Paranoidní charakter umožní implementaci aplikace v prostředí s nízkou systémovou režií, tedy s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

1.9.2.4. Základní principy bezpečnostní politiky organizace

Následující výčet má generický charakter. Níže popsané principy se musí při vypracovávání bezpečnostní politiky pro konkrétní organizaci přesně a konkrétně specifikovat. (7, str. 61)

- **Princip adresné odpovědnosti** – princip adresné odpovědnosti požaduje, aby byly stanoveny odpovědnosti vlastníka, správce, uživatelů IS, managementu organizace, programátorů, pracovníků údržby, operátorů a pracovníků provozních složek organizace, správce sítě, externího a interního auditoru tak, aby jejich činnost byla na potřebné úrovni detailizace bezpečně protokolována.
- **Princip znalosti** – požaduje, aby cíle bezpečnostní politiky a použitá opatření byly známy všem subjektům participujícím na IS a uměly je aplikovat. Být informován a rozumět principům zabezpečení je legitimním zájmem takovýchto subjektů. Příkladem může být provozovatel nějaké sítě, který umožní další organizaci síť používat pro poskytování služeb třetím stranám. Může si do smlouvy dát požadavek, že musí být jako provozovatel sítě seznámen s bezpečností takového IS.
- **Princip etiky** – princip etiky požaduje respektování práv a legitimních zájmů ostatních, a to i na úrovni sociálních norem chování.
- **Princip multidisciplinárnosti** – požaduje akceptovat všechna relevantní technická, provozní, komerční, administrativní, legislativní a výchovná hlediska bezpečnosti IS a organizace. Politika musí být vybudována s respektováním zájmů a povinností managementu organizace, oddělení technické podpory, obchodního i právního oddělení, atd. Například pro vojenskou organizaci, školu, městský úřad je vhodná jiná bezpečnostní politika.
- **Princip úměrnosti** – princip úměrnosti požaduje, aby síla bezpečnostních funkcí byla úměrná jak možným hrozbám, tak rizikům i možným škodám. Dosažení maximální bezpečnosti za každou cenu nemusí být ekonomické. Bezpečnostním opatřením může být například i pojištění.
- **Princip integrity** – bezpečnostní politika musí zajistit celý cyklus života informací – jejich získávání, zpracování, vytváření, přenášení, uchovávání

a rušení. Celková bezpečnost IS je dána úrovní bezpečnosti jejího nejslabšího článku.

- **Princip aktuálnosti** – vyžaduje spolupráci partnerů při čelení aktuálním hrozbám a způsobům jejich projevu.
- **Princip periodického hodnocení** – je dáno tím, že prvky IS jsou obvykle dynamickou jednotkou. Požadavky na bezpečnost a efektivnost se v průběhu času mění.
- **Princip kompatibility s legitimním použitím a toky dat** – vychází z norem a obecně platných normativních aktů. Dodržování tohoto principu zabraňuje zevšeobecňování požadavků na bezpečnost jednou stranou znemožnit oprávněnou činnost jiným stranám. (7, str. 61-62)

1.9.2.5. Problematika a nedostatky při realizaci bezpečnostní politiky organizace

Práce nekončí vytvořením bezpečnostní politiky. Politiku je třeba přijmout a vyhlásit. Bez managementu organizace, který chce a je ochotný tuto záležitost prosadit a rozhodnout, nelze jednoduše ustát schvalovací proces. Bezpečnostní politika by měla být relativně neměnným dokumentem s frekvencí aktualizace ne kratší než dva roky. (7, str. 62)

Bezpečnostní politika je vytvořena v průběhu prvního roku. Ve druhém se jedná o jejím přijetí. Klíčovým okamžikem je však schválení politiky managementem, který podstatným dílem rozhoduje o úspěchu či neúspěchu řešení informační bezpečnosti. Je-li přijata, zbývá ji už jen vyhlásit. (7, str. 62)

Je nutné, aby s dokumentem byli obeznámeni všichni zaměstnanci. Ne s celým obsahem, ale vždy s tou částí, která bezprostředně souvisí s jejich výkonem práce. Nesmírně důležitý je také způsob formy seznamování zaměstnanců s bezpečnostní politikou. Má-li být dosaženo očekávaného efektu, je vhodné spolupracovat s profesionály. (7, str. 63)

V praktické realizaci bezpečnostní politiky se mohou vyskytovat problémy a nedostatky jako jsou: (7, str. 63)

- **velké množství kompromisů** – jedná se o častý jev, kdy z procesu schvalování z původní verze zůstala jen část. Pasáže, které byly problematické, byly vypuštěny nebo přepsány. Také pravomoci a zodpovědnosti byly zredukovány na nezbytné minimum. Politika se v tomto případě stává naprosto sterilní a společnosti neumožňuje řešit to, co je skutečným problémem.
- **nereálná bezpečnostní politika** – nesmírně přísná politika. Jedná se o stav, kdy jí společnost téměř v žádném případě nevyhovuje. V takovém případě je nutné definovat přechodné období a postupný proces implementace. Nestane-li tak, je velice pravděpodobné, že zaměstnanci celý proces seznámení s politikou budou vnímat odlišně od reality a budou jej jako celek ignorovat. Taková neúcta k interní legislativě by mohla vést k daleko horší situaci, než byla před přijetím politiky.
- **neadekvátní rozsah politiky** – znamená, že byla managementu předložena příliš rozsáhlá politika. Nemožnost managementu se seznámit detailně s celým dokumentem a pochopit význam jednotlivých ustanovení zpomalí nebo dokonce zastaví proces schvalování politiky.
- **podcenění propagace politiky** – v praxi se můžeme setkat s případy, kdy existence bezpečnostní politiky není známa většině zaměstnanců. Obvykle se nejedná o úmysl, ale podcenění situace, kdy se nezvládla komunikace směrem dovnitř organizace. Dokument, který může být zpracován excelentně, nebude k ničemu, neseznámí-li se s ním zaměstnanci a nebudou se podle něj řídit.
- **nekritické přebírání vzorců** – má-li jedna společnost kvalitní politiku, není zaručeno, že její přenesení do druhé společnosti bude mít stejný výsledek. Takovéto vylepšování bez předchozí analýzy může přinést velice špatný výsledek.

1.9.3. Bezpečnostní projekt

Úkolem bezpečnostního projektu je praktická implementace bezpečnostní politiky v prostředí dané organizace. Představuje konkrétní požadavky v konkrétní oblasti (například zabezpečení vstupu pro fyzickou ochranu objektu). (2)

Dělení bezpečnostních projektů do skupin (podle zákona č. 119/2007 Sb. o ochraně utajovaných skutečností a bezpečnostní způsobilosti): (2)

- administrativní
- technická
- personální
- objektová
- kryptografická ochrana informací
- bezpečnost informačních systémů

Vstupem pro zpracování bezpečnostních projektů jsou: (8, str. 76-77)

- globální (strategická) bezpečnostní politika (bezpečnostní politika IS)
- požadavky bezpečnostního managementu
- požadavky a návrhy řešení bezpečnostních konzultantů
- požadavky od vedoucích pracovníků

Výstupy bezpečnostního projektu: (7)

- technická a technologická opatření (pracovní postupy, HW, SW, aj.)
- organizační a administrativní opatření (dokumentace a krizové plány)

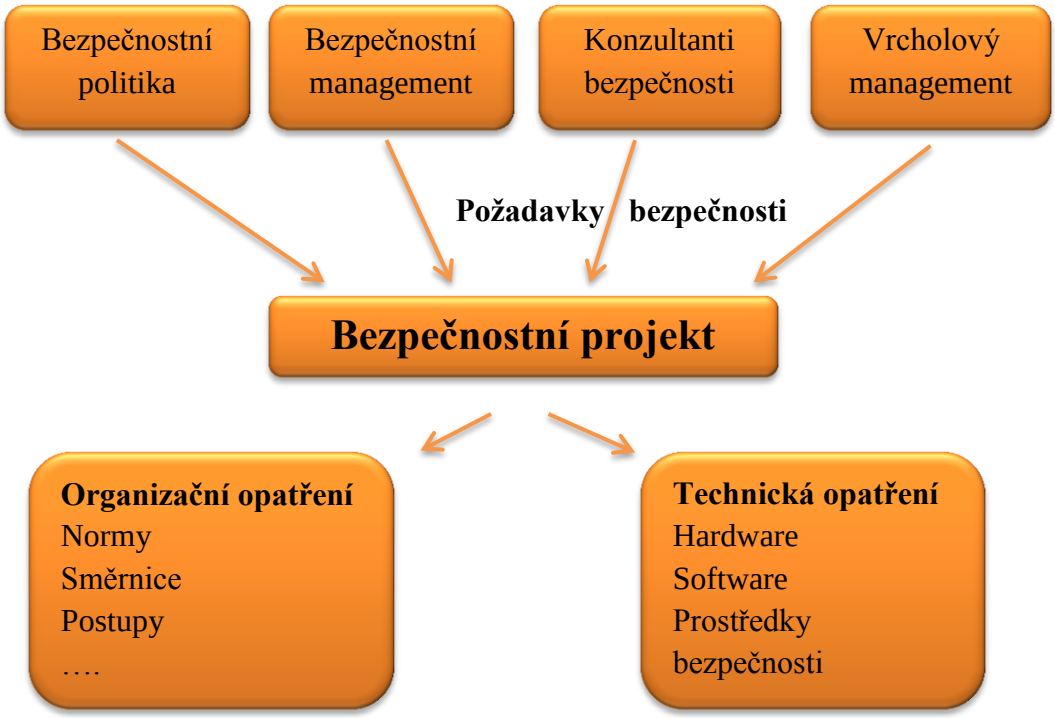
Výstupní návazné dokumenty (2; 8, str. 77)

- podnikové směrnice, nařízení a opatření
    - Funkční bezpečnostní politika IS
    - Personální bezpečnostní politika IS
    - Řešení bezpečnostních incidentů
    - Používání výpočetní techniky
    - Unifikace SW a uživatelského prostředí
    - Tvorba a zavádění automatizovaných úloh do provozu

- Využívání elektronické pošty v datové síti a přístup do Internetu
- Používání antivirových systémů
- Klasifikace dat IS
- Klasifikace IS
- Klasifikace uživatelů IS
- Režim přístupu pracovníků vývoje SW k datům, serverům a k prostředí operačního systému

- metodiky
  - Metodika vývoje IS
  - Metodika zavádění IS do provozu
  - Metodika pro zpracování dokumentací

- provozní řády
  - Provozní řády oddělení
  - Provozní řády aplikací

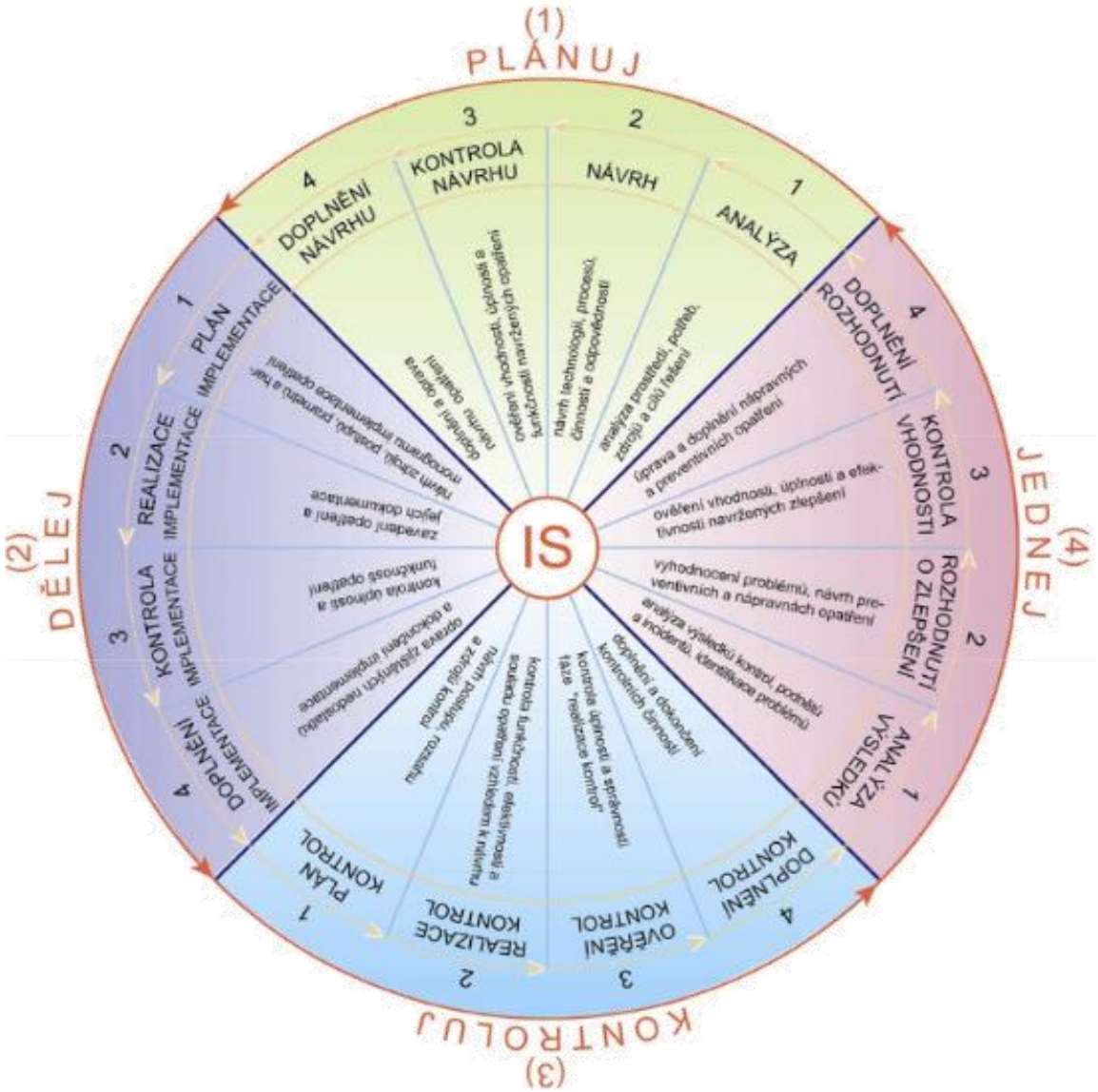


Obrázek 14: Bezpečnostní projekt
Upraveno podle (7, str. 74)

1.9.4. Údržba a zlepšování ISMS

Údržba a zlepšování ISMS jsou poslední fází cyklu PDCA a představují nejdůležitější rozhodovací krok celého procesu. Když by model PDCA nebyl rozšířen o tuto 4. fázi, stal by se pouze jednorázovým procesem, díky němuž by se zabezpečení informací stalo statickou a velmi rychle zastaralou událostí v historii. (9)

Klíčovým významem této fáze je vyhodnocení výsledků auditu a kontrol funkčnosti bezpečnostních opatření i ISMS procesu samotného a nastartování dalšího cyklu PDCA, ve kterém budou naplánovány, zavedeny, zkontrolovány a opět vyhodnoceny nápravná a preventivní opatření k zajištění požadovaného a konzistentního stavu bezpečnosti v čase. (9)



Obrázek 15: Princip vnořených PDCA fází
Zdroj (9)

Každou fázi PDCA cyklu je vhodné naplánovat, zrealizovat, poté zkontrolovat a doplnit. Z tohoto důvodu v sobě zahrnují další vnořené PDCA cykly, které se samostatně roztáčejí pro realizaci každého kroku. (9)

Princip vnořených PDCA fází uvnitř základního PDCA procesu znázorňuje obrázek č. 15.

Nápravná a preventivní opatření

Nápravná opatření slouží k odstranění nalezených nedostatků a chyb spojených s implementací a provozem ISMS a k zabránění jejich dalšímu trvání. Příkladem může být neúplná dokumentace, nedostatečné proškolení pracovníků, neúplná implementace opatření zvolených v Prohlášení o aplikovatelnosti opatření apod. (9)

Cílem opatření je zabránit výskytu potencionálních neshod v budoucnu. Tedy za účelem eliminace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody může být například nedodržení rolí u některých činností a opatření ISMS, nebo také nedůsledné provádění monitorovacích a kontrolních činností. (9)

Pro malé organizace je typická rychlá praktická změna. Proto se přiklání především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější. (9)

Už ale pro středně velké organizace, není již hledisko nákladů na pořízení a zavedení opatření tak palčivé jako pro malé organizace. Proto bude při jejich výběru více rozhodovat účinnost a pokrytí nalezených nedostatků. (9)

Měření účinnosti

Měření účinnosti aplikovaných bezpečnostních opatření patří k prosazování efektivního řízení bezpečnosti. Na obrázku č. 16 je zobrazen model měření bezpečnosti informací.

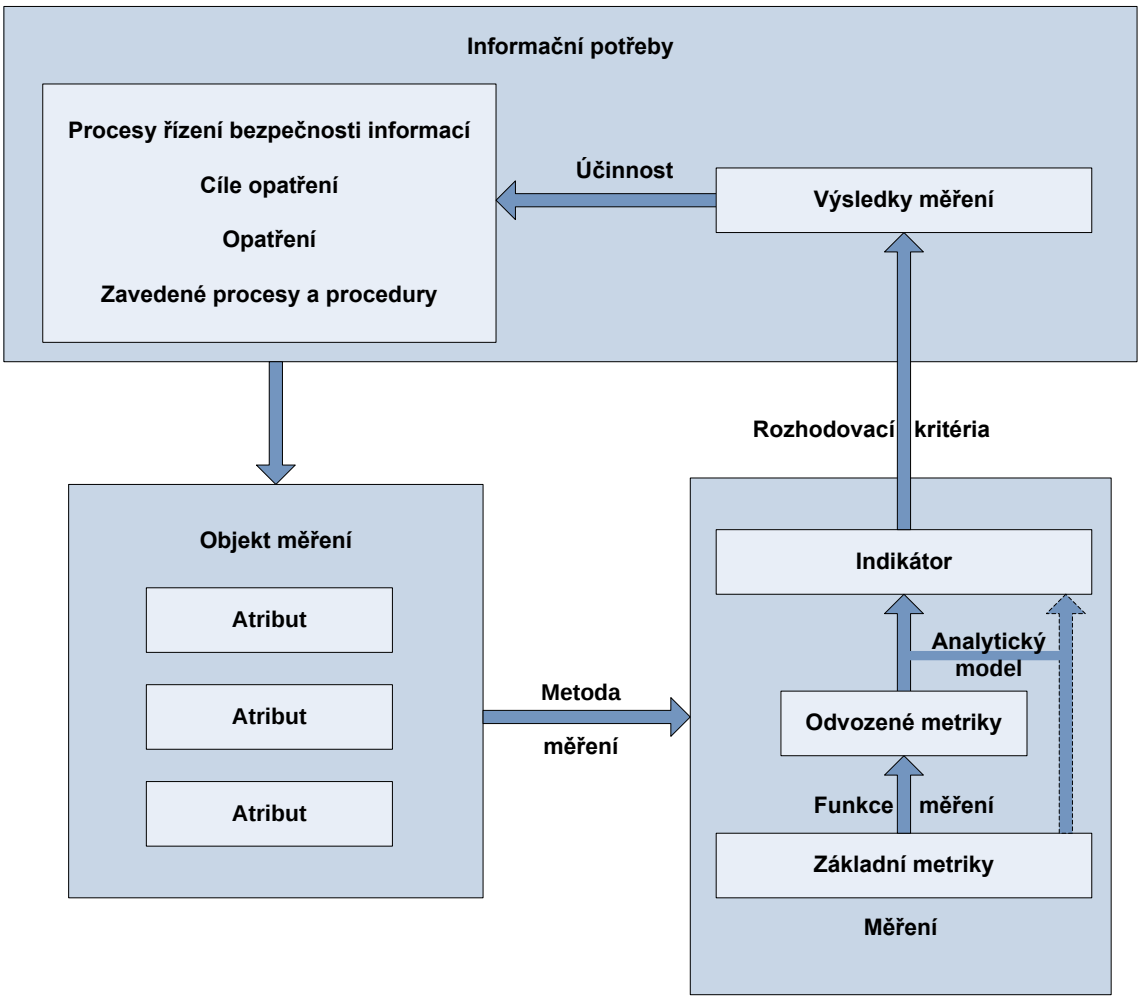
Metrika je přesně vymezený ukazatel nebo hodnotící kritérium používané k objektivnímu hodnocení úrovně efektivnosti. (8, str. 71)

Metriky podle NIST dělíme na: (8, str. 71)

- implementační
- výkonnostní
- dopadové

Ukazatele pro měření bezpečnosti informací lze rozdělit na základní skupiny: (8, str. 72)

- finanční
- personální
- technické (ukazatele provozu IS/ICT)



Obrázek 16: Model měření bezpečnosti informací
Zdroj (8, str. 72)

Podle ISO/IEC 27004:2009 je uveden příklad struktury měření, přílohy B

Tabulka metrik pro hodnocení účinnosti: (8, str. 72-73)

B.1 ISMS školení

B.1.1 ISMS - vyškolený personál

B.1.2 Školení informační bezpečnosti

B.1.3 Dodržování povědomí informační bezpečnosti

B.2 Politiky hesel

B.2.1 Kvalita hesel – manuální

B.2.2 Kvalita hesel – automatizovaná

B.3 Kontrola procesu ISMS

B.4 Neustálé zlepšování správy incidentů bezpečnosti informací (ISMS)

B.4.1 Účinnost

B.4.2 Provádění nápravného opatření

B.5 Závazek vedení (managementu)

B.6 Ochrana proti škodlivým kódům

B.7 Kontrola fyzického přístupu

B.8 Vyhodnocení Log souborů

B. 9 Řízení periodické údržby

B.10 Bezpečnost ve smlouvách s třetími stranami

1.10. Školení uživatelů

Tato kapitola slouží jako teoretický podklad ke školení zaměstnanců. V praktické části se budeme zabývat metodikou školení pro výukové středisko.

Povinnost pravidelného školení, v případě, že je ISMS ve společnosti certifikován, vyplývá přímo z normy, která nařizuje pravidelné opakování školení. Opatření přímo říká: „Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran musí, s ohledem na svou pracovní náplň absolvovat odpovídající a pravidelně se opakující školení v oblasti bezpečnosti informací, bezpečnostní politiky organizace jejich směrnic.“ (10)

V případě, že organizace má pravidla ISMS implementována, ale není certifikována, nic ji nenutí provádět pravidelná školení. Je jasné, že pokud základní pravidla dodržována nejsou, není celý systém řízení bezpečnosti informací vůbec funkční. (10)

Obecně totiž platí, že kontrolovat a vytýkat chyby uživateli je možné, je-li proškolen. Správně poučený uživatel také znamená menší riziko pro IS. (10)

Jak uživatele školit

Jedním ze základních dokumentů v rámci ISMS jsou tzv. „Minimální bezpečnostní pravidla pro uživatele." Veškerá základní školení by měla tedy logicky vycházet z tohoto dokumentu. Jedná se o základní návod, jak se má uživatel chovat při práci s IS a výpočetní technikou. Je vhodné při školení dodržet tyto základní body: (10)

- krátké vysvětlení co ISMS znamená a jaký je jeho přínos pro organizaci
- aktuální stav bezpečnostní politiky organizace
- ujasnění odborných pojmů (analýza rizik, aktivum, informační bezpečnost)
- dokument „Minimální bezpečnostní pravidla pro uživatele"
- zdůraznění změn oproti předchozímu školení
- ověření znalosti uživatelů (například formou testů)

Školení je vhodné rozvrhnout alespoň do dvou hodin, neboť se doporučuje jak forma názorných příkladů tak případů bezpečnostních incidentů. Běžné uživatele není možné zahrnout technickými podrobnostmi. Taková školení jsou vhodná pro administrátory, případně ostatní technický personál. (10; 11)

Nedoporučují se masová školení v počtu několika desítek uživatelů. Vhodným počtem je max. 15 pracovníků. V takové situaci je možné se věnovat řešení různých individuálních problémů, případně se vrátit ke složitějším souvislostem. (10;11)

Příklad struktury školení: (10;11)

- úvod do informační bezpečnosti

- hrozby informační bezpečnosti (příklady z praxe)
  - příklady vnějších hrozeb
  - příklady vnitřních hrozeb
  - nebezpečí elektronické komunikace
  - rizika používání sociálních sítí
  - útoky sociálního inženýrství
  - lesk a bída mobilních technologií
  - aktuální hrozby internetu
- metody řízení informační bezpečnosti
- pravidla pro uživatele (podle požadavků konkrétní organizace)
- shrnutí
- diskuse

O průběhu každého školení je vhodné zpracovat záznam, který bude obsahovat podpisy všech zúčastněných o absolvování daného školení. Za vypracování záznamu a následné uchování může odpovídat například bezpečnostní manažer. (10;11)

Kdy uživatele školit

Proškolení uživatelů by mělo být minimálně před vznikem pracovního poměru a následně v jeho průběhu. Před vznikem pracovního poměru je důležité, aby se svými povinnostmi a právy byli srozuměni jak zaměstnanci, tak pracovníci smluvních a třetích stran. Pracovníci jsou zároveň seznamováni s bezpečnostními pravidly a s odpovědností za jejich dodržování. V průběhu pracovního poměru je vhodné školení provádět pravidelně. V prvním cyklu zavádění ISMS, neboli v prvním cyklu PDCA, se doporučuje školit nejméně 1x za 6 měsíců. Po zavedení a „usazení“ systému bezpečnosti lze přejít na roční cyklus školení. (10)

Jestliže jsou všichni zaměstnanci proškoleni na základní bezpečnostní pravidla, je vhodné zavést pokročilá školení. Především pro administrátory, obslužný personál a dále pro vysoce odborné uživatele. (10)

Výše byla popsána standardní školení, která jsou plánována pravidelně a v dostatečném časovém předstihu. Je-li však mezi těmito pravidelnými školeními provedena zásadní změna v IS, je nutné všechny uživatele upozornit a provést nové školení. V tomto případě není potřeba procházet jeho celou náplň, ale soustředit se jen na nové funkčnosti systému a nová rizika z nich vyplývající. (10;11)

Při nástupu do zaměstnání bývají nařízena školení v oblasti BOZP apod. Je vhodné v rámci těchto školení zařadit i problematiku ISMS, která dodá alespoň základní pohled. (10;11)

Doporučuje se také provést individuální školení jednotlivých uživatelů při ukončení pracovního poměru, především z důvodu připomenutí závazku mlčenlivosti atd. (10)

2. Analýza současného stavu

Návrh projektu je určen pro výukové středisko zabývající se chemickým průmyslem. V tomto středisku bude probíhat nejen školení zaměstnanců, ale také výzkum ve speciálně vybavených laboratořích. Toto středisko odkoupili noví majitelé a plánují celkovou rekonstrukci objektu do podoby, která je uvedena v přiložených půdorysech.

Doposud byl objekt veden jako hotel se stravovacím zařízením, společenskou místností a posilovnou. Níže uvedené kapitoly se z tohoto důvodu nebudou zabývat starým objektem, který projde kompletní rekonstrukcí, ale popisem objektu, který bude realizován. Zabezpečení objektu před koupí novými majiteli bylo téměř zanedbatelné, proto popíšeme především požadavky investora a také jeho možnosti.

Z důvodu, že se tato práce zabývá zabezpečením tohoto střediska, nebudou blíže specifikováni majitelé ani umístění objektu.

2.1. Popis výukového střediska

Výukové středisko zaměřené na školení zaměstnanců a výzkum v oblasti chemického průmyslu projde celkovou rekonstrukcí stávajícího objektu. Níže v této kapitole jsou stručně popsány jednotlivá patra výukového střediska a základní místnosti. Rozpis všech místností je uveden v kapitole č. 2.2.

Zaměstnanci i návštěvníci budou disponovat čipovými kartami, pro něž bude nastaven konkrétní přístup do jednotlivých oblastí. Pouze hoteloví hosté nemají v tomto případě přístup ke kancelářím, technologickým místnostem či konferenčnímu sálu.

V prvním patře je plánována vstupní hala s recepcí. V levém křídle bude zrealizována technologická zóna, v níž bude umístěna zkušební laboratoř se skladem náhradních dílů a přípravnou surovin. Nalezneme zde i kanceláře. V pravém křídle bude umístěná restaurace s vlastní výrobou pokrmů, terasou a samostatným zásobovacím vstupem. Počet míst k sezení je plánováno na 50 s kapacitou cca 120 jídel. Skladová část je oddělena podle jednotlivých druhů surovin a tak znemožňuje ovlivňování

jednotlivých částí. Řešením je oddělená umývárna od kuchyňského provozu, provozní kancelář, úklid, odpadky, kiosek, šatna a WC s koupelnou.

Pro výukové centrum je nezbytná provozní plošina kam se dostaneme buď chodbou v druhém patře, anebo po schodech z prvního patra ze zkušební laboratoře. Nezbytnou součástí je laboratoř a místnost, kde se provádí fermentace. V pravé části budou vybudovány kanceláře a nad recepcí posluchárna. Nezbytností je umístění toalet vedle posluchárny.

Ve třetím patře bude vybudováno 8 hotelových pokojů. Čtyři pokoje v levém křídle a další čtyři v křídle pravém. Každý pokoj disponuje chodbou a šatnou, která je buď oddělena, nebo je součástí chodby či předsíně. Koupelna je umístěná v první části pokoje. Ve druh části pokoje, je umístěn kuchyňský kout. Nad recepcí bude vybudována konferenční místnost, u níž budou umístěné toalety.

Dalších 8 hotelových pokojů je umístěno v patře čtvrtém. I zde, každý pokoj disponuje chodbou a šatnou, která je buď oddělena, nebo je součástí chodby či předsíně. Koupelna je umístěná v první části. Ve druhé obytné části pokoje, je umístěn kuchyňský kout. Navíc v tomto patře bude vybudován byt 1-2KK a dvě technologické místnosti, které budou umístěné nad recepcí.

2.2. Přehled místností výukového střediska

V příloze č. 1 jsou uvedené tabulky obsahující čísla místností, které odpovídají přiloženým půdorysům a popisu těchto místností, rozdělených po jednotlivých patrech.

2.3. Požadavky investora

Pro přehlednost jsou rozděleny následovně:

Po celém objektu:

- Elektronický zabezpečovací systém (EZS)
- Elektronický požární systém (EPS)

- Nouzové LED osvětlení
- Čtečky karet pro přístup

V přízemí:

- Bezpečnostní okna
- Čidla rozbití oken
- Kamerový systém

Specifický požadavek:

- Zabezpečení dokumentů

2.4. Základní kritéria a požadavky investora

Základním kritériem investora je parametr poměr cena/výkon. Investor požaduje „TOP“ řešení a záruku na certifikovanou instalaci. Ke smlouvě mohou být v průběhu návrhu či instalace přidány dodatky, které návrh projektu pozmění. Projekt je navrhován na maximální vhodné řešení.

Investor požaduje nepřekročení částky 2 500 000,-Kč. V případě překročení stanovené částky je potřeba tuto překročenou sumu zdůvodnit a vyčíslit.

3. Návrh řešení

Tato kapitola se nejdříve zaměřuje na návrh zabezpečení IS, které není řešeno technologicky. Zaměstnanci či návštěvníci musí mít přiřazena pouze vymezená práva a je také nezbytné, aby se zaměstnanci zaměřili na kvalitu svých hesel. Z důvodu, co možné nejvyšší úrovně zabezpečení, bude vymezen seznam zakázaných činností. Zaměstnanci musí projít školeními, na něž se kapitola „Metodika školeními provozního řádu“ zaměřuje. V další části této kapitoly je popsán návrh umístění jednotlivých komponent, které mají zvýšit úroveň zabezpečení a taktéž orientační ceník. V závěru se podíváme na soulad s požadavky (viz. příloha 59) a certifikaci ISMS (viz. příloha 60).

Vlastní návrh řešení se primárně odkazuje do příloh, neboť tyto přílohy jsou stěžejní částí zpracování zabezpečení výukového střediska zpracovaného jako samostatný projekt. Výjimku tvoří kapitola 3. 3. „Návrh umístění jednotlivých komponent“, kde jsou popsány vlastnosti včetně požadavků a jejich umístění, které je následně znázorněno v přiložených přílohách.

3.1. Návrh zabezpečení IS výukového střediska

Zabezpečení objektu je možné po technologické stránce mnoha řešeními. Vše ale technologie zabezpečit nedokáže. Lidská činnost je nejslabším článkem v rámci bezpečnosti. Proto se v této kapitole zaměříme na nastavení práv pro vedení i zaměstnance dle jednotlivých pracovních pozic. Nezbytností je vymezit zákaz činností a také postihů za nedodržování těchto pravidel. Lidé všeobecně nepoužívají kvalitní, silná hesla a proto se zaměříme také na jejich vytvoření a pravidelnou obměnu. Návrh zabezpečení IS je rozepsán v příloze č. 2.

3.2. Metodika školení provozního řádu

Metodika školení provozního řádu bude rozdělena na několik kapitol. V první kapitole se budeme zaměřovat na základní školení určené pro všechny zaměstnance, ve kterém budou vysvětleny základní pojmy včetně nejčastějších chyb. V dalších kapitolách jsou popsána školení specifická pro vedení, žáky výukového centra

a výzkumu, školitele a na zaměstnance, kteří pracují ve výzkumu. Jednotlivé metodiky školení dle výše zmíněného rozdělení jsou uvedeny v příloze č. 3

Podle zákona o kybernetické bezpečnosti a o změně souvisejících zákonů, schváleného dne 2.1.2014 se podle §5 rozumí bezpečnostními opatřeními opatření organizační a technická. (12)

Organizačními opatřeními jsou: systém řízení bezpečnostních informací, řízení rizik, bezpečnostní politika, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností, kontrola a audit kritické informační infrastruktury a významných informačních systémů. (13)

Technickými opatřeními jsou: fyzická bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných IS, jejich uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů. (13)

V §6 paragrafu prováděcí předpis stanovuje: obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace, rozsah bezpečnostních opatření pro orgány i osoby uvedené v zákoně v §3 odstavců c) až e), významné informační systémy a jejich určující kritéria. (13)

V základním školení, které musí absolvovat všichni zaměstnanci, jsou v základních pojmech uvedena některá organizační a technická opatření, se kterými budou posluchači seznámeni. (13)

3.3. Návrh umístění jednotlivých komponent

Níže v této kapitole jsou popsány jednotlivé bezpečností komponenty včetně umístění a jejich specifické požadavky. Umístění těchto komponent je znázorněno v přílohách, na něž se jednotlivé kapitoly odkazují.

3.3.1. Návrh kamerového systému

Kamerový systém navrhuji do venkovních prostor 1. patra. Kamery doporučuji skryté, a jejich umístění znázorňuji na půdorysech, v přílohách 40-42. Z půdorysů je zřejmé, že umístění kamer jsem řešila na základě vstupů do budovy a oken. Kamerový systém pokrývá i terasu restauračního provozu.

Podle návrhu umístění kamer a domluvy s investorem, nenavrhuji kamerový systém implementovat do vyšších pater budovy.

Pro kamerový systém navrhuji IP kamery s nočním viděním a full real time nahráváním. Lze nastavit detekční zóny s několika úrovňovou citlivostí detekcí pohybu. Podporován je JPEG formát. (14)

Detekce pohybu je oznamována odesláním zprávy o alarmu na FTP nebo e-mail. Dálkový přístup možný odkudkoli – z internetu, nebo mobilního sledování, s rozhraním Ethernet. (14)

IP kamery jsou do venkovních prostor, proto je navrženo pro 90- ti % relativní vlhkost krytí IP66. (14)

Oznamovací povinnost provozování kamerového systému

Provozování kamerového systému je považováno za zpracování osobních údajů, jestliže je kromě kamerového sledování prováděn obrazový nebo zvukový záznam pořizovaných záběrů a účelem pořizovaných záznamů je využití k přímé či nepřímé identifikaci fyzických osob v souvislosti s jejich určitým jednáním. (15)

V našem případě doporučuji provozovat kamerový systém se záznamem, který je možný na základě několika právních důvodů: (15)

- je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce nebo jiného subjektu – jedná se typicky o ochranu majetku, která je nejčastějším důvodem provozování kamer se záznamem
- pokud je zpracování nezbytné pro dodržení právní povinnosti správce – především v rámci plnění úkolů stanovených zákonem
- na základě souhlasu subjektu údajů – v omezených případech. Neboť v souvislosti s často se objevujícím provozováním kamerového systému na pracovišti zaměstnavatele v pracovní době, které je místem výkonu práce zaměstnance, je nutné, kromě zákona č.101/2000 Sb., aplikovat konkrétní ustanovení č. 262/2006 Sb. a zákoník práce zejména §316.

Toto provozování podléhá oznamovací povinnosti Úřadu pro ochranu osobních údajů podle § 16 zákona č. 101/2000 Sb. K plnění povinnosti je možné využít elektronický formulář oznámení o zpracování osobních údajů, který můžeme naleznout na webových stránkách Úřadu www.uoou.cz. K formuláři je potřebné připojit i přílohy, pokud existují. Jedná se o kopii plné moci (není potřeba notářského ověření), pokud oznamovatele zastupuje jiný subjekt a seznamy míst zpracování, jestliže se nevešly do formuláře. Následně má úřad pro ochranu osobních údajů lhůtu 30-ti dní na zapsání oznámení o zpracování osobních údajů do registru. Vznikem zápisu vzniká správci kamerového systému oprávnění zahájit provoz zpracování osobních údajů. Úřad pro ochranu osobních údajů vydává osvědčení o zápisu do registru pouze na žádost správce/oznamovatele. (15)

Žádost o vydání dokladu o bezpečnostní způsobilosti fyzické osoby z důvodu výkonu citlivé činnosti podle zákona č. 229/2013 Sb. vydává Národní bezpečnostní úřad. (15)

Výčet citlivých činností, jejichž zneužitím, by mohlo také dojít k ohrožení zájmu České republiky, je vymezen v §6 odstavci 2 zákona č. 229/2013 a jsou následující: (15)

- nakládání s bezpečnostním materiálem skupiny 5 nebo 6
- výkon funkce odpovědného zástupce při činnosti podle a)

- výkon funkce člena dozorní rady, statutárního orgánu nebo jiného kontrolního orgánu, prokuristy, odpovědného zástupce, je-li ustaven, právnické osoby, která nakládá s bezpečnostním materiálem skupiny 5 nebo 6

Pro výkon výše uvedených citlivých činností ze strany fyzických i právnických osob je nutné, aby dané osoby byly držiteli dokladu o bezpečnostní způsobilosti. (15)

Platnost dokladu o bezpečnostní způsobilosti je 5 let od data vydání. Platnost dokladu může zaniknout také z následujících důvodů: (15)

- uplynutím doby platnosti dokladu, úmrtím fyzické osoby
- zrušením platnosti dokladu
- poškozením dokladu
- vrácením dokladu na úřad
- dnem doručení osvědčení fyzické osoby nebo nového dokladu

3.3.2. Návrh LED osvětlení

Ve výukovém středisku zaměřeném na výzkum doporučuji implementovat LED osvětlení. LED osvětlení navrhuji z důvodu nouzového či orientačního osvětlení při výpadku el. energie.

Nouzové osvětlení navrhuji tak, aby při výpadku el. energie a místnosti zaplněné lidmi, předměty či vybudovaným schodištěm, zaměstnanci, studenti, hoteloví hosti či návštěva, bez rizika ublížení si na zdraví, či zničení materiálu a přístrojů, měli možnost se po místnosti pohybovat alespoň omezeně.

Návrh umístění LED osvětlení znázorňuji v přílohách 43-54. Doporučuji umístění zhruba ve 20-ti centimetrech nad zemí a s minimálně 5-ti LED zdroji.

3.3.3. Návrh nasazení bezpečnostních oken a umístění čidel

Z důvodu výzkumu ve výukovém středisku bylo jedním ze základních požadavků investora implementovat po celém prvním patře čidla rozbití oken a také nasadit bezpečnostní okna. I když je po areálu pohyb omezen na základě čipových karet a jsou

umístěna po areálu PIR čidla, zákazník požadoval bezpečnostní okna a čidla i do prostor restauračního provozu.

Toto opatření navrhuji z důvodu jak zabezpečení výzkumu, tak z důvodu restauračního provozu, kde jsou skladovány suroviny.

K detekci rozbití skla doporučuji čidla využívající duální metodu, při které je vyhodnocován náraz do skleněné výplně, přičemž jsou zároveň vyhodnocovány nepatrné změny tlaku vzduchu v místnosti. Takovéto řešení dosahuje vysoké spolehlivosti reakce při rozbití skleněné výplně. Citlivost detektoru je možné nastavit dle požadavků na vzdálenost a rozměry chráněných oken. Připojuje se k ústřednám poplachových systémů, z nichž je napájen. (14)

Detektor vyniká vysokou odolností proti vysokofrekvenčnímu rušení a jiným falešným signálům. Pro testování k aktivaci má čidlo v sobě zabudovanou červenou signálku. (14)

Na základě požadavků investora o nasazení bezpečnostních oken, v pravém křídle prvního patra, tedy v restauračním provozu a také na chodbách v pravém křídle a u recepce, navrhuji nasazení bezpečnostních oken 3. třídy. Vyznačují se střední odolností vůči vloupání. Těžkým nástrojem je možné je vypáčit až po 16-ti minutách.

V celém levém křídle, kde probíhá výzkum, navrhuji použití bezpečnostních oken 4. třídy, která se vyznačují nejvyšší odolností vůči pokusům o vypáčení a rozbití skel.

I když v druhém patře je taktéž pracovní plošina, nenavrhuji zde nasazení bezpečnostních oken, ani čidel rozbití skel. Rozhoduji tak z důvodu absence venkovních teras či balkónů.

Návrh umístění čidel znázorňuji v půdorysech v přílohách 55-57.

3.3.4. Návrh čteček karet

Vlastní návrh umístění čteček znázorňuji v přílohách 4-15.

Přístupy do těchto prostor jsem omezila nastavením práv, které jsou uvedeny v kapitole č. 3.1.

Čtečky neumísťuji do prostor veřejných WC a místností, kde je přístup povolen omezenými právy a jsou pro tyto zaměstnance, školitele, žáky či hotelové hosty společné místnosti.

Pro toto řešení navrhuji přístupový terminál, který eviduje všechny průchody, které přes něj byly provedeny. V počítači je pak zaznamenáno jméno a čas průchodu. Přístupový terminál je možné mít v režimu off-line, neboť u každého terminálu je vyveden konektor. Jackem je možné následné naprogramování či vymazání terminálu během několika málo sekund. (16;17)

3.3.5. Návrh EZS

PIR čidla navrhuji tak, aby směřovala především k oknům či dveřím. Na chodbách či schodech umisťuji PIR čidla jak s omezeným úhlem senzoru 180°, tak s úhlem 360°. PIR čidla neumísťuji do prostor, kde nehrozí krádeže, eventuálně krádež neohrozí výzkum či chod střediska. V restauračním provozu navrhuji umístění i do prostor uchování potravin, aby se zamezilo nežádoucímu pohybu v těchto prostorách.

Přílohy 28-39 znázorňují návrh umístění PIR čidel jak s omezeným úhlem senzoru 180°, tak umístění PIR čidel s úhlem 360°.

Ovládání PIR čidel je především systémové. Umístěny jsou dvě klávesnice u vchodu, které jsou využívané v případě uzavření celého areálu, nebo při neočekávaných událostech. Znázorňuji v příloze č. 30. Umístění sirény navrhuji skryté a návrh umístění zobrazuji ve stejné příloze (č. 30).

Napojení EZS

Pro potřeby střediska jsme rozhodla vybrat elektronický zabezpečovací systém, který je nabízen ve dvou variantách. Hlavní rozdíl spočívá v komunikaci mezi jednotlivými prvky EZS, které spolu mohou komunikovat buď po sběrnici, nebo bezdrátově. Primárním řešením bude komunikace po sběrnici. Výhodou pro nás je dodatečné řešení, které může chtít zákazník po několika letech doinstalovat na špatně dostupná místa. V tomto případě navrhuji využívat bezdrátové prvky, které komunikují pomocí rádiových vln. (18)

Podle zvoleného modelu, který bude ještě řešen se zákazníkem, budeme mít možnost vybavit ovládání EZS RFID čtečkou čipů/karet a také klávesnicí i displejem. K modulům budou připojeny ovládací segmenty, které slouží k ovládání jednotlivých sekcí EZS, výstupů poplachu alarmu, či přivolání tísňové linky. Pro detekci EZS zde bude napojení nejen PIR čidel, ale také přístupových karet, RFID čipů citlivých dokumentů, čidel tříštění skla a detektorů kouře a plynu. Tím zvýšíme bezpečnost o další stupeň, neboť napojení na EZS, které disponuje venkovní sirénou, může spustit poplach i možné tísňové volání. (18)

3.3.6. Návrh a umístění detektorů kouře a plynu

V levém křídle, prvním a druhém patře, kde probíhá výzkum, oba tyto detektory navrhuji umístit do všech prostor kromě kanceláří, společenské místnosti či sprch a WC.

V 1. patře restauračního provozu umisťuji detektory plynu v kuchyňském prostoru a na chodbách. V ostatních místnostech navrhuji pouze detektory kouře. Ve střední části areálu, kde je zázemí silnoproudých rozvodů dostačuje detektor kouře. Naopak v kotelnách doporučuji oba tyto detektory. Ve 2. patře v levém křídle a ve středu areálu, v prostorách kanceláří a posluchárny, tyto detektory neumísťuji.

V obytných prostorách je umístění detektorů kouře a plynu v kuchyňských koutech.

Detektory kouře jsou navrženy také ve 4. patře, v technických místnostech.

Po celém areálu jsou detektory kouře i plynu navrhuji umístění na schodištích a hlavních chodbách. U menších místností jako jsou WC, sklady, úklid či další podobné místnosti, detektory nenavrhuji.

Více znázorňuji v půdorysech, v přílohách 16-27.

3.3.7. Zabezpečení citlivých dokumentů

V rámci výukového střediska, kde probíhá výzkum v chemickém průmyslu je mnoho citlivých informací. Tyto informace nestačí jen zavřít do skříňky, neboť klíč lze snadno ukrást či skříň vypáčit. Proto jsem rozhodla, že tyto dokumenty budou označeny RFID štítky. Pro toto zabezpečení navrhuji RFID štítky následující: (16)

- **dle použité frekvence** – nízkofrekvenční systémy s frekvencí od 30KHz do 500KHz. Mají nižší operační systém a typicky jsou používány pro zabezpečení či sledování majetku.
- **podle typu** – pasivní – není potřeba na štítky zapisovat. Štítky byly vytvořeny pro dohledatelnost a identifikaci objektů, což je v našem případě základní požadavek.
- **formáty štítku** budou vybírány dle budoucího řešení a požadavků z následujících:
    1) lepící vložené – mohou být připevněny na produkt pomocí lepící hmoty umístěné na druhé straně
    2) samolepky – RFID lepící štítek
    3) zabudované – laminované nebo „zapouzdřené“ do speciálních obalů

3.4. Předpokládané náklady

Ať už dodavatel přijde s návrhem projektu, nebo sám zákazník bude požadovat zpracování takového návrhu, vždy nabídka musí obsahovat alespoň orientační cenovou kalkulaci. Kalkulace slouží nejen jako podklad pro výběrová řízení, ale také zákazníkovi jako orientační suma, kterou bude muset za vykonaný materiál a služby zaplatit.

Předpokládané náklady bez DPH dle jednotlivých komponent:

- EZS 249 334,-Kč
- Čidla rozbití skel 115 134,-Kč
- Detektory kouře 264 000,-Kč
- Detektory plynu 242 000,-Kč
- LED osvětlení 535 334,-Kč
- Čtečky karet 336 747,-Kč
- RFID 4 950,-Kč
- Kamerový systém 293 334,-Kč
- Bezpečnostní okna 164 835,-Kč

V rámci předběžné kalkulace činí **celková suma 2 108 398,- Kč bez DPH**, **se sazbou 21% činí částka 2 668 858,- Kč s DPH.**

Orientační cenová kalkulace je podrobněji rozepsána v příloze 58.

Závěr

Cílem diplomové práce bylo zabezpečení výukového střediska zaměřeného na výzkum v chemickém průmyslu ve speciálně vybavených laboratořích. Tento objekt bude disponovat také restauračním provozem a hotelem. V tomto objektu se tedy budou pohybovat i návštěvníci, kteří by mohli mít v úmyslu poškození tohoto výzkumu. Proto je nezbytné, abychom se důkladně zaměřili na bezpečnost. Nejde však jen o úmyslné či neúmyslné poškození zvenčí, ale také ze strany zaměstnanců či manažerů.

V této práci navrhuji po technické stránce rozmístění komponent, které jsou znázorněny v přiložených přílohách pro zabezpečení objektu. Níže jsou shrnuty požadavky investora:

Požadavek	**Umístění po celém areálu**
EZS	✓
Detektor kouře a plynu	✓
Nouzové LED osvětlení	✓

Požadavek	**Umístění v přízemí**
Bezpečnostní okna	✓
Čidla rozbití skel	✓
Kamerový systém	✓

Požadavek	**Umístění – vybrané dokumenty**
Zabezpečení dokumentů	✓

Nejslabším článkem jsou lidé, proto je nutností, abychom nastavili každému manažeru, zaměstnanci i návštěvníkovi jeho specifická práva, o kterých budou rozhodovat příslušní manažeři a zaměstnanci zabývající se výzkumem. Nepůjde však jen o nastavení práv na kartách. Musíme se také zaměřit na nastavení dostatečně silných hesel a jejich pravidelné změně. Následně i o případném uložení budou zaměstnanci a manažeři proškoleni na příslušných školeních. Školení rozděluji na všechny

zaměstnance, kde bude rozebrán i význam takovéhoto zabezpečení a základní pojmy a další dodatečná školení, která jsou přidělena podle jednotlivých pracovních pozic. Řazeni jsou do nich i žáci absolvující školení.

V rámci projektu jsem zpracovala orientační cenovou kalkulaci, jejíž částka činí 2 668 858,- Kč s DPH.

Investor požaduje nepřekročení částky 2 500 000,- Kč s DPH. Vypočtená cenová kalkulace převyšuje tuto požadovanou částku investorem, ale v tomto případě se jedná o orientační cenu, kde mám zahrnutou i rezervu. Není možné v tuto chvíli říci, zda požadovaná částka bude na konci projektu dodržena, nebo překročena.

I když jsou obě tyto částky poměrně vysoké, únik informací do nepovolaných rukou, nebo narušení výzkumu by mohlo v konečném důsledku překročit i tuto částku investovanou do zabezpečení objektu. Majiteli objektu by tím hrozila také ztráta dalších potencionálních zákazníků, kteří by si chtěli toto místo pro svoje účely v budoucnosti pronajmout.

Majitelé se rozhodli, že budou požadovat vydání certifikátu, kterým budou moci prokazovat svoji schopnost trvale uplatňovat bezpečnostní opatření s cílem poskytnout svým zákazníkům a partnerům jistotu o úrovni zabezpečení.

Použitá literatura

(1) *Kybernetická bezpečnost* [online]. 2010-2013 [cit. 2013-10-15]. Dostupné z: http://cybersecurity.cz/

(2) SEDLÁK, P. Informační management. Přednášky. Brno: VUT Fakulta podnikatelská, 2013.

(3) CLEVERANDSMART. Analýza rizik: Jemný úvod do analýzy rizik. *cleverandsmart.cz* [online]. © 2008 – 2014 [cit. 2013-10-30]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

(4) MALINKA, K. Manažerská informatika. Přednášky. Brno: VUT Fakulta podnikatelská, 2010.

(5) DOUCEK P., NOVÁK L., NEDOMOVÁ L. a SVATÁ V. *Řízení bezpečnosti informací: 2. Rozšířené vydání o BCM*. Praha: Professional Publishing, 2011. ISBN: 978-80-7431-050-8.

(6) KNÝ M., POŽÁR J. *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti.* Brno: Tribun EU 2010. ISBN: 978-80-7399-067-1.

(7) POŽÁR J. Základy teorie informační bezpečnosti informací. Praha: Professional Publishing, 2007. ISBN: 978-80-7251-250-8.

(8) ONDRÁK V., SEDLÁK P., MAZÁLEK V. *Problematika ISMS v manažerské informatice.* Brno: CERM, 2014. ISBN: 978-80-7204-784-0

(9) RAC – Infocentrum [online]. © 2014 [cit. 2014-02-13]. Dostupné z: http://www.rac.cz/

(10) Bezpečnostní kostka - seriál o ISMS. *chrantesidata.cz* [online]. 2008 [cit. 2014-22-02]. http://www.chrantesidata.cz/cs/art/1146-isms/

(11) *DCIT, a.s. – konzultační a auditorské služby v IT* [online]. © 2013 [cit. 2014-13-02]. Dostupné z: http://www.dcit.cz/

(12) Národní centrum kybernetické bezpečnosti [online] 2014 [2014-03-01]. Dostupné z: http://www.govcert.cz/cs/

(13) Návrh vyhlášky ze dne 21.2.2014 o bezpečnostních opatření, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

(14) Kamerové systémy – Zabezpecovacky.cz [online] © 2007 – 2014 [2014-03-03]. Dostupné z: http://www.zabezpecovacky.cz/

(15) Národní bezpečnostní úřad – Informace pro žadatele o doklad o bezpečnostní způsobilosti fyzické osoby z důvodu výkonu citlivé činnosti dle zákona č. 229/2013 Sb. (zákon o nakládání s bezpečnostním materiálem) *nbu.cz/cs* [online] 2013 [cit. 2014-03-01]. Dostupné z: http://www.nbu.cz/cs/aktuality/1956-informace-pro-zadatele-o-doklad-o-bezpecnostni-zpusobilosti-fyzicke-osoby-znduvodu-vykonu-citlive-cinnosti-dle-zakona-cn2292013-sb-zakon-o-nakladani-s-bezpecnostnim-materialem/

(16) Druhy a typy RFID štítků | Combitrading *combitrading.cz* [online] 2014 [cit. 2014-03-02]. Dostupné z: http://www.combitrading.cz/technologie/druha-a-typy-rfid.html

(17) Přístupové systémy *z-ware.cz* [online] 2006-2008 [cit. 2014-03-02]. Dostupné z: http://www.z-ware.cz/?28-pristupove-systemy

(18) *Zabezpečovací technika a zastoupení firmy Jablotron alarms a.s*. [online]. © 2014 [cit. 2014-02-24]. Dostupné z: http://www.etechcz.com/

(19) *Bezpečný internet.cz* [online] 2014 [cit. 2014-03-07]. Dostupné z: http://www.bezpecnyinternet.cz/

(20) *Institut celoživotního vzdělávání VUT v Brně (dříve Centrum vzdělávání a poradenství)* [online] © 2000–2014 [cit. 2014-03-08]. Dostupné z: http://www.lli.vutbr.cz/

(21) *Profesní vzdělávání - TUTOR - Profesní kurzy a semináře* [online] © 2000 – 2014 [cit. 2014-03-08]. Dostupné z: http://www.tutor.cz/skoleni-seminare/?ref=topmenu

(22) ČESKÝ NORMALIZAČNÍ INSTITUT ČSN ISO 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky.* Praha: Český normalizační institut, 2006. 36 s. Třídící znak: 369790

(23) Podmínky provedení - EURO CERT CZ eurocert.cz [online] 2014 [cit. 2014-03-07]. Dostupné z: http://www.eurocert.cz/certifikace/cz/podminky-provedeni

(24) ČESKÝ NORMALIZAČNÍ INSTITUT ČSN ISO 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.* Praha: Český normalizační institut 2005.

(25) DOBDA L. *Ochrana dat v informačních systémech.* Praha: Grada Publishing, 1998. ISBN: 80-716-9479-7.

(26) POŽÁR J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN: 80-86898-38-5.

Seznam obrázků

Seznam obrázků - přílohy

Seznam tabulek

Seznam tabulek - přílohy

Seznam zkratek

ANSI (American National Standards Institute) – americký státní normalizační institut

BCM (Business Continuity Management) – řízení kontinutity činností

BCMS (Business Continuity Management System) – systém řízení kontinuity organizace

BOZP – bezpečnost a ochrana zdraví při práci

BP – bezpečnostní politika

BSI (British Standard Institute) – britský standardizační institut

CEN (Comité Européen Normalisation) – evropský výbor pro normalizaci

CENELEC (Comité Européen de Normalisation Eléctrotechnique) – evropský výbor pro technologickou normalizaci

CF – certifikace

COBIT (Control Objectives for Information and Related Technology) – metodika (Je považována za soubor těch nejlepších praktik pro řízen informatiky)

CRAMM (CCTA Risk Analysis and Management Method) – metodika pro řízení rizik

ČSNI – český normalizační institut

DIN (Deutches Institut für Normung) – německý úřad pro normování

DR plán – plán obnovy po havárii

EMS (environmental MS) – systém řízení vztahu k okolí

EPS – elektronický požární systém

ETSI (European Telecommunications Standards Institute) – institut

EZS (Electrical security signaling) – elektronický zabezpečovací systém

FRAP (Faciliated Risk Analysis Process) – otevřená komunikace mezi oběma stranami

FTP – Foil Shielded Twisted Pair

HR – personalistika

HW – hardware

ICT (Information and Communication Technologies) – informační a komunikační technologie

IEC (International Electrotechnical Comission) – mezinárodní elektrotechnická komise

IMS (integrated MS) – integrovaný systém řízení

IP (Internet Protocol) – internetový protokol

IS (Information System) – informační systémy

ISMS (Information Security Management System) – systém řízení informační bezpečnosti

ISO (International Organization for Standardization) – mezinárodní organizace pro standardizaci

ISO/OSI model – sedmivrstvý referenční komunikační model podle něhož dochází k propojování systémů

IT (Information Technology) – informační technologie

ITIL (Information Technology Infrastructure Library) – knihovna (poskytuje ucelený soubor pro řízení služeb IT)

ITSM (IT Service Management) – řízení služeb informačních technologií

ITU (International Telecommunications Union) – mezinárodní telekomunikační unie telekomunikačních norem

OHASMS – ochrana a bezpečnost zdraví při práci

PDCA model – Demingův model, pro životní cyklus IMS se zpětnou vazbou

PIR – PIR čidla

PO – požární ochrana

QMS (quality MS) – systém řízení kvality

RFID (Radio Frequency Identification) – identifikace na rádiové frekvenci

SW – software

TR – technické zprávy

TS – technická specifikace

TTA – dohody o technických trendech

UPS (Uninterruptible power supply) – záložní zdroj

Seznam příloh

Příloha 1

Tabulka 2: Přehled místností prvního nadzemního podlaží
Zdroj: Vlastní zpracování

Tabulka místností prvního nadzemního podlaží			
Číslo místnosti	**Popis místnosti**	**Číslo místnosti**	**Popis místnosti**
101	Schodiště	**123**	Venkovní terasa
102	Chodba	**124**	Venkovní terasa
103	Kancelář	**125**	Chodba
104	Kancelář	**126**	Schodiště
105	Chodba	**127**	Restaurace 40-50 míst
106	Zkušební laboratoř	**128**	Kiosek
107	Chodba	**129**	Bar
108	Ústředna EPS	**130**	Sklad
109	Sklad náhradních dílů	**131**	Sklad obalů
110	Přípravna surovin	**132**	Sklad nápojů
111	Chodba	**133**	Kuchyně
112	Silnoproud	**134**	Umývárna nádobí
113	Kotelna - technologie	**135**	Chodba
114	Silnoproud	**136**	Úklid
115	WC invalidé	**137**	Odpadky
116	Úklid	**138**	Kancelář
117	WC muži - předsíň	**139**	Sklad a hrubá přípravna zeleniny
118	WC muži	**140**	Sklad suchých potravin
119	WC ženy - předsíň	**141**	WC + umývárna - personál
120	WC ženy	**142**	Šatna personál
121	Kotelna - domovní	**143**	Venkovní terasa
122	Vstupní hala a recepce		

Tabulka 3: Přehled místností druhého nadzemního podlaží
Zdroj: Vlastní zpracování

Tabulka místností druhého nadzemního podlaží			
Číslo místnosti	**Popis místnosti**	**Číslo místnosti**	**Popis místnosti**
201	Schodiště	**215**	WC muži
202	Chodba	**216**	Sklad
203	Sprchy	**217**	WC invalidé
204	WC	**218**	WC ženy - předsíň
205	Kuchyňský kout	**219**	WC ženy
206	Šatna + denní místnost	**220**	Chodba
207	Chodba	**221**	Schodiště
208	Provozní plošina	**222**	Kancelář
209	Laboratoř	**223**	Kancelář
210	Fermentace	**224**	Kancelář
211	Chodba	**225**	Kancelář
212	Hala	**226**	Kancelář
213	Posluchárna	**227**	Kancelář
214	WC muži - předsíň	**228**	Kancelář

Tabulka 4: Přehled místností třetího nadzemního podlaží
Zdroj: Vlastní zpracování

Tabulka místností třetího nadzemního podlaží			
Číslo místnosti	**Popis místnosti**	**Číslo místnosti**	**Popis místnosti**
301	Schodiště	**328**	WC muži - předsíň
302	Chodba	**329**	WC ženy - předsíň
303	Vchod	**330**	Sklad prádla
304	Předsíň + šatna	**331**	WC muži
305	Koupelna + WC	**332**	WC ženy
306	Kuchyňský kout	**333**	Chodba
307	Obytný prostor	**334**	Schodiště
308	Předsíň	**335**	Šatna
309	Šatna	**336**	Předsíň
310	Koupelna + WC	**337**	Koupelna + WC
311	Kuchyňský kout	**338**	Kuchyňský kout
312	Obytný prostor	**339**	Obytný prostor
313	Předsíň	**340**	Předsíň

314	Šatna	**341**	Šatna
315	Koupelna + WC	**342**	Koupelna + WC
316	Kuchyňský kout	**343**	Kuchyňský kout
317	Obytný prostor	**344**	Obytný prostor
318	Koupelna	**345**	Předsíň
319	WC	**346**	Šatna
320	Předsíň + šatna	**347**	Koupelna + WC
321	WC	**348**	Kuchyňský kout
322	Kuchyňský kout	**349**	Obytný prostor
323	Obytný prostor	**350**	Předsíň
324	Chodba	**351**	Chodba + Šatna
325	Chodba	**352**	Koupelna + WC
326	Společenská místnost	**353**	Kuchyňský kout
327	Společenská místnost	**354**	Obytný prostor

Tabulka 5: Přehled místností čtvrtého nadzemního podlaží
Zdroj: Vlastní zpracování

Tabulka místností čtvrtého nadzemního podlaží			
Číslo místnosti	**Popis místnosti**	**Číslo místnosti**	**Popis místnosti**
401	Chodba	**427**	Ložnice
402	Schodiště	**428**	Koupelna + WC
403	Předsíň	**429**	Technická místnost
404	Chodba + šatna	**430**	Technická místnost
405	Koupelna + WC	**431**	Chodba
406	Kuchyňský kout	**432**	Schodiště
407	Obytný prostor	**433**	Šatna
408	Šatna	**434**	Předsíň
409	Předsíň	**435**	Koupelna + WC
410	Koupelna + WC	**436**	Kuchyňský kout
411	Kuchyňský kout	**437**	Obytný prostor
412	Obytný prostor	**438**	Šatna
413	Předsíň	**439**	Předsíň
414	Koupelna + WC	**440**	Koupelna + WC
415	Kuchyňský kout	**441**	Kuchyňský kout
416	Obytný prostor	**442**	Obytný prostor
417	Sklad špinavého	**443**	Šatna

	prádla		
418	Předsíň	**444**	Předsíň
419	Koupelna + WC	**445**	Koupelna + WC
420	Kuchyňský kout	**446**	Kuchyňský kout
421	Obytný prostor	**447**	Obytný prostor
422	Chodba	**448**	Předsíň
423	Předsíň	**449**	Chodba + šatna
424	Kuchyň + jídelna	**450**	Koupelna + WC
425	Komora	**451**	Kuchyňský kout
426	Obývací pokoj	**452**	Obytný prostor

Příloha 2

Nastavení práv

Čipové karty budou používány po celém areálu výukového centra. Omezíme tím nežádoucí přístupy do konkrétních oblastí. Ať už nově příchozímu hostu nebo stálému zaměstnanci není obtížné přiřadit oprávnění, která se mohou v průběhu změnit. Toto řešení zjednodušuje variantu, kdy bude potřeba ať už přidání či odebrání práv.

Krádeži či ztrátě čipové karty nezamezíme, avšak nastane-li tato situace, poškozený musí ihned po zjištění ztráty tuto skutečnost nahlásit, aby byla karta co nejdříve zablokována.

Základní čipové karty a jejich nastavení práv dle rozdělení jsou vypsány níže. Pro všechny budou vypsána jak základní práva, která budou na začátku nastavena, tak rozšíření práv, které musí projít schválením. V omezení nalezneme zakázané oblasti, kam daná osoba nesmí mít přístup. I přesto může požádat o rozšíření práv, avšak záleží na vedení každé oblasti střediska, která zodpovídá za svoji činnost, zda toto přidání práva povolí.

Nastavení práv vedení

- vedení má nastaveno základní právo do všech oblastí výukového střediska, až na technologickou zónu, kde probíhá výzkum, sklad, příprava surovin, fermentace. Na pracovní plošinu a do laboratoře je přístup také přísně zakázán. Taktéž nesmí bez povolení vstupovat do kotelny a místností se silnoproudými a slaboproudými rozvody.
- z důvodu bezpečnosti, nesmí ani vedení bez specializované osoby vstupovat do těchto místností, a tedy si přiřadit práva.

Nastavení práv zaměstnanců

zaměstnanci ve stravovacím zařízení

- zaměstnanci pro tuto celou oblast mají přiřazena základní práva. Základní práva jsou také pro přednáškový sál a společenské místnosti z důvodu nachystání občerstvení.
- další práva nejsou přiřazena

zaměstnanci v oblasti IT

- zaměstnancům jsou v základních právech přiřazené technické místnosti, EPS, kanceláře a společenské místnosti
- v případě havárie v technologických zónách pro výzkum, je přístup možný za doprovodu příslušné osoby
- do zadní části stravovacího zařízení je potřeba přiřazení práv

zaměstnanci spravující – elektro, plyn, voda

- přístup do technických místností na základě domluvy se specialisty z oboru IT, kotelny, restaurace, kanceláří a společenské místnosti
- v případě havárie v technologických zónách pro výzkum, je přístup možný za doprovodu příslušné osoby
- do zadní části stravovacího zařízení je potřeba přiřazení práv

pokojské

- přístup je možný do restaurace, obytných prostor, společenské místnosti, posluchárny, úklidu a kanceláří. Do prostor pro výzkum je možné pouze do prostor, které jsou volně přístupné (haly, WC, kuchyňské kouty). Kanceláře v technologické zóně jsou pro pokojské nepřípustné.

recepční

- základní práva jsou přiřazena do restaurace, obytných prostor, společenské místnosti a posluchárny

školitelé

- školitelé musí podepsat na recepci prohlášení o zachování mlčenlivosti a zákazu využívání nabitých znalostí pro soukromé účely
- práva jsou přiřazena do obytných prostor, restaurace, společenské místnosti, přednáškového sálu, pracovní plošiny, laboratoře a zkušební laboratoře
- na základě potřeby je možné rozšíření o místnost, kde se provádí fermentace, sklad náhradních dílů a přípravny surovin
- ostatní práva jsou omezená a přístup do ostatních prostor musí být důkladně zvážen a projít schválením více příslušných osob

zaměstnanci pro výzkum

- zaměstnanci zabývající se výzkumem musí podepsat na recepci prohlášení o zachování mlčenlivosti a zákazu využívání nabitých znalostí pro soukromé účely
- práva jsou přiřazena do obytných prostor, restaurace, společenské místnosti, přednáškového sálu, pracovní plošiny, laboratoře, zkušební laboratoře, skladu náhradních dílů, přípravny surovin a prostor, v nichž se provádí fermentace
- ostatní práva jsou omezená a přístup do ostatních prostor musí být důkladně zvážen a projít schválením více příslušných osob

úředníci a HR pracovníci

- základní přístup je povolen do restaurace, kanceláří a společenské místnosti
- na žádost je možné bez zvláštních schválení povolit přístup do posluchárny
- do všech ostatních prostor by muselo další přiřazení práv projít přísným zvážením a schválením více příslušných osob

hoteloví hosté

- hoteloví hosti mají přístup pouze do obytné oblasti, společenské místnosti a restaurace
- není možné, aby hoteloví hosti měli či dostali přístup do ostatních oblastí, pokud neprobíhá školení v posluchárně, kam jsou v tomto případě práva rozšířena

studenti pro výzkum a školení

- studenti musí podepsat na recepci prohlášení o zachování mlčenlivosti a zákazu využívání nabitých znalostí pro soukromé účely
- práva jsou přiřazena do obytných prostor, restaurace, společenské místnosti, přednáškového sálu, pracovní plošiny, laboratoře a zkušební laboratoře
- na základě potřeby je možné rozšíření o místnost, kde se provádí fermentace, sklad náhradních dílů a přípravny surovin
- ostatní práva jsou omezená a přístup do ostatních prostor musí být důkladně zvážen a projít schválením více příslušných osob

návštěvy

- za návštěvu jsou považovány osoby, které nejsou ubytováni a jdou navštívit stravovací zařízení, kde je automaticky přiřazeno toto základní právo
- pokud za ubytovaným hostem přijde návštěva a bude-li chtít jít na pokoj, je nezbytné, aby byla na recepci nahlášena a odevzdala občanský průkaz. V tomto případě se práva návštěvě rozšíří o obytný prostor.
- pokud jsou ve středisku organizována školení a zúčastnění nejsou ubytováni, rozšíření práv se povolí na posluchárnu či společenskou místnost
- žádné další přiřazení práv není možné. Pokud je k tomu závažný důvod, je potřeba zažádat o toto rozšíření dopředu, neboť musí projít důkladným šetřením a schválením více než jedné oprávněné osoby.

Kvalita hesel a jejich pravidelná změna

Zaměstnanci a studenti budou muset ve výukovém středisku co nejvíce chránit citlivé informace. Proto je zde důkladně řešena kvalita hesel a jejich pravidelná změna. Zaměstnanci i studenti budou proškoleni i na toto téma. Tato kapitola se bude zabývat tím, jaké jsou nesprávné metody při vytváření hesel, jak vypadá silné heslo a jakým způsobem jej můžeme například vytvořit. Poté se budeme věnovat přístupu hesel a důležitou pravidelnou změnou hesla. (19)

Nesprávné metody při vytváření hesla

Mnoho lidí, ať už pro soukromé účely, nebo naopak zaměstnanci, ve velkých korporátních firmách používají hesla, která jsou snadno odhalitelné zločinci. Snadno uhodnutelným heslům se můžeme vyhnout následovným způsobem: (19)

- nepoužívat řadu čísel nebo písmen a to ani zpětnou, nepoužívat opakující se znaky
    - bezpečné heslo nevytvoříme například řadou: 123456789, abcdefg, aaaaaa, atd.
    - na internetu jsou často vystavovány statistiky používání nejčastějších hesel, do nichž se právě tato skupina řadí
- nenahrazovat čísla a symboly podobnými znaky

    - nahrazování čísel a symbolů nezastaví zločince, kteří mají mnoho zkušeností
    - takováto nahrazování mohou být však účinná se spojením dalších opatření, která zvyšují bezpečnost hesel
- nepoužívat hesla ze slovníku v žádném jazyce
    - pro odhalení hesel se v dnešní době využívá propracovaných nástrojů. S nimi není problém odhalit heslo vytvořené na základě slov obsažených ve slovnících a to i pozpátku, obsahující běžné pravopisné chyby a nahrazení. Patří sem i nespisovná a neslušná slova.
- nepoužívat na všech místech stejná hesla
    - napadne-li útočník jeden z počítačů nebo on-line systémů, je v tomto případě ohrožena bezpečnost všech dalších údajů
    - v rámci fyzické bezpečnosti při používání jednotného hesla je z klávesnice značné, která písmena se používají nejčastěji
- nepoužívat online ukládání
    - objeví-li uživatelé se zlými úmysly hesla uložená on-line nebo v počítači zapojeném v síti, získají tak přístup ke všem našim údajům
- délka hesla
    - ve výukovém středisku zaměřeném na výzkum se za nedostatečné heslo považuje i heslo kratší než 12 znaků

Vytvoření silného hesla

Jak již bylo zmíněno, požaduje se od zaměstnanců a studentů používání silných hesel. Existuje mnoho způsobů jak silné heslo vytvořit a na některé z nich se podíváme níže: (19)

1) Vymyslet větu nebo událost, která je nám blízká a snadno zapamatovatelná
    - tato věta či událost bude následně tvořit základ složitého hesla
    - doplníme následně o znaky a číslice, které mohou jednotlivá slova spojovat či číslice nahrazovat jednotky
2) Náhodné vygenerování systémem
3) Vlastní náhodné generování

Pro výše zmíněné možnosti je nutné: (19)

Kombinovat – heslo nebude přijato, pokud nebude obsahovat alespoň jedno písmeno, jednu číslici a jeden znak

Stanovit délku hesla – pro výše zmíněné vytvoření hesel je povinnost v tomto systému mít minimální délku hesla 12 znaků

Přístup k heslům

Hesla, která používáme ať už pro soukromé účely nebo v zaměstnání, je potřeba chránit a neposkytovat je dalším osobám. Více o této tématice je uvedeno v příslušné kapitole: (19)

1) Hesla neprozrazovat dalším osobám
    - hesla nesdělovat dalším osobám, ani nejbližším příbuzným či přátelům v zaměstnání. Takováto informace je dále snadno šiřitelná, především při objevení dětmi, které nejen mohou heslo předat dále, ale mohou se přihlásit k účtu a dostat se k citlivým informacím, které se tak mohou dostat k neoprávněným osobám.
2) Neposkytovat hesla pomocí e-mailu nebo v odpovědi na e-mailovou žádost
    - e-mail který žádá o heslo nebo ověření hesla na webu je s největší pravděpodobností podvodný. Do této kategorie spadají i žádosti od důvěryhodných společností a osob.
    - e-mail lze při přenosu zachytit a nemusí pocházet nebo nemusí dojít uvedenému žadateli
    - v dnešní době se využívá také zasílání nevyžádaných zpráv za účelem vylákání osobních údajů a tak z nich podvodníci získají uživatelská jména a hesla, čímž dojde ke ztrátě identity
3) Ochrana hesel
    - hesla, která jsou obtížně zapamatovatelná, si mnoho lidí napíše na papír a někam uschová. V horším případě je nechá vystavené u počítače na očích dalších lidí. Toto řešení není ve výukovém středisku možné a bude penalizováno za nedodržování ochrany hesel.

- zaměstnanci a studenti jsou povinni si tyto citlivé informace buď pamatovat, anebo uschovat na bezpečném místě, kam nemají přístup ostatní.

4) Nezadávat hesla na počítačích, nad nimiž nemáme kontrolu
    - internetové kavárny, sdílené systémy, konferenční místnosti, letiště a další veřejná místa nejsou vhodné pro osobní natož pracovní využití. Tyto počítače nejsou vhodné k tomuto užití, neboť zločinci mohou snadno získat informace k pracovní či soukromé poště, bankovnímu účtu a podobně. Toto je možné právě již zmíněným zařízením, které zaznamenává úhozy a není vůbec těžké ho na veřejném místě nainstalovat.

Změna hesla

Heslo ve výukovém středisku musí být v délce minimálně 12-ti znaků. Bylo vedením a několika příslušnými osobami stanoveno, že automaticky bude žádost pro změnu hesla přicházet uživatelům i vedení 1x za 3 měsíce. Systém automaticky nebude povolat změnu hesla, která bude obsahovat heslo původní. (19)

Zákaz činností

Zaměstnanci a studenti nesmí v době své pracovní činnosti využívat webové stránky k těmto účelům:

- sociální sítě
- erotické stránky
- seznamky
- online sledování filmů a seriálů
- stahování k soukromým účelům

Zákaz činností může být v průběhu let doplněn, neboť se nejen obor IT neustále vyvíjí, ale lidé jsou čím dál více vynalézavější.

Postihy za nedodržování pravidel

Neexistovaly by žádné postihy za nedodržování pravidel, nikdo by tato pravidla nedodržoval. Protože ve výukovém středisku probíhá také výzkum v chemickém průmyslu, jsou postihy za nedodržování předpisů přísnější, i když se v méně závažných případech snažíme dát ještě jednu šanci, neboť lidé nejsou neomylní. V této kapitole jsou základní postihy za nedodržování pravidel, které mohou být časem rozšířeny a doplněny.

Nenahlášení ztráty čipové karty

Nenahlásí-li zaměstnanec či student ztrátu čipové karty, bude mu sníženo platové ohodnocení a celkové hodnocení zaměstnance či studenta. V případě, že ztráta čipové karty nebude nahlášena a dojde ke škodě ve výukovém středisku, bude muset poškozenému zaplatit v případě citlivých informací polovinu ceny ze vzniklé škody. Je-li zaměstnanec po delší dobu nepřítomnosti na středisku a tedy nezjistil by tuto ztrátu včas, bude tato situace řešena individuálně.

Zneužití čipové karty

Nalezne-li zaměstnanec či student čipovou kartu, která mu nepatří, je povinen ji odevzdat na recepci. Pokud je zjištěno zneužití této čipové karty a bude-li mít zaměstnanec či student uzavřený pracovní poměr, ihned s ním bude rozvázán. Navíc podle škody, kterou způsobil, bude možná i žaloba. Nebude-li v pracovním poměru, bude vykázán ze střediska a podle škody, která byla způsobena, je možné zažalování.

Porušení zákazu činností

Zaměstnanci i studenti mají vybraný zákaz činností, které nesmí provádět ve své pracovní době jak na privátní, tak i na veřejné síti. Tyto postihy jsou zpočátku řešeny pokáráním, následně snížením platu a na celkovém ohodnocení. Je-li tento zákaz činnosti porušován i nadále a na zaměstnance či studenta již zmíněné postihy neplatí a má-li uzavřený pracovní poměr, je možné jej rozvázat. Nemá-li uzavřen pracovní poměr, bude ze střediska vykázán.

Pozn.: Na privátní síti jsou větší sankce a vyšší možnost ukončení pracovního poměru.

Nastavení práv bez povolení

V případě, že recepční rozšíří práva do oblastí, kam by dotyčná osoba žádající toto přidání neměla mít přístup bez povolení vedení a příslušných osob, je postih rozdělen.

Přiřadí-li práva do oblastí, kde jsou tajné informace či stravovací zařízení, bude jí odejmut pracovní poměr. Jestli-že práva přiřadí do oblastí, kde tajné informace uschovány nejsou a kde se nepracuje se surovinami, bude poprvé pokárána a sníží se platové i osobní ohodnocení. Nastala by tato situace podruhé, bez ohledu na oblast přidání práv, bude jí ukončen pracovní poměr.

Nesplnění zachování mlčenlivosti

V případě, že zaměstnanec nebo student, který podepsal prohlášení o mlčenlivosti, toto pravidlo poruší, za každé jednotlivé porušení činnosti zaplatí ¾ ceny z ušlého zisku. Je-li zaměstnanec či student zavázán pracovním poměrem, bude mu k tomuto dni ukončen pracovní poměr bez nároku na odškodné.

Poruší-li zaměstnanec či student prohlášení o mlčenlivosti u více jak jedné činnosti, a je-li zaměstnanec či student zavázán pracovním poměrem, bude mu k tomuto dni ukončen pracovní poměr bez nároku na odškodné. Na tomto základě musí vyplatit poškozenému 1 a půl násobek ceny z celkové škody.

Využívání nabitých znalostí pro soukromé účely

Poruší-li zaměstnanec či student podepsané prohlášení o zákazu využívání jejich nabitých znalostí pro soukromé účely, ať už k výdělečné činnosti nebo bez ní, a je-li zavázán pracovním poměrem, bude mu k tomuto dni ukončen pracovní poměr bez nároku na odškodné.

V případě využívání nabitých znalostí pro soukromé účely bez výdělečné činnosti, musí toto využívání neprodleně ukončit a zaplatit poškozenému plnou částku z ušlého zisku.

V případě využívání nabitých znalostí pro soukromé účely k výdělečné činnosti, musí toto využívání neprodleně ukončit a zaplatit poškozenému, plnou částku, kterou touto výdělečnou činností získal a z ušlého zisku.

Porušení ochrany hesla

Předání hesla jiné právnické či fyzické osobě

Je-li zjištěno, že zaměstnanec či student předali heslo neoprávněné osobě pro přístup, bude nejdříve pokárán a bude mu sníženo jak platové tak celkové ohodnocení. Ihned si musí heslo změnit.

Pokud není zjištěna škoda, dotyčná osoba nemusí nic uhradit, avšak v případě zpětného zjištění, je povinen tuto škodu uhradit zpětně za 5 let od této události.

Dojde-li ke zjištění předání hesel podruhé a je-li v pracovním poměru, bude mu na místě pracovní poměr ihned ukončen. Nebude-li v pracovním poměru, bude muset tuto situaci řešit jeho nadřízený, který jej může vykázat ze střediska.

Zaznamenání hesla není bezpečně uloženo

V případě uchování si hesel, zaměstnanec i student, mají povinnost uchovávat hesla na místech, kam nemají přístup ostatní. Je-li zjištěno, že toto pravidlo je porušeno, a hesla jsou uchovávána například na stolech, přilepené na počítači či na jakémkoli jiném viditelném místě, bude nejdříve pokárán. Nastane-li tato situace podruhé, bude pokárán znovu a bude mu sníženo platové hodnocení a celkové hodnocení zaměstnance. Zjistí-li se, že opakovaně přes tato dvě napomenutí nedošlo ke změně, je možné diskutovat o propuštění zaměstnance či studenta je-li v pracovním poměru. Nebude-li student v pracovním poměru a nebude dodržovat pravidla, záleží na jeho nadřízeném, zda student nebude moci pokračovat ve vykonávání této činnosti, nebo bude i nadále součástí týmu. Taktéž v pravomoci nadřízeného bude jaká opatření a jaké postihy budou studentovi přiřazeny.

Příloha 3

Základní školení pro všechny zaměstnance

Základní školení pro zaměstnance a vedení výukového střediska bude probíhat v průběhu pracovního poměru 1x za rok. Před vznikem pracovního poměru je důležité, aby zaměstnanci a především pracovníci smluvních a třetích stran byli srozuměni se svými povinnostmi a právy. Při nástupu jsou nařízena základní školení BOZP a PO. V rámci těchto školení proběhne základní školení do problematiky ISMS a zavedených pravidel na středisku.

V základním školení budou posluchači seznámeni s pojmem bezpečnost, ISMS, PDCA model a základními pojmy. Bude zde probírána základní bezpečnostní politika a také změny, které nastanou. Posluchači se dozví o nejčastějších chybách v rámci výukového střediska, kde probíhá výzkum a na závěr si ověří své získané znalosti.

Bezpečnost

Pod pojmem bezpečnost IT obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich jak uchovány, zpracovány, tak přenášeny. Součástí je i komunikační bezpečnost, kterou rozumíme ochranu informace přenášení mezi počítači a dále fyzickou bezpečnost. Tento pojem je pak označován jako ICT. ICT znamená pro primární business nepostradatelnou složku. V dnešní době máme velké množství různých ochranných a obranných nástrojů SW či HW. (10)

Postupem času se pak zjistilo, že největším rizikem se stávají vlastní zaměstnanci. Jedním z nejúčinnějších opatření je nasazení jasných a přesných bezpečnostních pravidel opírajících se o standardy. (10)

Nejrozšířenějším celosvětově uznávaným standardem, který je určený k zavedení systému řízení bezpečnosti je právě ISMS, který bude popsán v druhé části. (10)

Pojem ISMS, model PDCA a přínosy

ISMS je soubor pravidel a opatření, po jejichž zavedení má úplné a správné informace včas k dispozici ten, kdo je skutečně potřebuje a pouze ten, kdo je k přístupu oprávněn. Zahrnuje část celkového systému řízení organizace, založen na přístupu organizace k rizikům činností. (1)

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv. Jeho cílem je eliminovat možnou ztrátu nebo poškození tím, že určíme aktiva, která se mají chránit. Zvolíme a řídíme možná rizika bezpečnosti informací, zavedeme opatření s požadovanou úrovní záruk a tak kontrolujeme. (1)

Je zaměřen na ustanovení, zavádění a provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. (1) Tímto se dostáváme k modelu PDCA.

PDCA model

Principem celého ISMS je tzv. PDCA model, který je znázorněn na obrázku č. 17.

Obrázek 17 – PDCA model
Zdroj (10)

Cyklus PDCA zavádí kontinuální systém řízení bezpečnosti informací v organizaci. Zaručuje, že zavedení systému nebude jen jednorázovou aktivitou, ale neustálým koloběhem. Vyznačuje se čtyřmi kroky: Plánuj, dělej, kontroluj a jednej. (10) Detailní problematika PDCA modelu je uvedena v kapitole 1.2.

Základní pojmy

Ze základních pojmů je potřeba se zaměřit minimálně na následující: (1; 10)

- ISMS
- PDCA model
- IT vs. ICT
- Informace vs. data
- Informační systém
- Bezpečnost organizace, IS/ICT a informací
- Aktivum
- Analýza rizik
- Bezpečnostní organizační opatření
  - systém řízení bezpečnostních informací
  - řízení rizik
  - organizační bezpečnost
  - stanovení bezpečnostních požadavků pro dodavatele
  - řízení aktiv
  - zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Bezpečnostní technická opatření
  - fyzická bezpečnost
  - nástroj pro ochranu integrity komunikačních sítí
  - nástroj pro ověřování identity uživatelů
  - nástroj pro řízení přístupových oprávnění
- Autentizace a autorizace
- Audit
- Certifikační problematika

Aktuální bezpečnostní politika

Aktuální bezpečnostní politika se bude zaobírat bezpečností objektu, jako je implementace EZS, EPS, čidel rozbití skel, kamerového systému, nouzového LED osvětlení a čteček karet.

Ke každému bodu bude objasněn důvod zavedení, jeho nastavení a stav. Problematika čteček karet bude navíc rozšířena o nastavení práv, která jsou uvedena v kapitole 3.1. Dalšími oblastmi bude nastavení hesel – jejich kvalita a obměna, zákaz činností na pracovišti a neméně důležité postihy za nedodržování pravidel. Tyto oblasti jsou uvedeny ve stejné kapitole 3.1. – nastavení práv.

Změny v bezpečnostní politice

V průběhu měsíců a let se bude bezpečnostní politika ve výukovém středisku měnit. Budou zjištěny nedostatky v zavedení či v nastavení pravidel. Všechny změny, které nastanou, budou probíhat v pravidelném školení 1x za rok. V případě potřeby bude školení vícekrát jak jednou za rok, nebo bude školení přesunuto.

Nejčastější chyby

Celá organizace by měla být informována o nejčastějších chybách, jakými mohou být např.:

- chyby při zavádění ISMS
- chyby v zavedeném ISMS
- chyby IS
- chyby způsobené lidskou činností
- chyby v rámci školení

Budeme se následně snažit vyvarovat chyb, o nichž na školení bude řečeno tím, že celá organizace bude znovu následně a důkladně proškolena v této problematice. Bude-li nutné, budou navržena také opatření, o kterých je potřeba znovu informovat, popřípadě také zaškolit i fyzicky. V tomto případě nebude nutné školit celý personál, ale pouze vybrané osoby.

Ověření znalostí

Na konci školení bude posluchačům rozdán test, který budou zpracovávat samostatně. Budou tři verze testu, test je možné 2x opakovat. Po každém kole testu budou testy řešeny v celé skupině se školitelem tak, aby si posluchači co nejvíce odnesli a ujasnili si doposud vše, co jim nebylo jasné. Pokud absolvent školením neprojde ani jedním ze tří testů, musí školení absolvovat znovu.

Posluchači budou s touto problematikou seznámeni na 4 denních školeních z důvodu velkého množství informací. Je potřebné, aby byly schopni toto množství zpracovat. Je zde plánováno dostatečné množství volného času, které budou moci posluchači využít i na samostudium a na dotazy.

Několik dní po školení proběhne namátkový interní audit a uživatelé, kteří nenaplní požadavky auditorů, musí toto školení absolvovat od začátku.

Metodika školení pro vedení

Základní školení se zaobírala pravidly také pro vedení. Nicméně pro vedení jsou navržena další školení, kterých by se měli zúčastnit. Jedná se o typy školení, jako je například „jak vést“, „jak zvládat krizové situace“ apod. Tyto druhy školení, se budou v průběhu času měnit a doplňovat. Níže je uveden výčet těch základních z nich.

Nejdříve se však zaměříme na dvě školení, BCM a DR plán, které musí absolvovat celé vedení, aby se tato problematika dostala více do podvědomí. Tato školení budou probíhat samostatně. Začátek bude v 8:00 a konec je plánován na druhý den kolem 15:00 hod. Zajištěno bude ubytování i občerstvení. Na konci školení získají posluchači certifikát o absolvování.

BCM – Business Continuity Management

BCM neboli Řízení kontinutity činností je aktivita úzce spojená a podřízená podnikání, která může poskytnout strategický a provozní rámec pro pohled na způsob, jakým organizace poskytuje svoje produkty a služby, a jak je přitom odolná proti jejich narušení, zničení či ztrátě. (9)

Toto školení v diplomové práci uvádím, neboť řada organizací má za to, že se jim incidenty nepřihodí, nebo že pojištění jako takové, jim dovolí se ze ztráty či incidentu rychle a účinně vzpamatovat. Právě pojištění je klíčovou komponentou celkového řešení BCM. Pojištění totiž může poskytnout finanční pokrytí ztráty nebo incidentu, ale nezabrání mu, nezajistí obnovení činností, znovuvybudování organizace a nezíská zpět ztracenou důvěru zákazníků. (9)

Účinnost BCM lze nejlépe demonstrovat na schopnosti organizace vrátit se k běžnému provozu. (9)

DR plán – Disaster Recovery

DR plán je plán obnovy po havárii, který shromažďuje postupy pro zajištění obnovy IT služeb po živelných pohromách a jiných zásadních událostech. (9)

Posluchači v rámci tohoto školení budou seznámeni s efektivním preventivním plánováním, které musí zahrnovat pět hlavních faktorů. Jedná se o dobu nečinnosti, integritu dat, náklady, jednoduchost a bezpečnost. Dalším tématem bude plánování pro záchranu dat organizace, jimiž mohou být datové pásky, záložní disky, cloudové technologie či vzájemná kombinace těchto technologií. (9)

Univerzální recovery plán, který by vyhovoval potřebám a specifikům všech organizací neexistuje, nicméně zmíněné oblasti slouží jako podklad při sestavování DR plánů a obecně při zvyšování připravenosti společnosti na různé nenadálé události. (9)

Krizový management

Cílem tohoto školení je seznámení posluchačů s možnostmi identifikace potenciálních krizových situací, s aplikací principů a metod krizového managementu, vytvářením a využíváním krizového scénáře pro vlastní organizaci. (20)

Posluchači budou seznámeni s prevencí krizových situací a také postupy pro zvládání krizové situace, když vypukne. (20)

Školení je dvoudenní. Je zajištěno ubytování, snídaně, obědy a večeře. Občerstvení a nápoje jsou k dispozici po celý den. Materiály jsou zahrnuty v ceně.

Začátek školení obvykle bývá první den od 9:00 do 18:30, druhý den je začátek v 8:00 a končí se obědem. Přibližně okolo 13:00 hod.

Posluchači získají certifikát o absolvování.

Manažerské dovednosti

Toto školení je určeno pro začínající manažery a zaměstnance, kteří přecházejí do role nadřízeného. (21)

Přínosy školení jsou následující: (21)

- upevnění sebedůvěry v roli manažera
- definice vlastní strategie
- eliminace vlastních chyb a nedostatků při práci s lidmi
- zaměření se na své silné i slabé stránky – individuální doporučení jak na nich i s nimi pracovat

Osnova školení: (21)

- základní předpoklady k výkonu manažerské funkce
- základní manažerské kompetence
- řízení a organizování práce
- asertivita a řešení konfliktních situací

Školení je dvoudenní. Je zajištěno ubytování, snídaně, obědy a večeře. Občerstvení a nápoje jsou k dispozici po celý den. Materiály jsou zahrnuty v ceně.

Začátek a konec školení je od 8:00 do 16:00 oba dva dny.

Posluchači získají certifikát o absolvování.

Leadership

Školení je určeno pro manažery, které zajímá, jak správně vést tým lidí k jeho maximální výkonnosti. (21)

Přínosy kurzu: (21)

- jak být motivujícím a inspirujícím lídrem
- zjistíte, jaký dopad má Váš styl vedení
- řešení konfliktních situací optimálním způsobem
- schopnost definovat a řídit prostřednictvím cílů
- jak vést tým citlivě a profesionálně
- naučíte se, jak efektivně delegovat kompetence a poznat bariéry delegování

Osnova školení: (21)

- co je leadership
- stanovení cílů
- překonávání překážek
- nástroje leadershipu

Školení je dvoudenní. Je zajištěno ubytování, snídaně, obědy a večeře. Občerstvení a nápoje jsou k dispozici po celý den. Materiály jsou zahrnuty v ceně.

Začátek a konec školení je od 9:00 do 16:00 oba dva dny.

Posluchači získají certifikát o absolvování.

Hodnocení a motivace zaměstnanců

V organizaci je většinou plánována dlouhodobá spolupráce. Pro ni neodmyslitelně patří propracovaný systém hodnocení a také motivace zaměstnanců. Cílem je dosáhnout nejen lepších výsledků, ale především spokojených a produktivnějších zaměstnanců. (21)

Přínosy školení: (21)

- posílit vztah nadřízených se svými podřízenými
- osvojit si techniky a nástroje pro hodnocení
- naučit se pracovat se zpětnou vazbou ze strany zaměstnanců
- vytvoření motivačního systému
- dosažení lepších výsledků

Osnova školení: (21)

- hodnocení jako předpoklad růstu zaměstnanců
- motivace a její dopad na výkon

Školení je dvoudenní. Je zajištěno ubytování, snídaně, obědy a večeře. Občerstvení a nápoje jsou k dispozici po celý den. Materiály jsou zahrnuty v ceně.

Začátek a konec školení je od 9:00 do 16:00 oba dva dny.

Posluchači získají certifikát o absolvování.

Právní minimum pro praxi

V rámci tohoto školení se posluchači dozví informace a budou vybaveni následující dovednostmi: (20)

- jak a kde hledat zákony, které potřebují
- orientace v obchodním a občanském zákoníku
- jak lze moderními způsoby komunikovat ve státní správě
- jak funguje správní, civilní nebo trestní soudní řízení
- sociální dávky
- správné sestavení pracovní smlouvy

Školení je jednodenní a probíhá v odpoledních hodinách. Většinou od 13:00 do 18:00, kde je po celou dobu zajištěno občerstvení. Materiály jsou zahrnuty v ceně.

Posluchači získají certifikát o absolvování.

Vedení porad

Tento typ školení je určen pro manažery, kteří chtějí zefektivnit vedení pracovních porad. (20)

Přínosy kurzu: (20)

- jak vhodně plánovat poradu s ohledem na účastníky
- jak dospět ke zvýšenému cíli porady
- naučíte se jak umět vést konstruktivní diskusi
- jak účinně a efektivně argumentovat

Osnova školení: (20)

- organizace a příprava jako základní kámen úspěchu
- průběh porady
- nejčastější problémy a jejich řešení

Školení je jednodenní, oběd a občerstvení s nápoji je k dispozici po celý den. V ceně, jsou zahrnuty i potřebné materiály. Doba trvání je obvykle 8:30-16:30 hod.

Posluchači získají certifikát o absolvování.

Metodika školení pro administrátory a ostatní technický personál

V této kapitole nebudou přiřazena přímo jednotlivá školení, neboť se pro tato školení budou připravovat tzv. školení „šitá na míru“. Spíše zde bude popsáno, na co je potřeba se u těchto pracovníků zaměřit.

Techničtí pracovníci přicházejí do styku se slaboproudými a silnoproudými rozvody, s rozvody plynu, klimatizací a dalšími přístroji, které mohou být životu nebezpečné a ohrozit život nejen servisních techniků, ale všech lidí, kteří se vyskytují v tomto objektu.

Důležité také je, aby se všemi komponentami uměli alespoň v základu pracovat. Proto budou vždy zaškoleni na základní ovládání, regulování, a také na problémy,

které by mohly nastat. Nebudou však specializováni, a proto musí vědět kdy a na koho se obrátit, aby neohrozili zdraví všech lidí nacházejících se uvnitř nebo blízko tohoto objektu.

Základní znalostí technických pracovníků by měly být i technické úpravy objektu.

Základní znalostí administrátorů je oprava počítačů, instalace, nastavení, zabezpečení včetně čipových karet. Také zaměstnanci, učitelé, žáci, zaměstnanci zabývající se výzkumem se obrací s problémy na tyto zaměstnance. Buď mohou telefonicky, osobně, nebo zadat požadavek přes Helpdesk.

Administrátoři budou zaškoleni na informační systémy, které budou dodávat subdodavatelé. Je potřebné základní školení, aby věděli, jak systém funguje, jak řešit situace, které nejsou běžné a kdy je čas volat specializovanou firmu.

Na konci školení posluchači obdrží certifikát o absolvování daného tématu.

Metodika pro školitele a žáky

Metodika pro školitele bude v první části kopírovat školení pro vedení. Jedná se o následující oblasti:

- právní minimum pro praxi
- leadership
- krizový management

Níže popsaná školení, které budou školitelé i žáci absolvovat, budou tzv. „šitá na míru“. Nadřízení mají vlastní požadavky a dle současných potřeb, neboť se výzkum bude teprve rozjíždět, budou školení obměňována a rozšiřována. Tvorba takového školení začne probíhat týden před jeho začátkem.

Základní školení pro školitele ve výukovém středisku jsou „Zásady chování v prostorách s výskytem nebezpečných látek chemického průmyslu“. Posluchači se seznámí s první pomocí při zásahu nebezpečnou látkou. Další školení, které musí

absolvovat, se nazývá „Jak efektivně vyučovat“. Tímto typem školení se má zamezit nesprávným metodám výuky a nesprávným chováním k žákům.

Žáci kromě základního školení musí taktéž absolvovat „Zásady chování v prostorách s výskytem nebezpečných látek chemického průmyslu“. Zde budou seznámeni s první pomocí, a jak postupovat při zásahu různých druhů chemikálií.

Pro školitele i žáky bude připraveno jednodenní pokročilé školení, zabývající se ochranou informací. Zaměstnanci ve výzkumu je následně proškolí na současný stav výzkumu a na jejich konkrétní práci a možnosti.

Na konci těchto školení, posluchači, kteří projdou testem, získají certifikáty o jejich absolvování.

Metodika pro zaměstnance ve výzkumu

Metodika pro zaměstnance ve výzkumu bude v první části kopírovat školení pro vedení a školitele. Jedná se o následující oblasti:

- právní minimum pro praxi
- leadership
- krizový management
- DR plán

Nedílnou součástí školení bude absolvování jednodenního pokročilého školení o ochraně informací. Zaměstnanci budou seznámení s tím, jak mají zabezpečovat a chránit citlivé dokumenty a chránit nebezpečné látky před neoprávněným přístupem.

Všichni zaměstnanci budou muset také absolvovat školení zabývající se zásadami chování v prostorách s výskytem nebezpečných látek chemického průmyslu. Posluchači se taktéž seznámí s první pomocí při zásahu chemikálií.

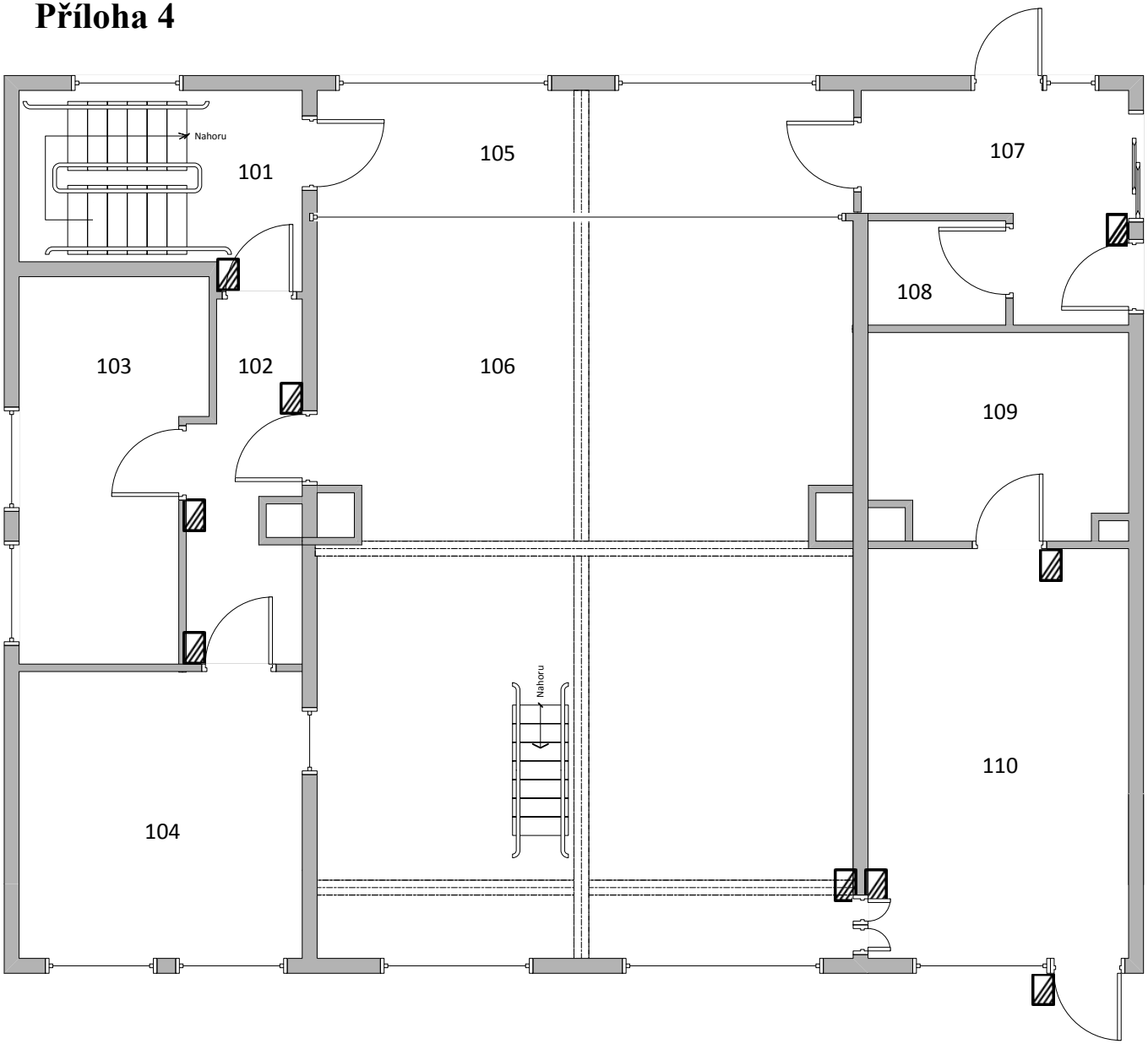
V tomto prostředí budou i složitější technické přístroje, na něž je potřeba uživatele zaškolit.

Dalším tématem bude zvládání řešení situací při krádeži či ztrátě dokumentů, materiálu a jeho možném postupu řešení.

Dle výběru nadřízených, budou některá školení zakončena testem. Při úspěšném výsledku, bude posluchačům vydán certifikát o absolvování. U školení, která nebudou zakončena testem, bude certifikát o absolvování vydán automaticky.

Zaměstnanci také projdou kurzem „Školení“. Neboť budou muset poučit školitele i žáky, kteří se budou pohybovat v prostorách už konkrétního výzkumu, na nějž bude toto školení zaměřeno. Na konci tohoto kurzu dostanou posluchači osvědčení o absolvování.

Příloha 4



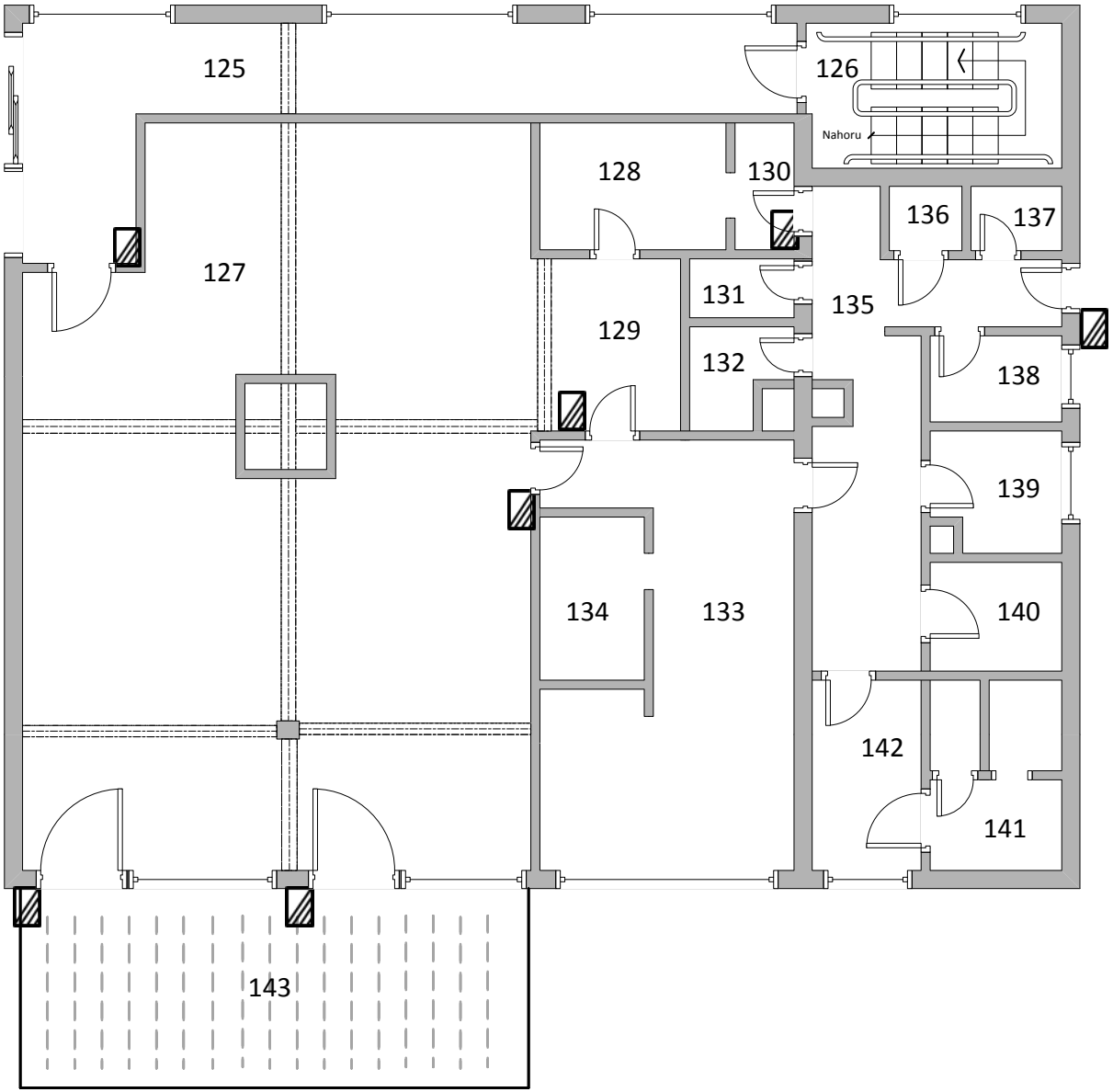
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - levé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 5



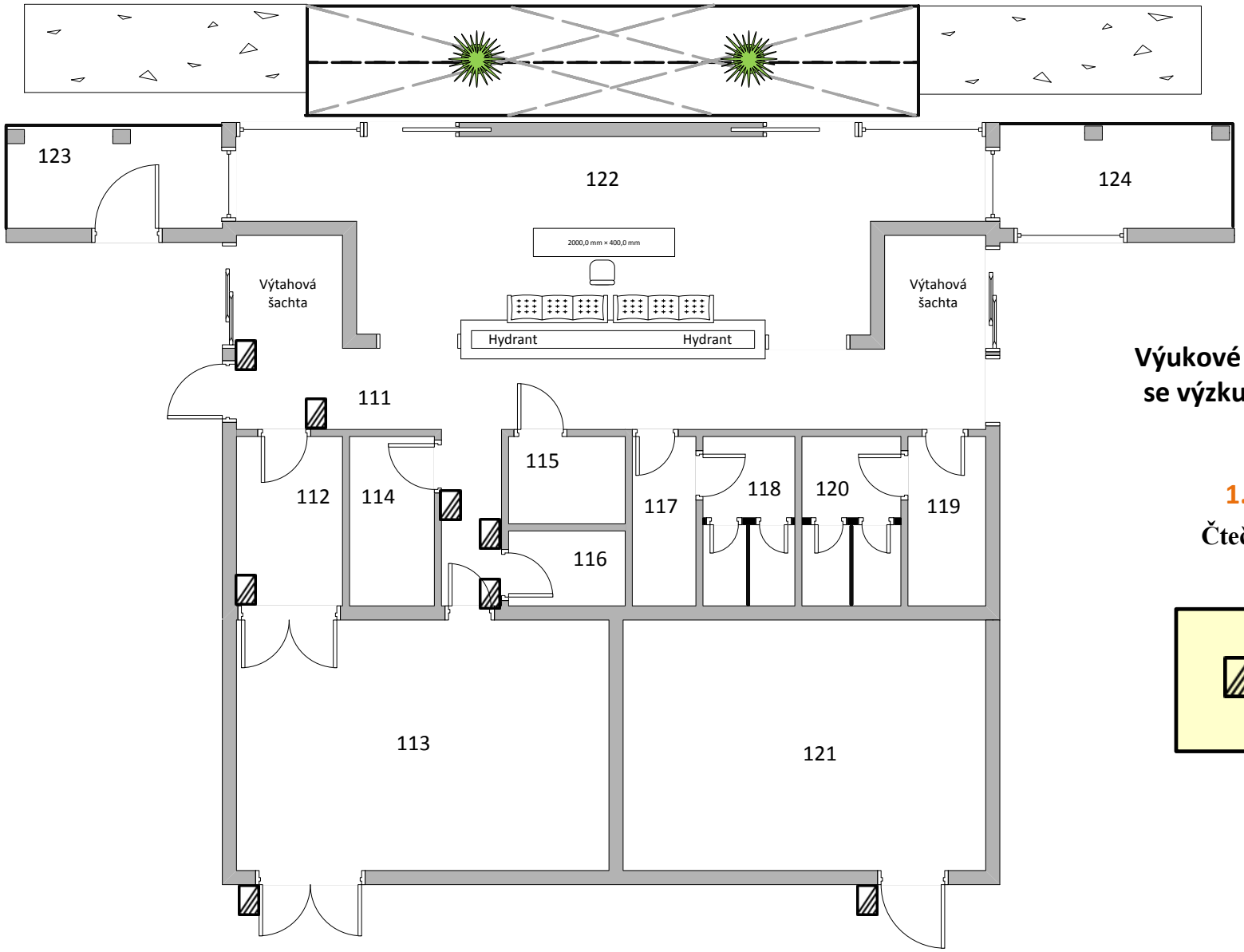
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - pravé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 6



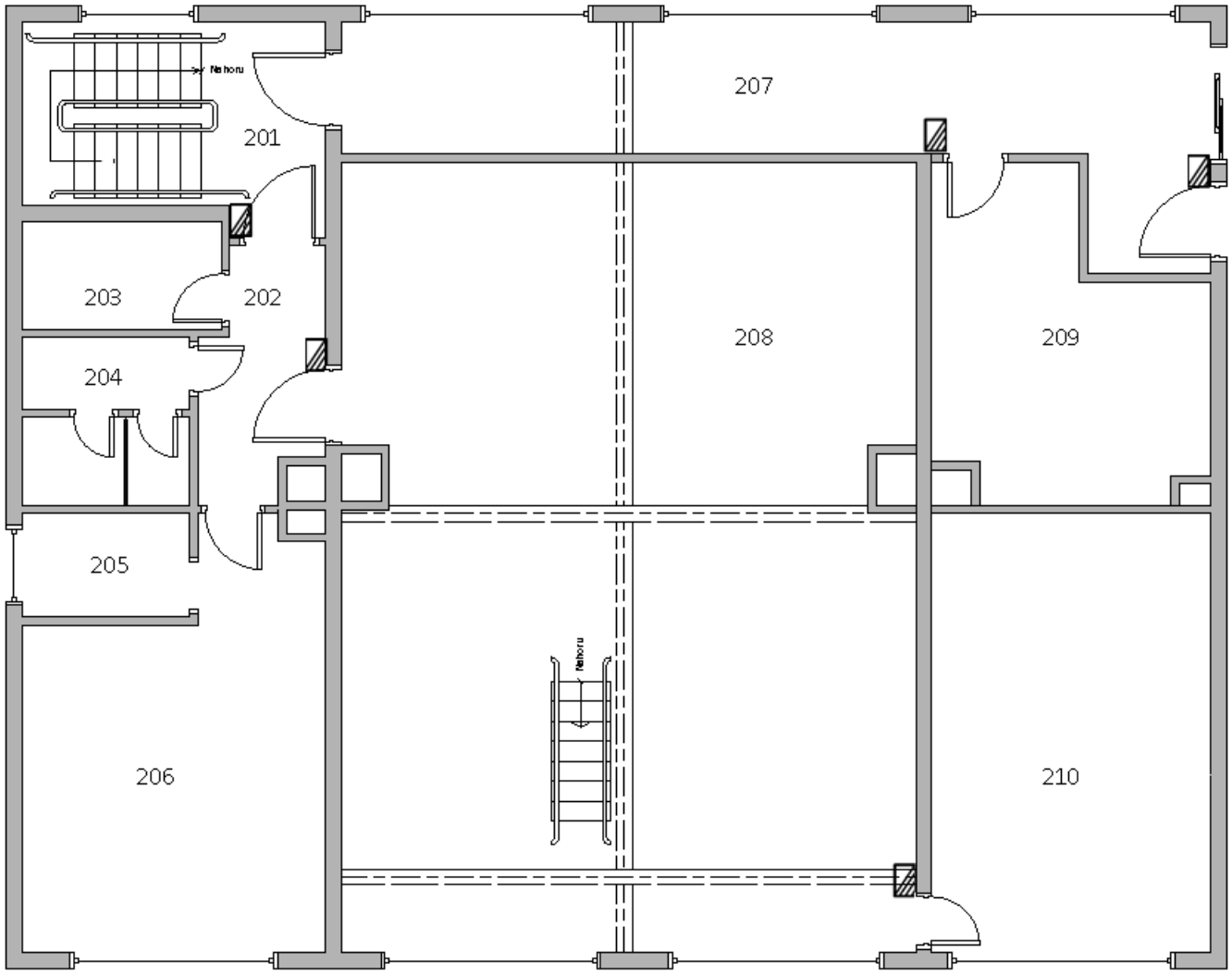
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - střed

Čtečky čipových karet

- čtečka karet

Příloha 7



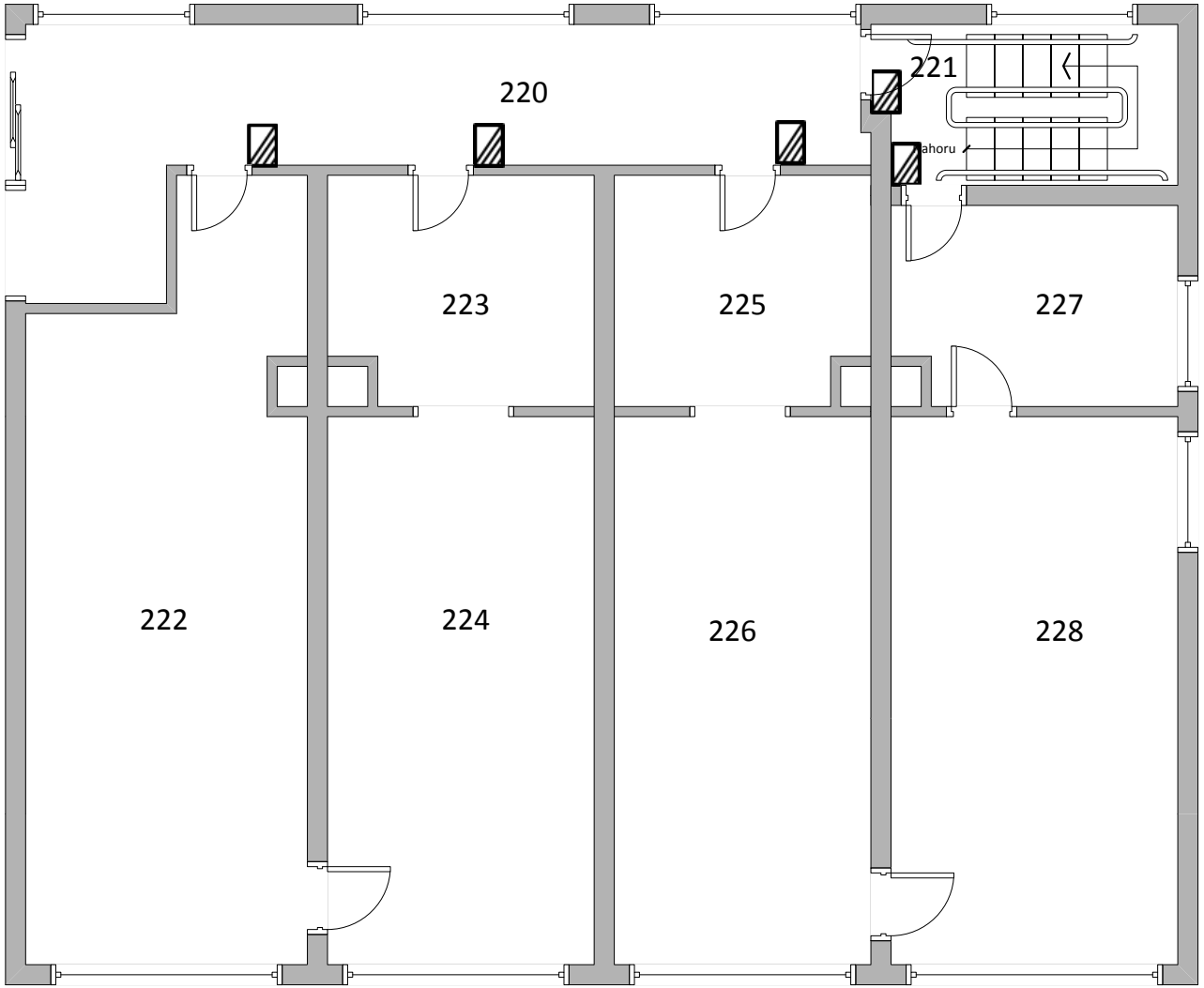
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - levé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 8



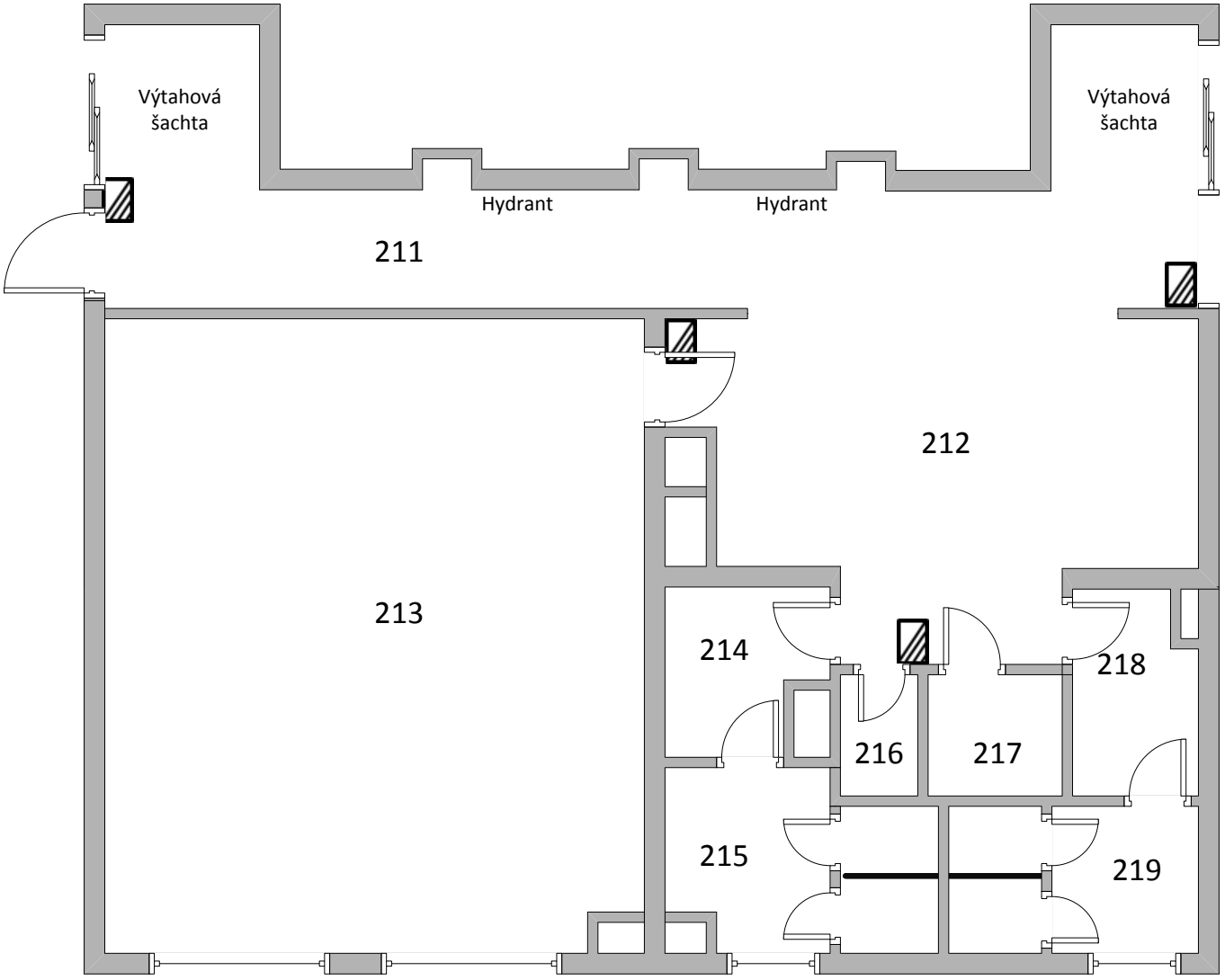
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - pravé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 9



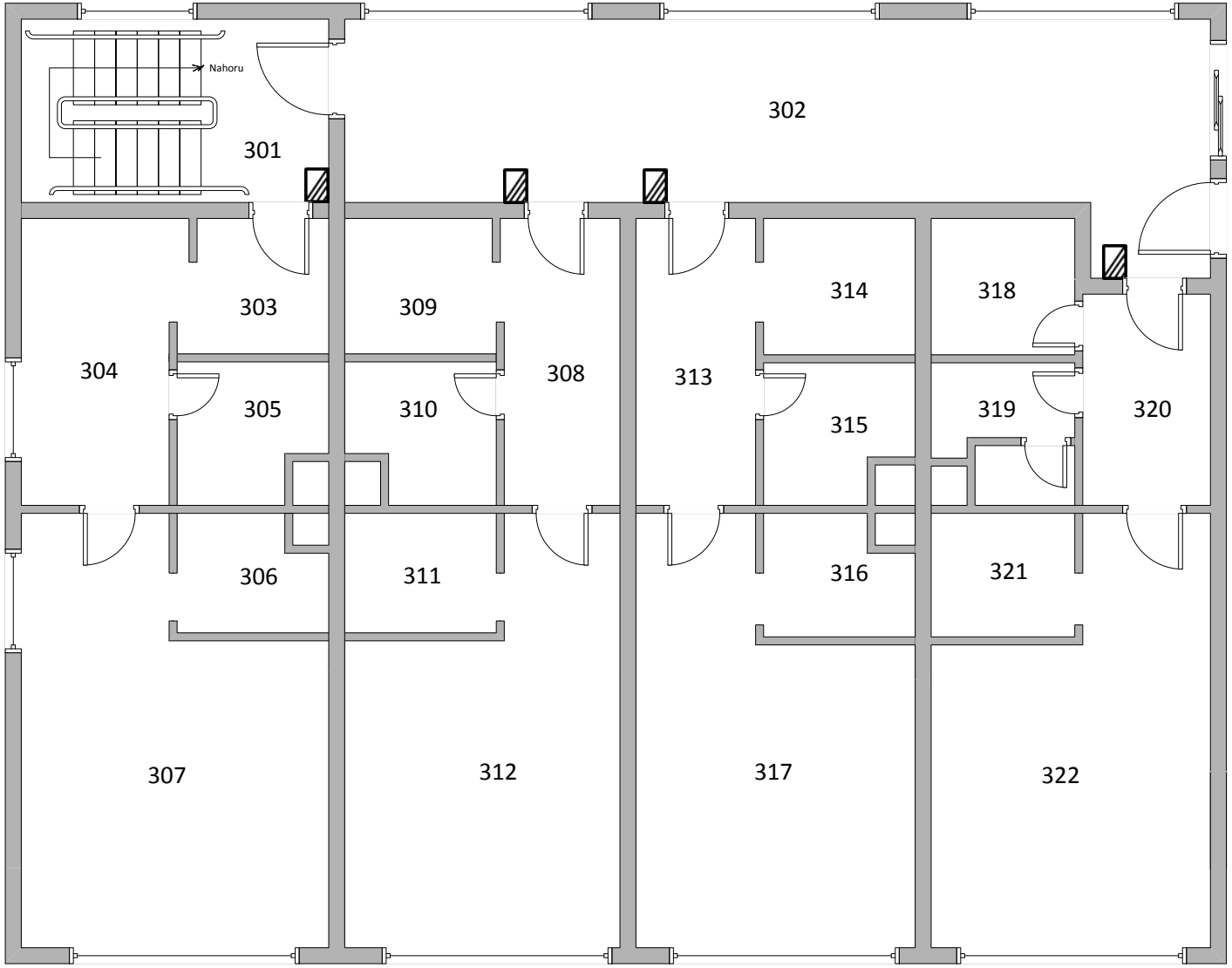
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - střed

Čtečky čipových karet

- čtečka karet

Příloha 10



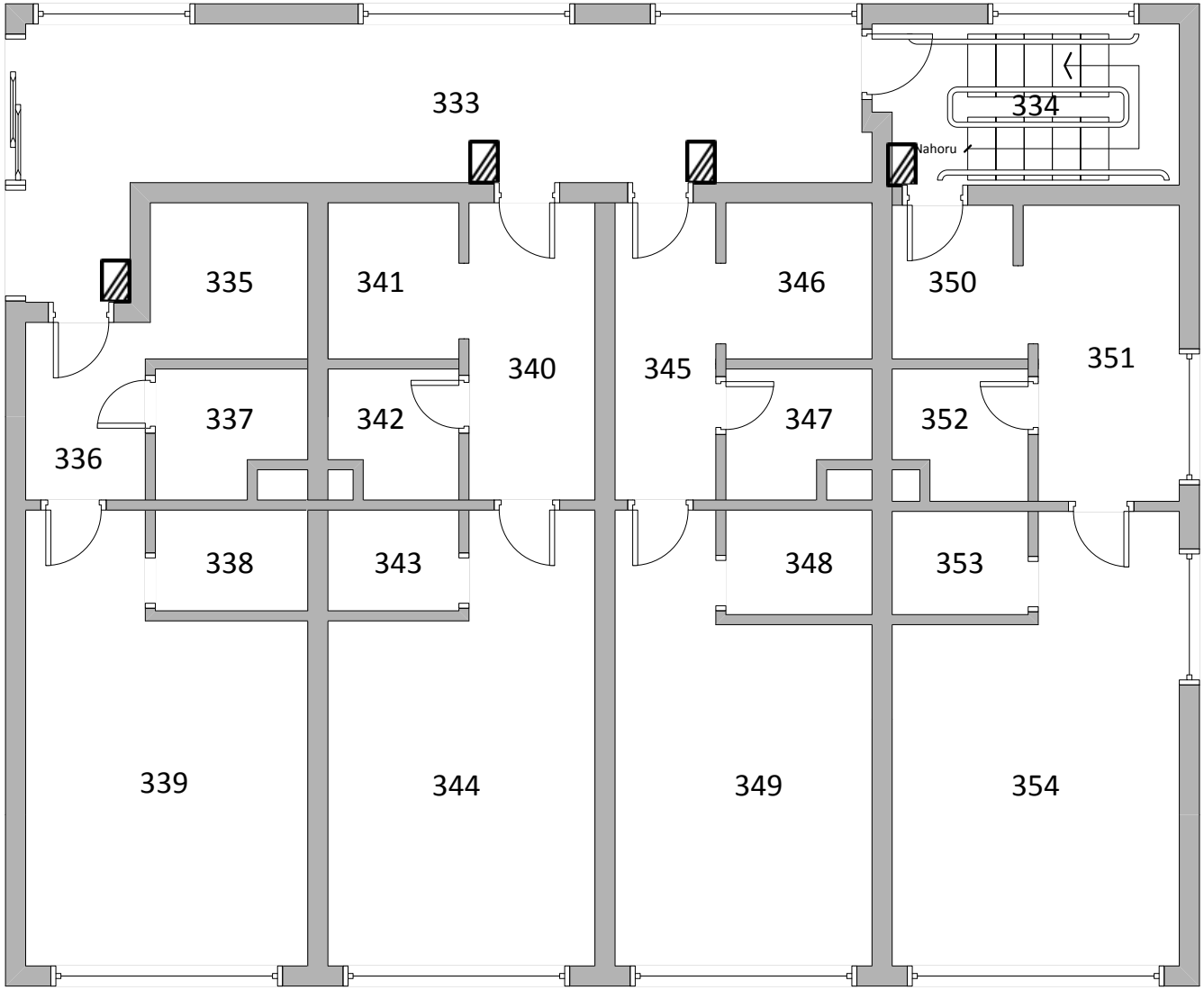
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - levé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 11



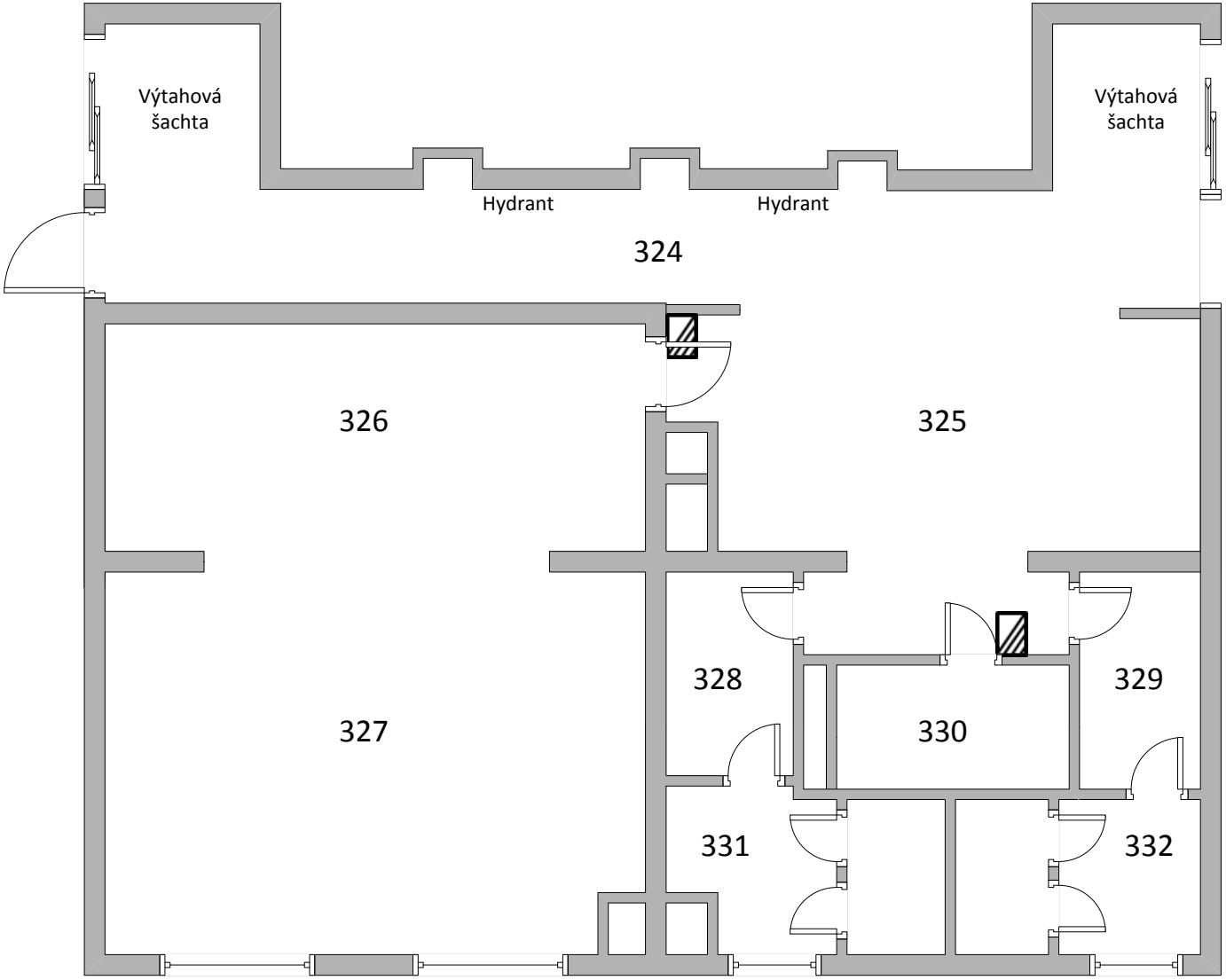
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - pravé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 12



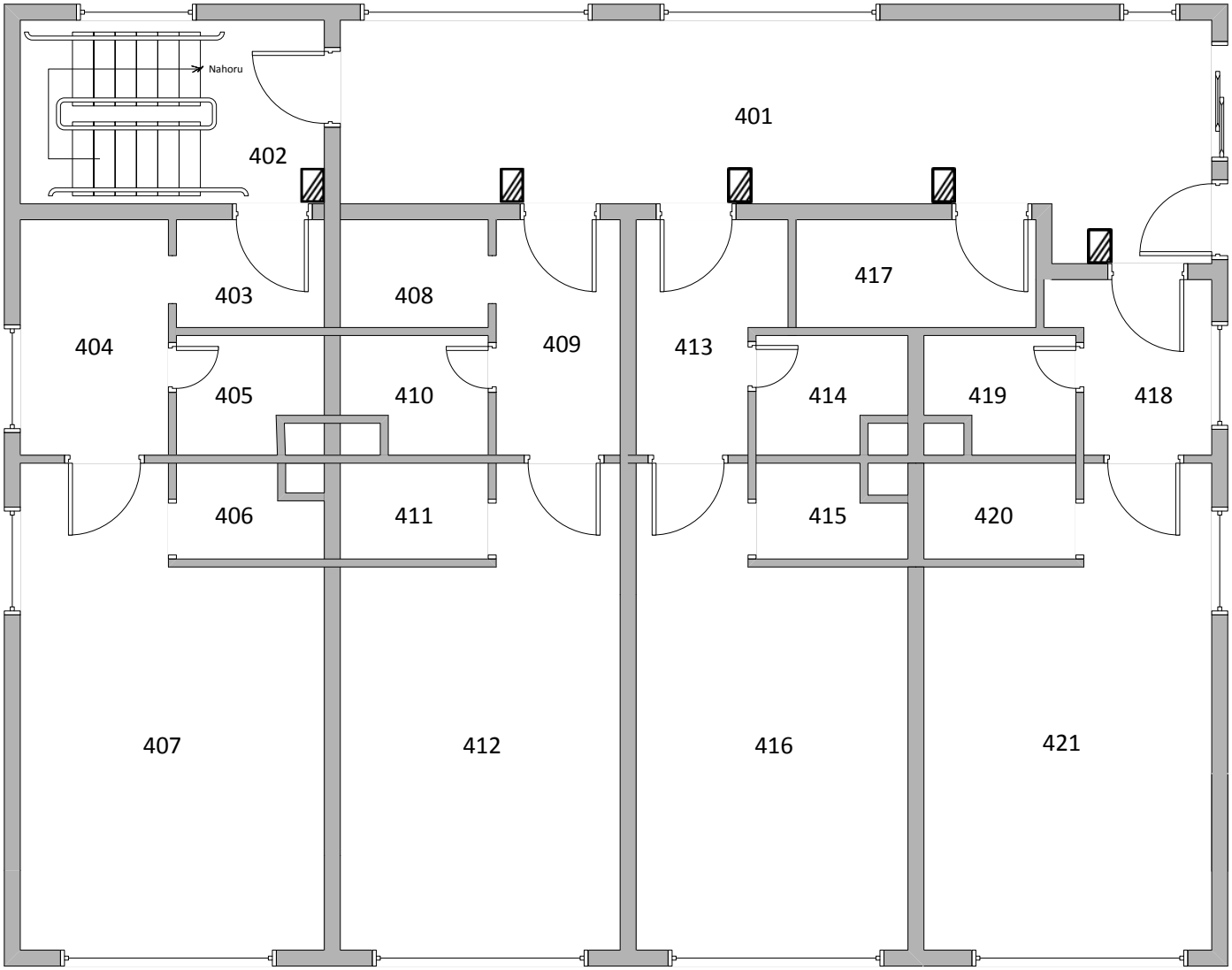
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - střed

Čtečky čipových karet

- čtečka karet

Příloha 13



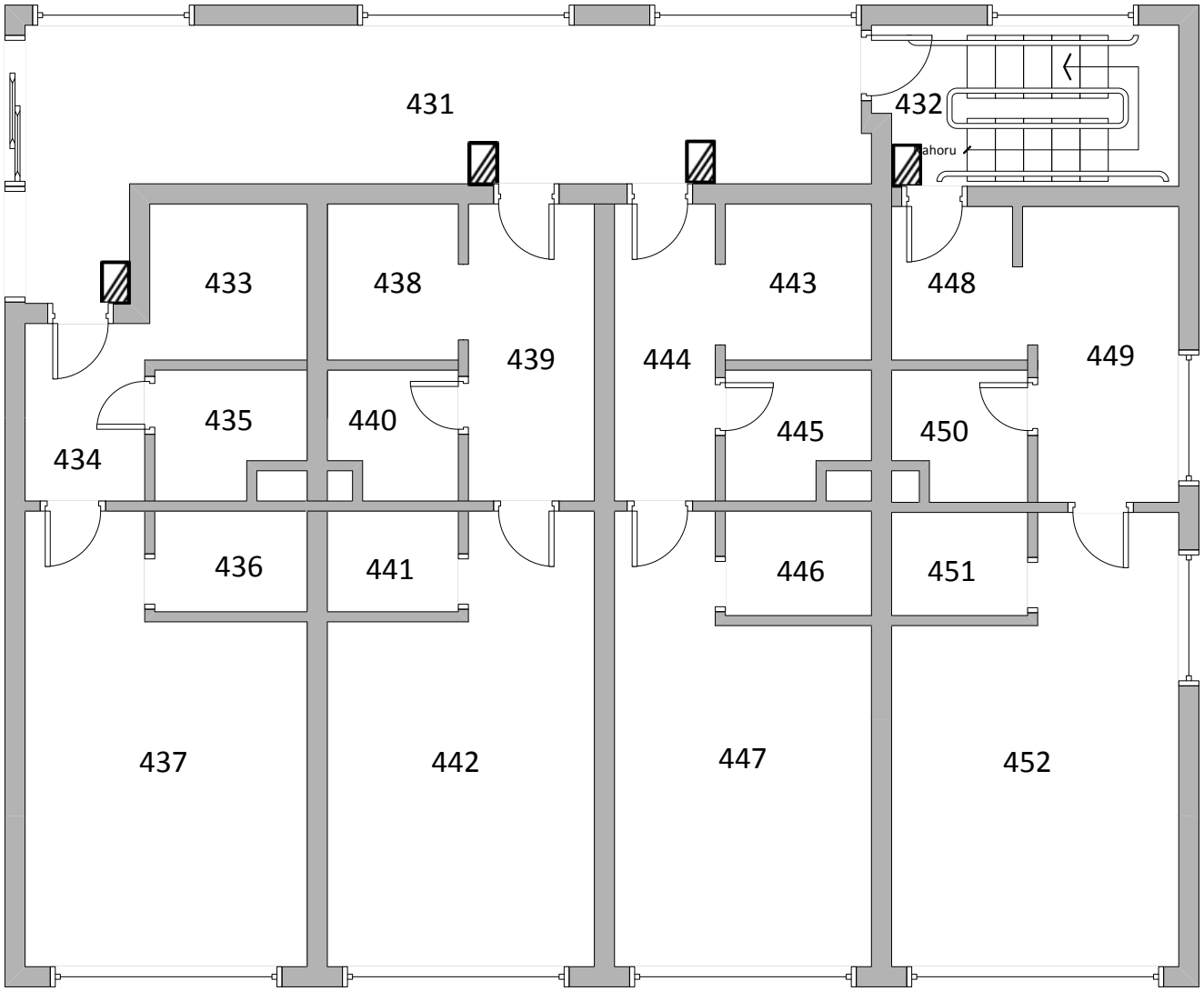
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - levé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 14



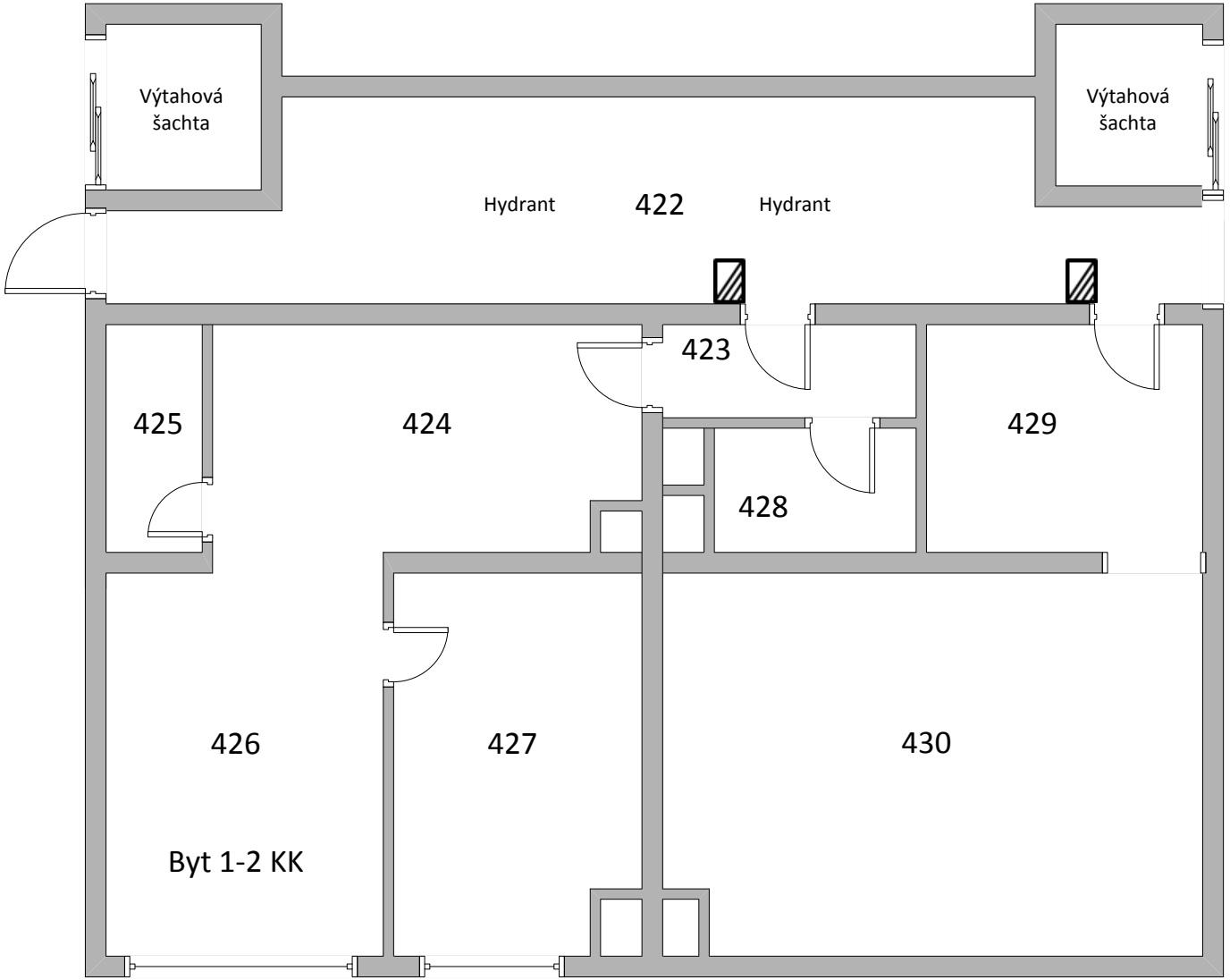
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - pravé křídlo

Čtečky čipových karet

- čtečka karet

Příloha 15



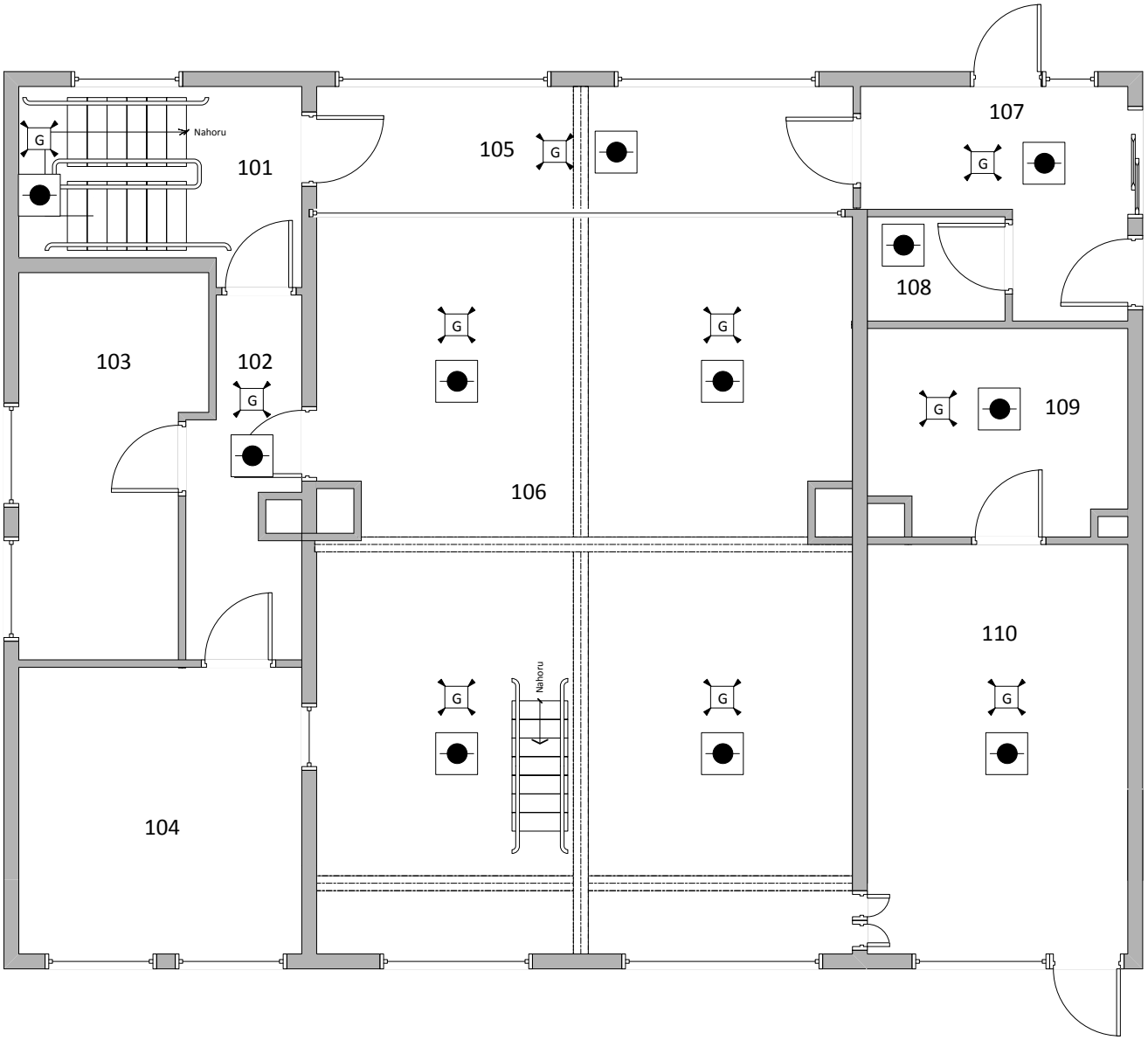
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - střed

Čtečky čipových karet

- čtečka karet

Příloha 16



Výukové středisko zabývající se výzkumem v chemickém průmyslu

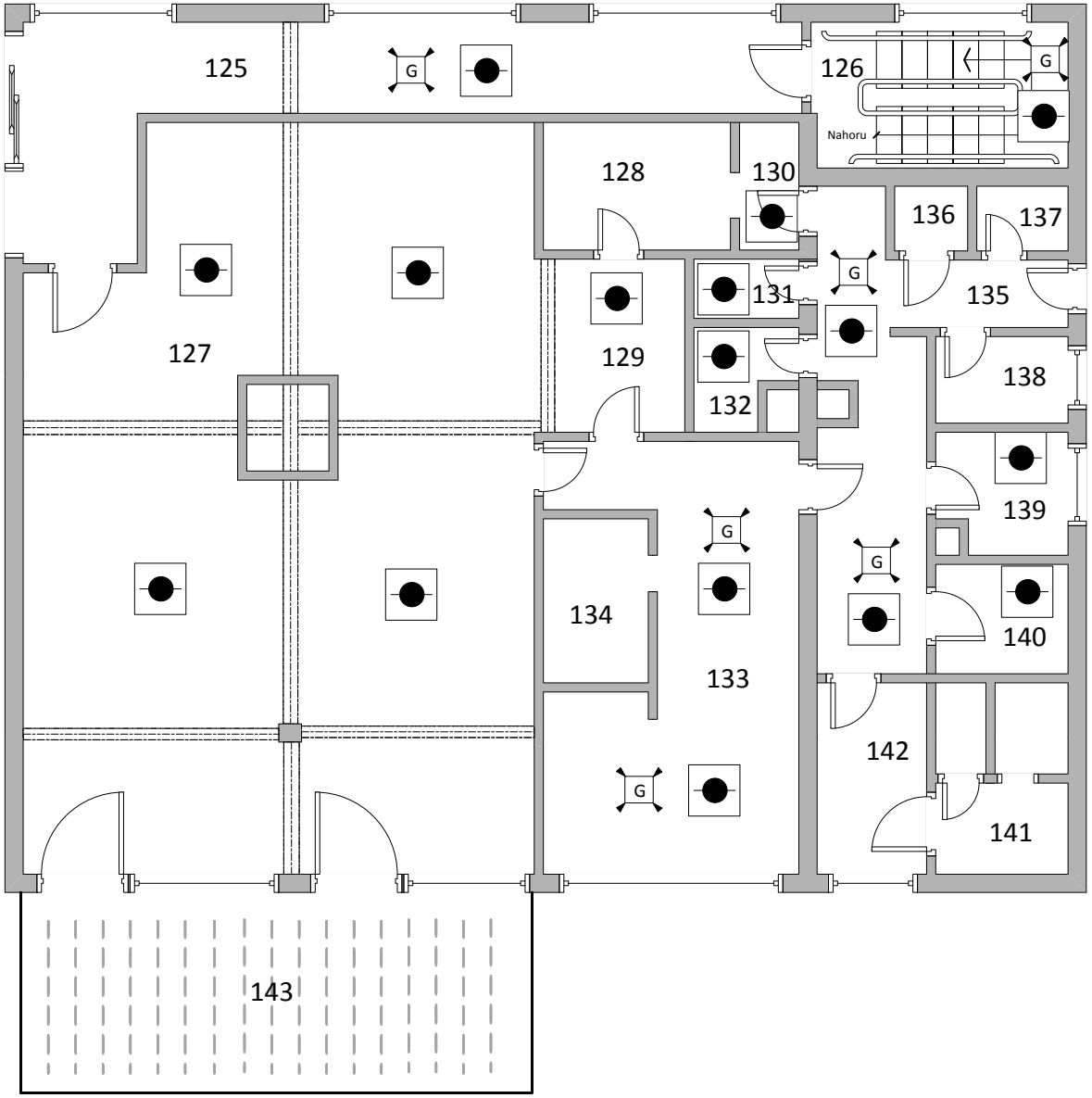
1.patro - levé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 17



Výukové středisko zabývající se výzkumem v chemickém průmyslu

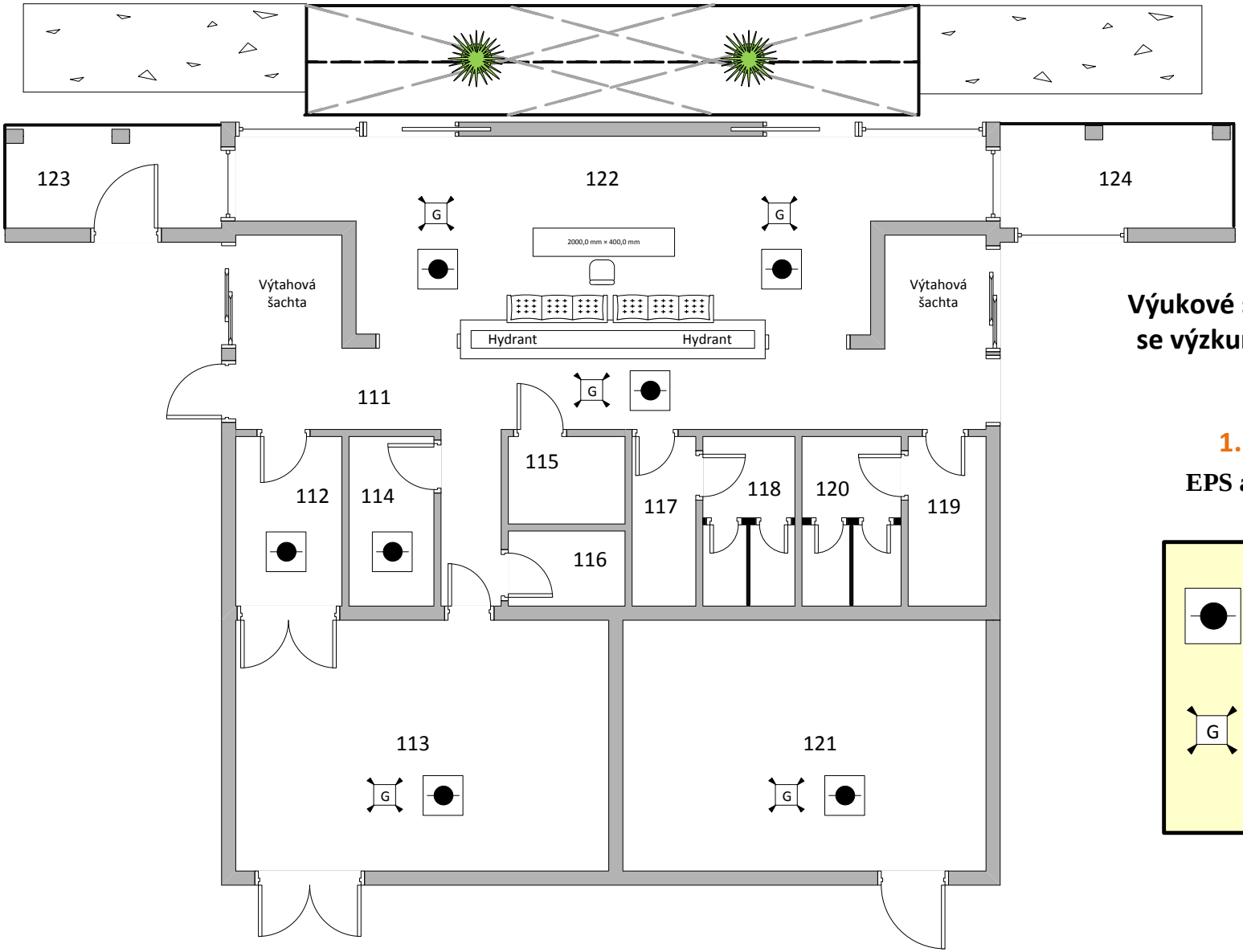
1.patro - pravé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 18



Výukové středisko zabývající se výzkumem v chemickém průmyslu

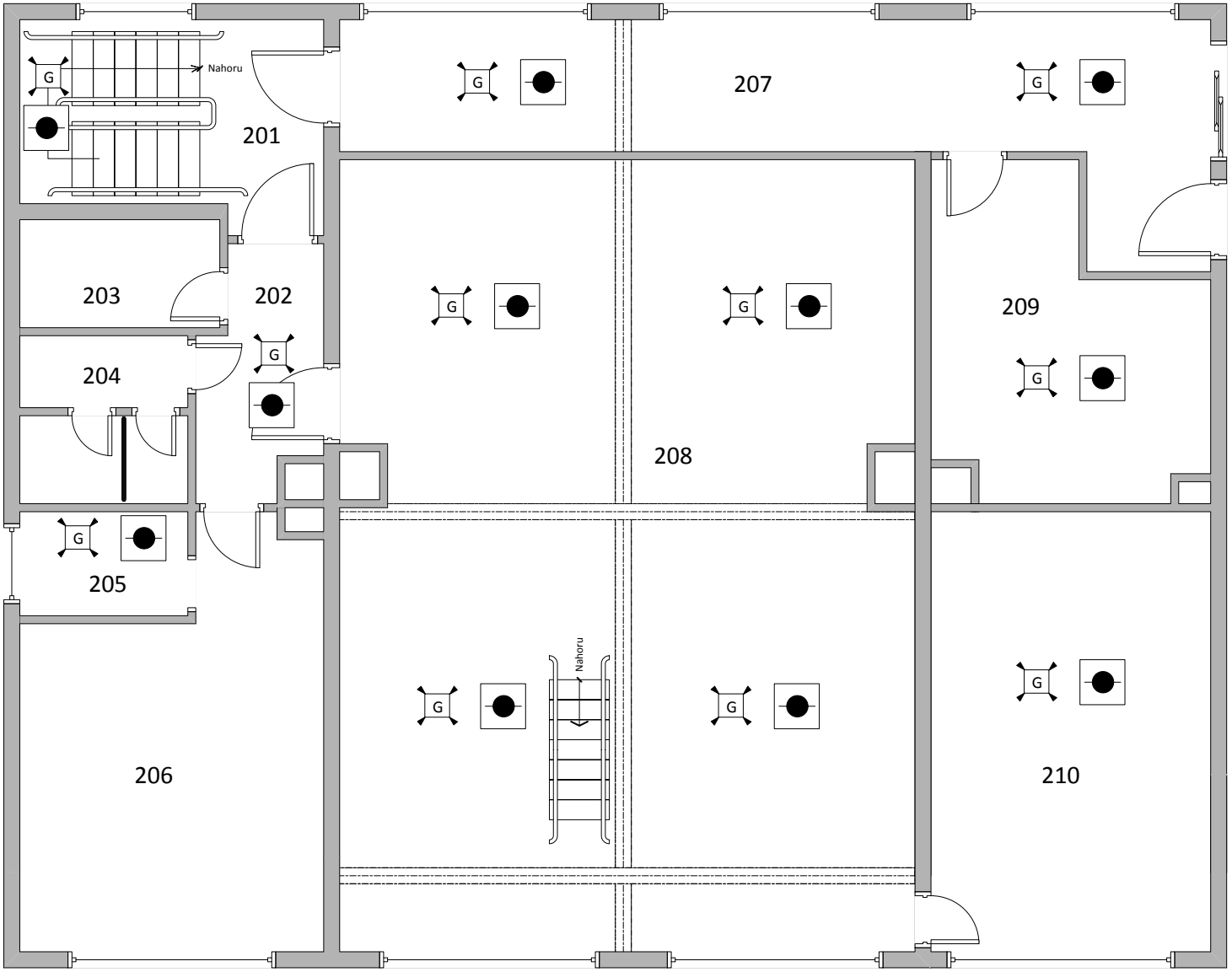
1.patro - střed

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 19



Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - levé křídlo

EPS a signalizace plynu

- detektor kouře

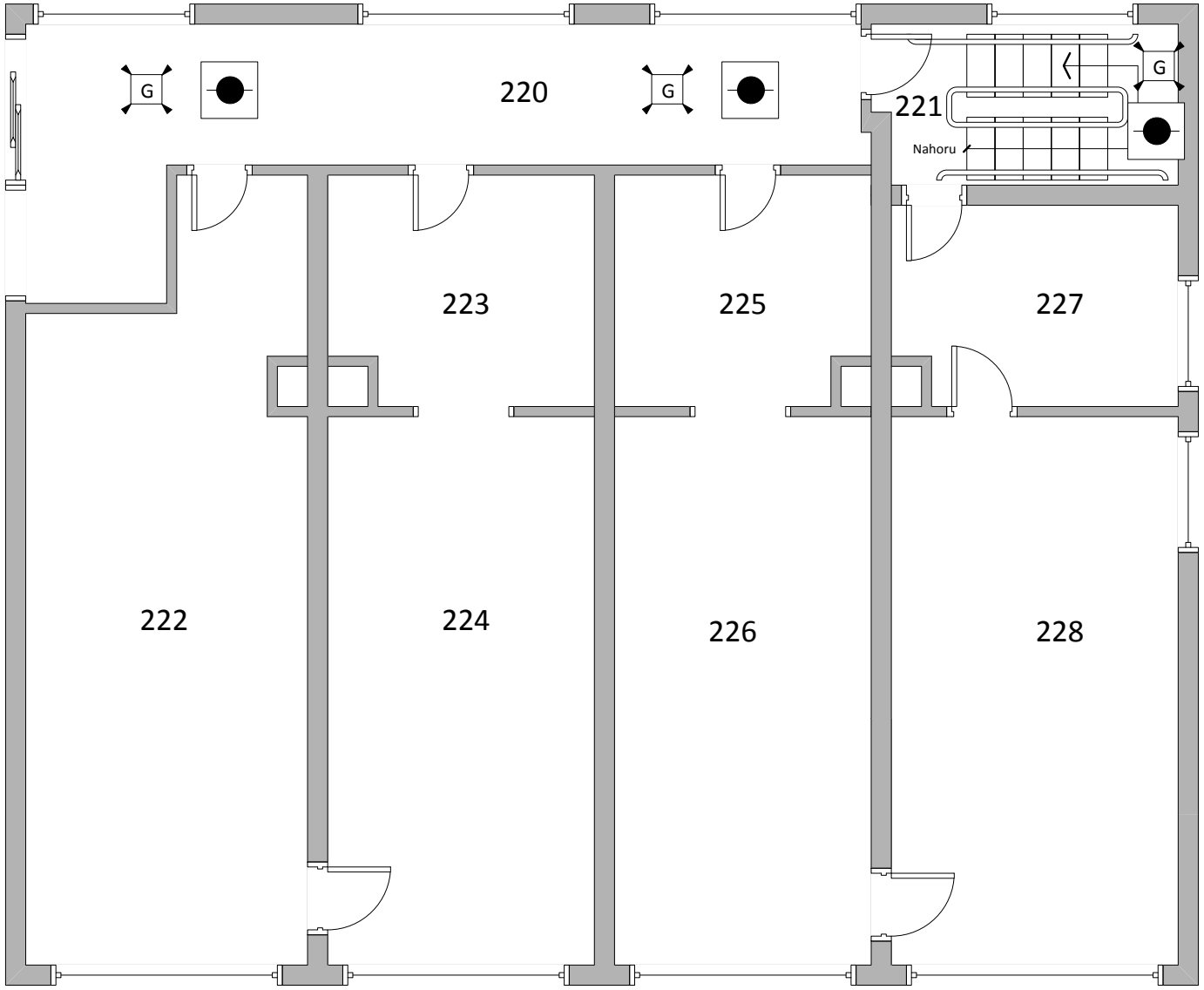
- detektor plynu

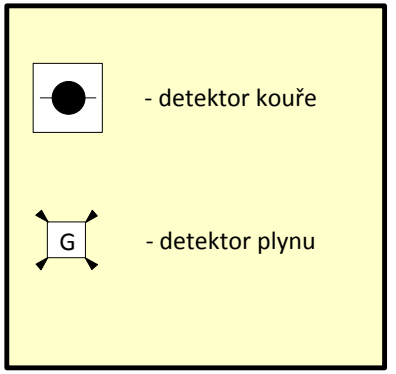
Příloha 20

Výukové středisko zabývající se výzkumem v chemickém průmyslu

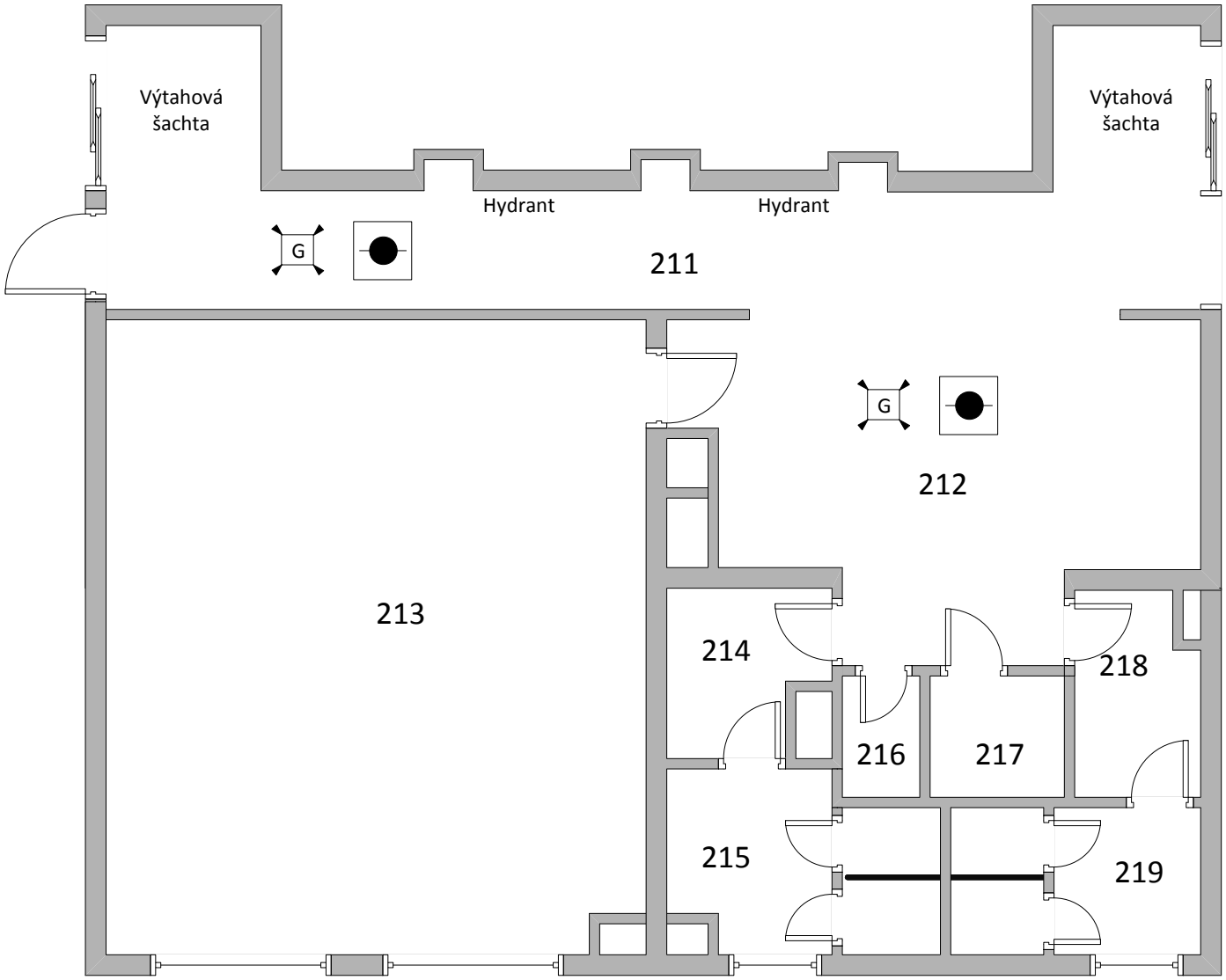
2.patro - pravé křídlo

EPS a signalizace plynu





Příloha 21



Výukové středisko zabývající se výzkumem v chemickém průmyslu

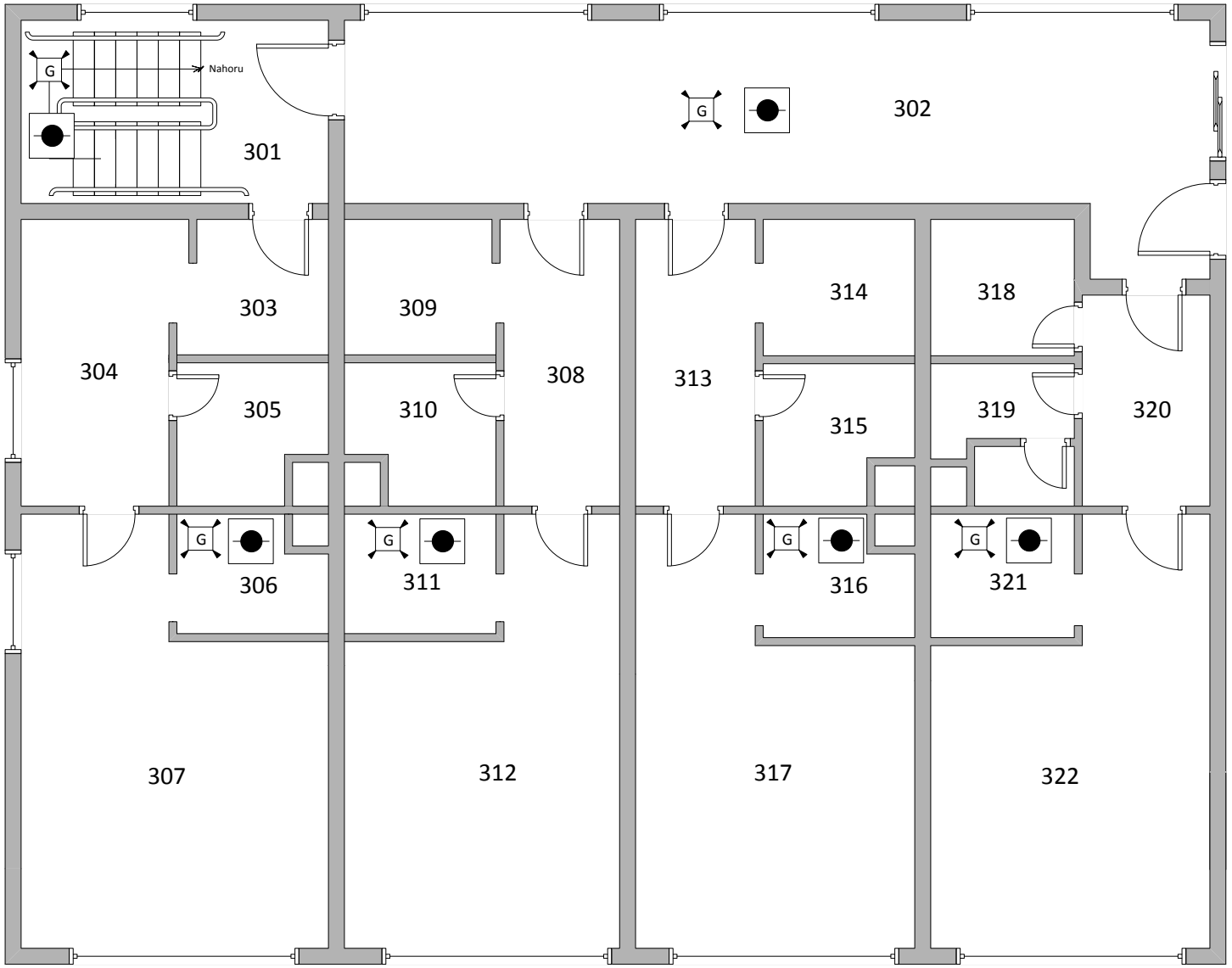
2.patro - střed

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 22



Výukové středisko zabývající se výzkumem v chemickém průmyslu

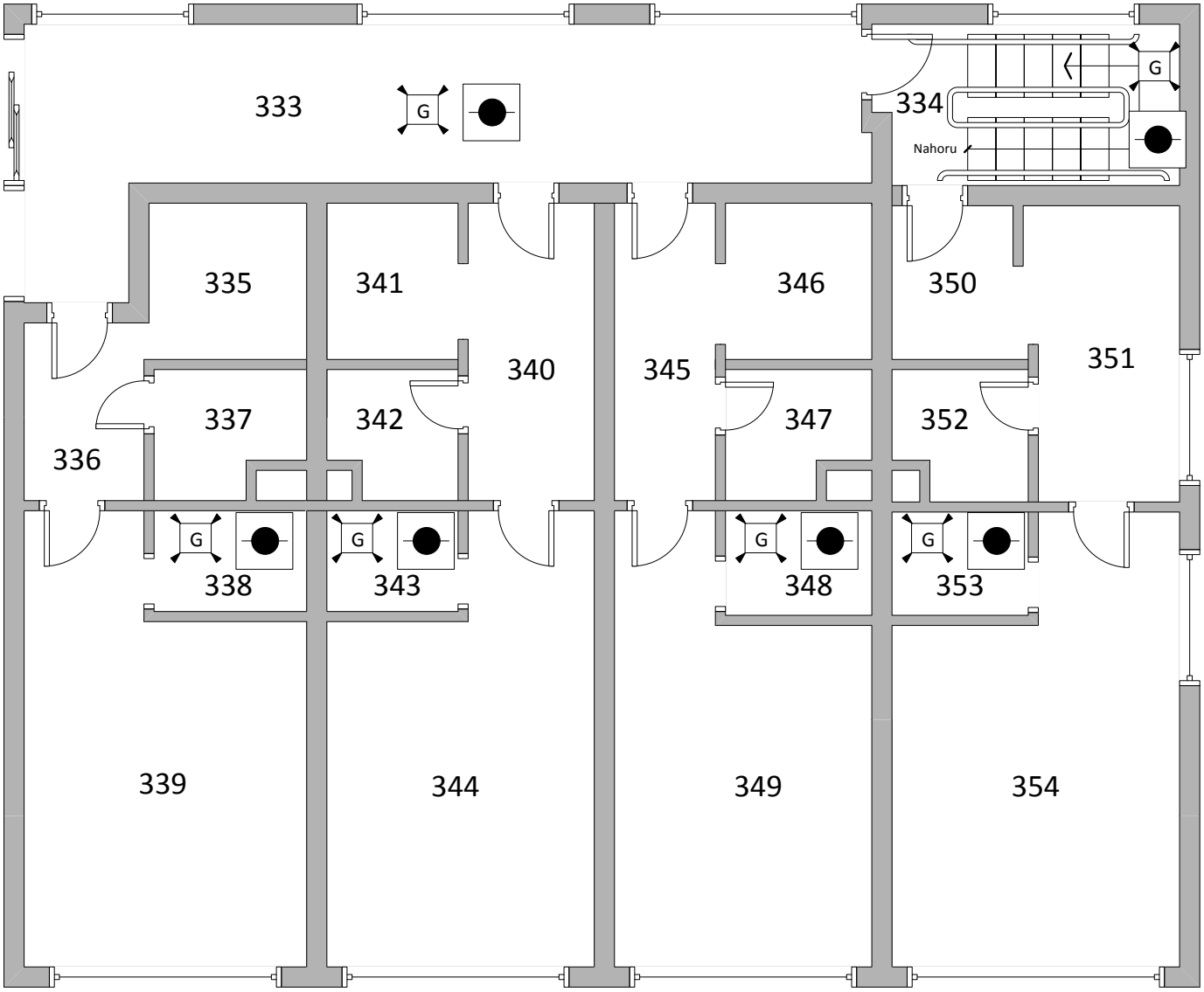
3.patro - levé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 23



Výukové středisko zabývající se výzkumem v chemickém průmyslu

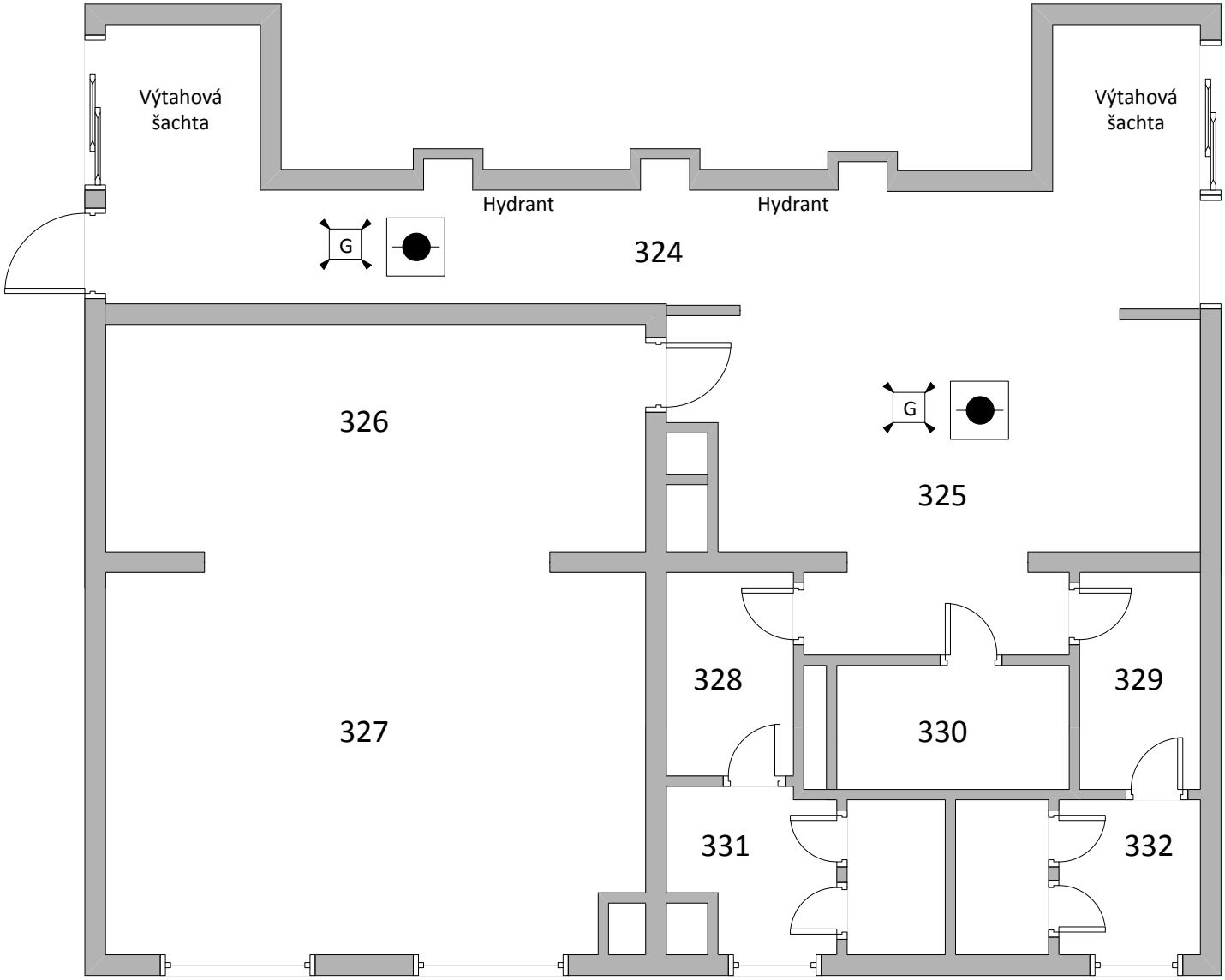
3.patro - pravé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 24



Výukové středisko zabývající se výzkumem v chemickém průmyslu

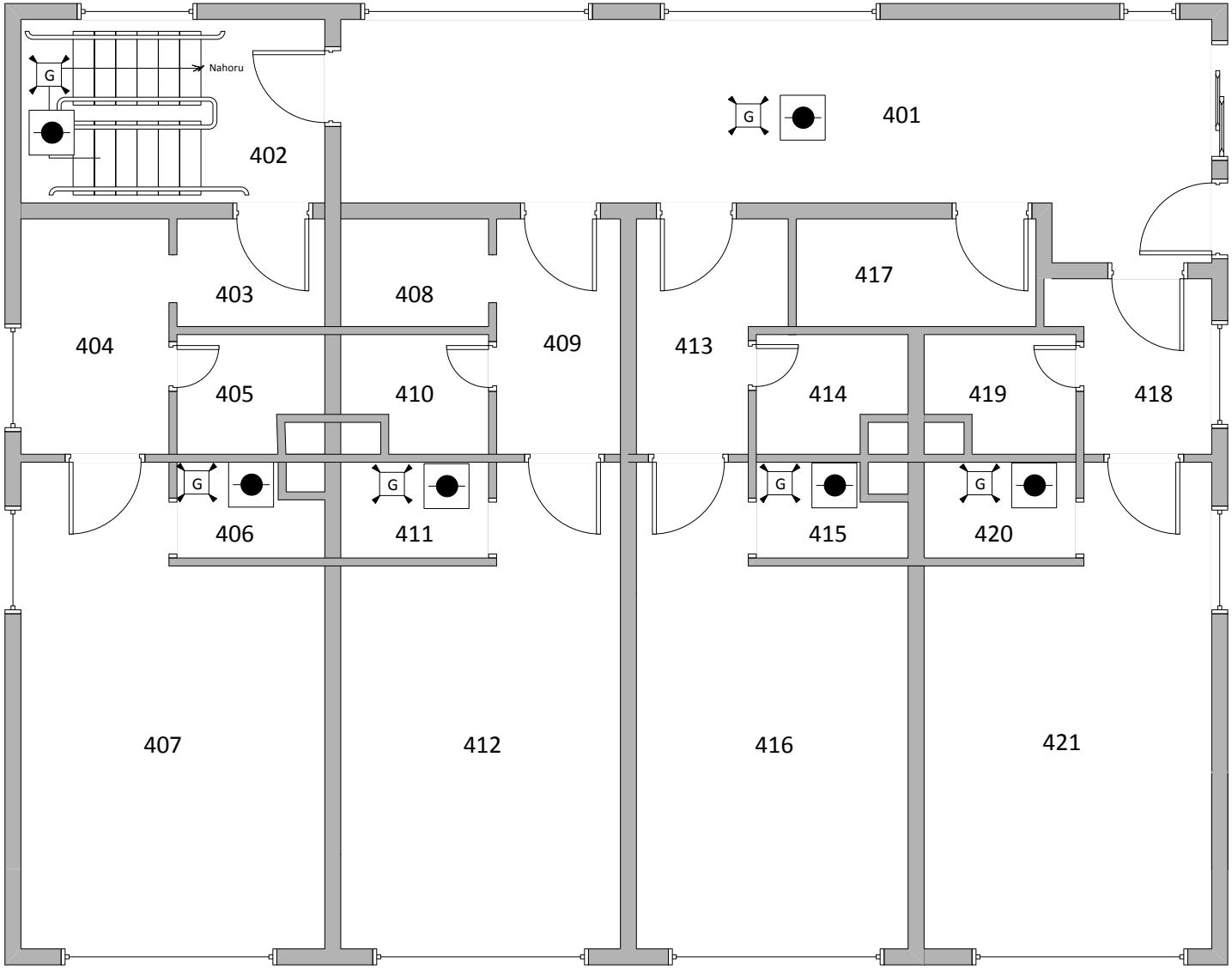
3.patro - střed

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 25



Výukové středisko zabývající se výzkumem v chemickém průmyslu

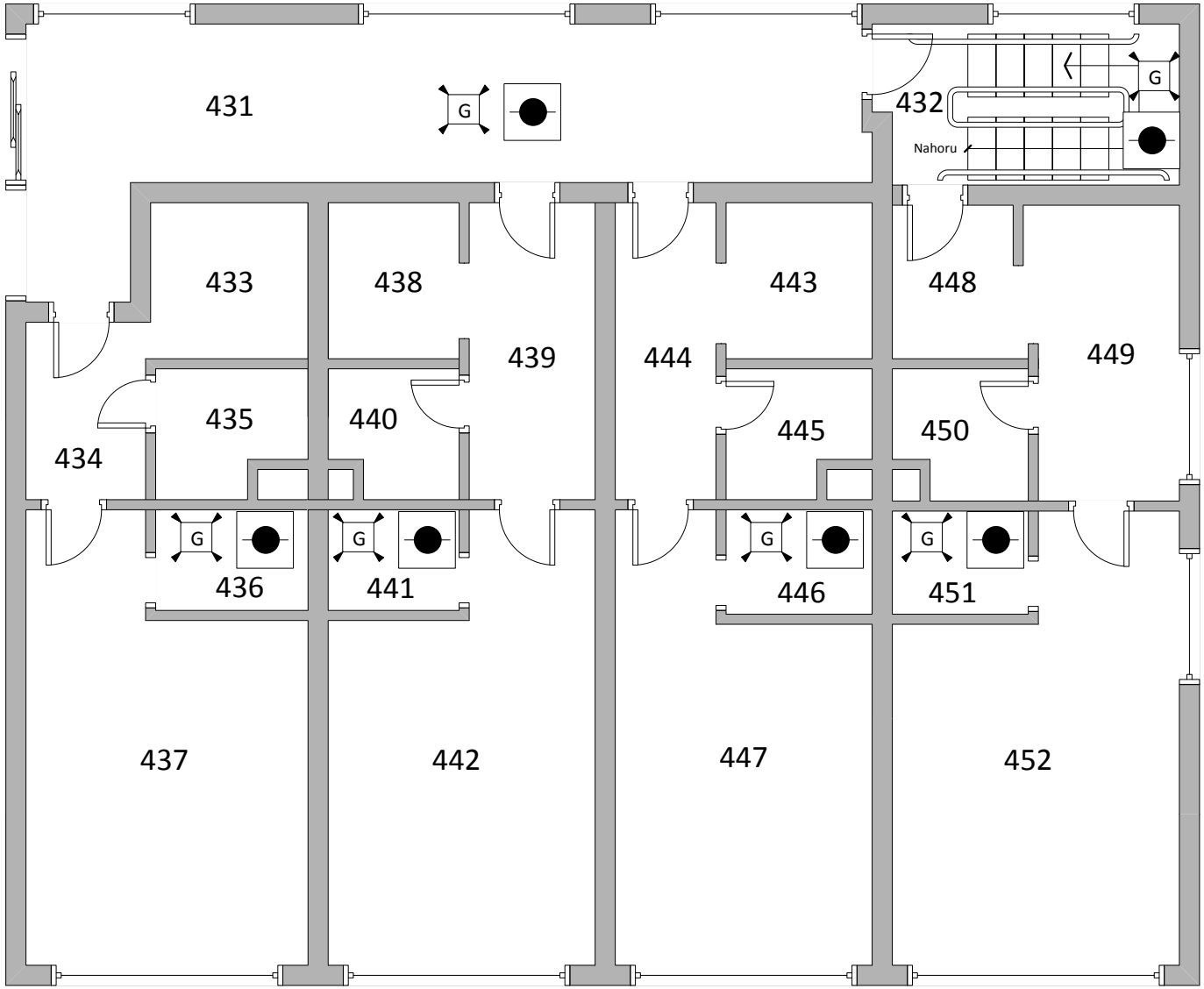
4.patro - levé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 26



Výukové středisko zabývající se výzkumem v chemickém průmyslu

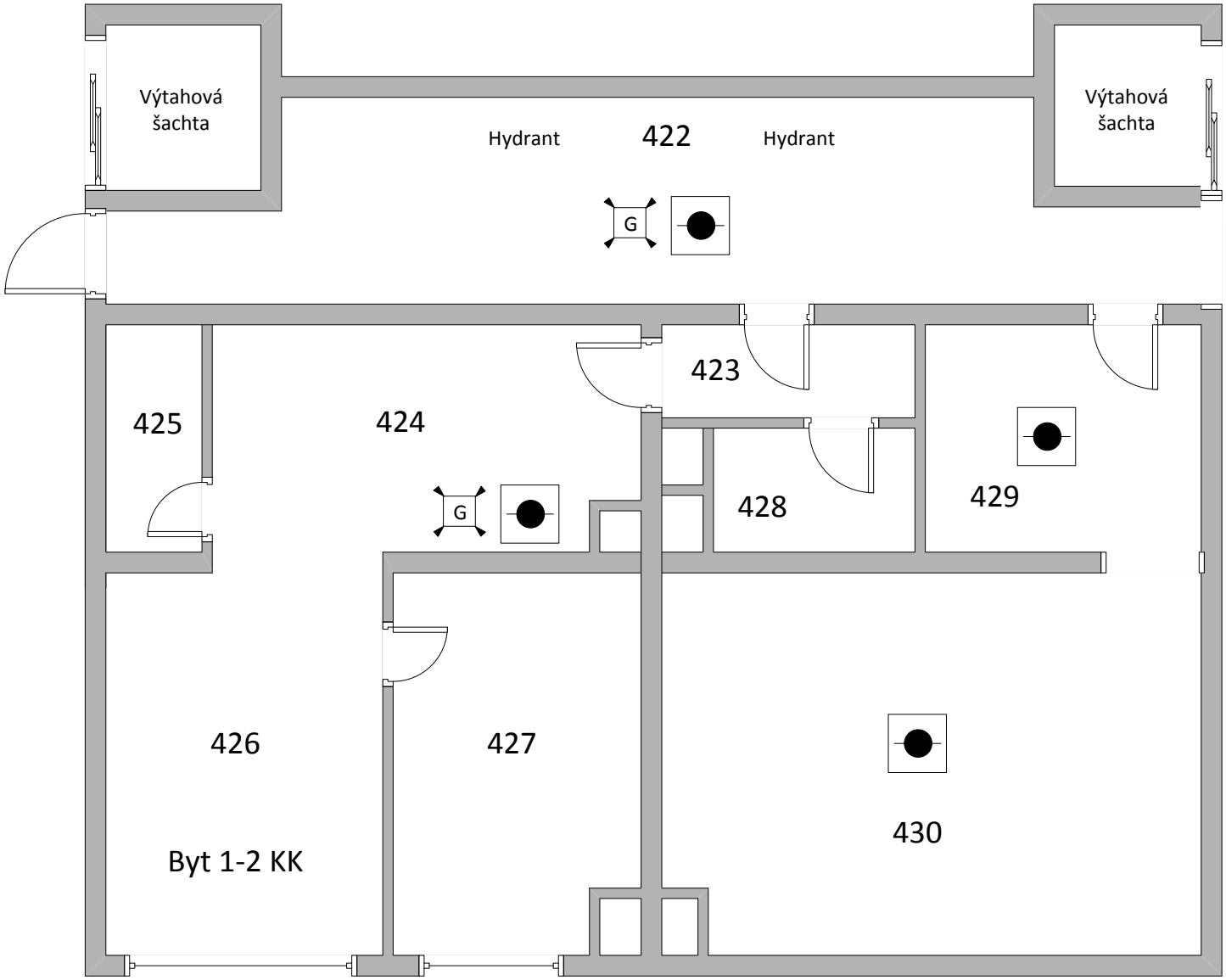
4.patro - pravé křídlo

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 27



Výukové středisko zabývající se výzkumem v chemickém průmyslu

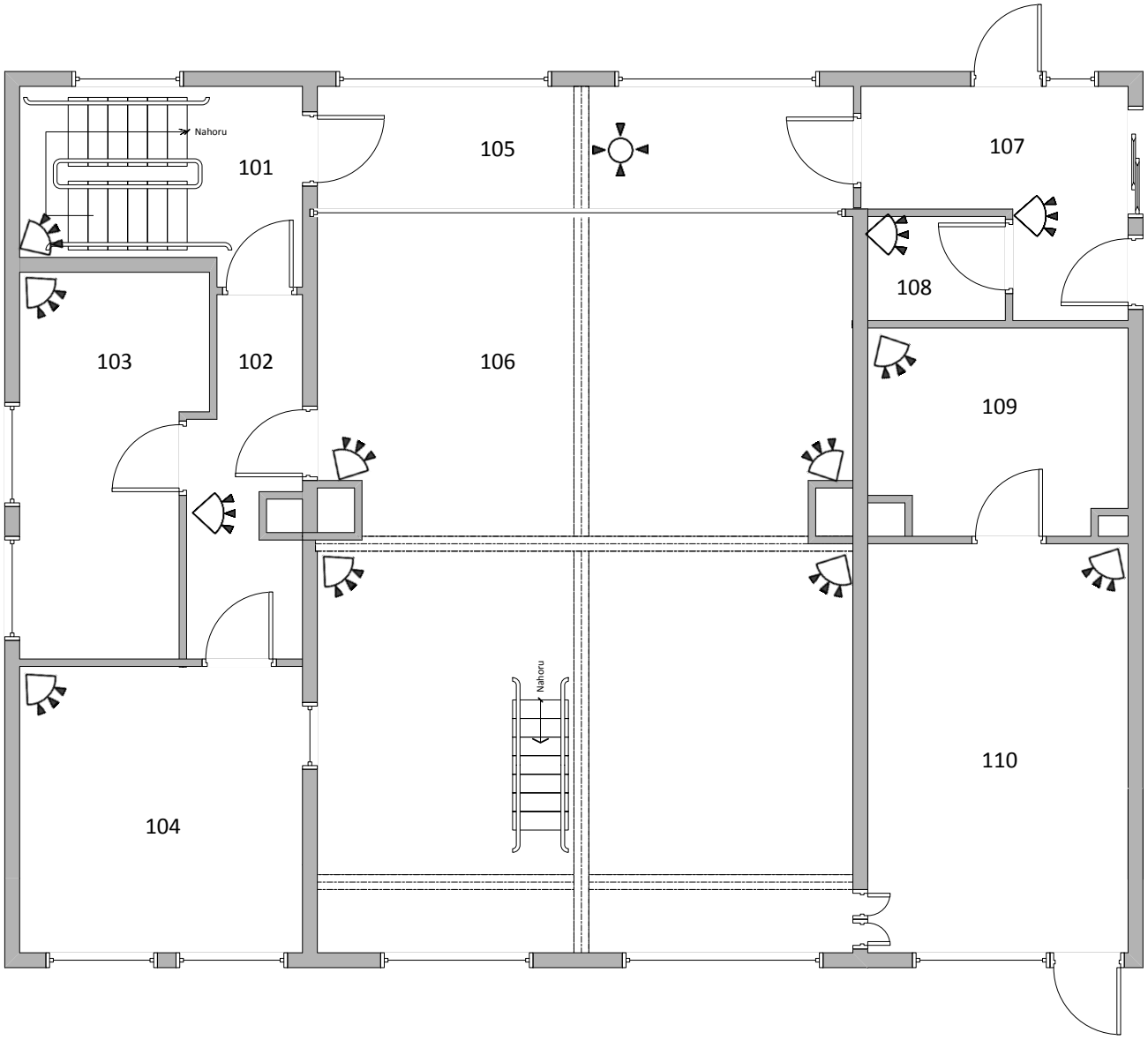
4.patro - střed

EPS a signalizace plynu

- detektor kouře

G - detektor plynu

Příloha 28



Výukové středisko zabývající se výzkumem v chemickém průmyslu

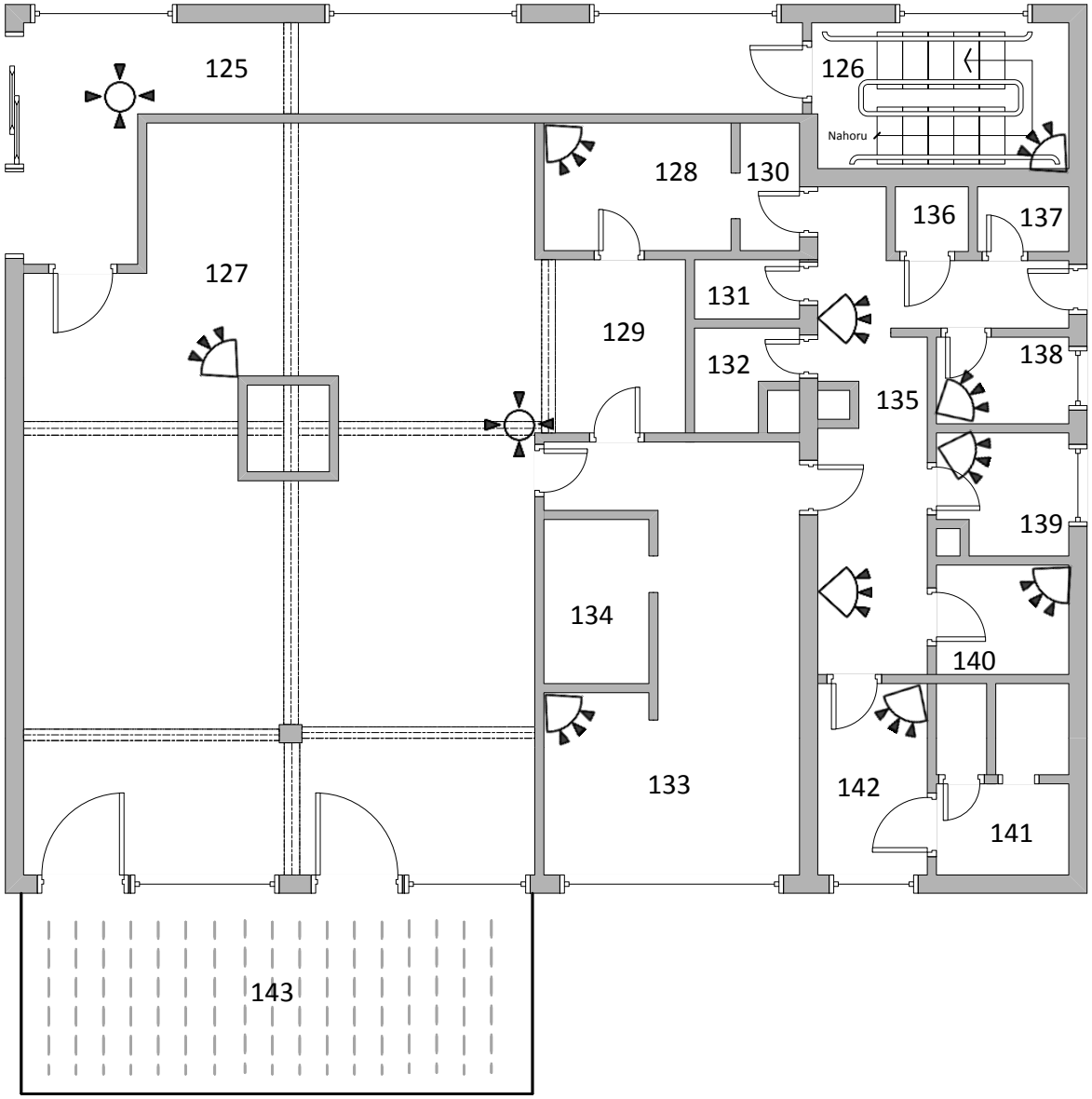
1.patro - levé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 29



Výukové středisko zabývající se výzkumem v chemickém průmyslu

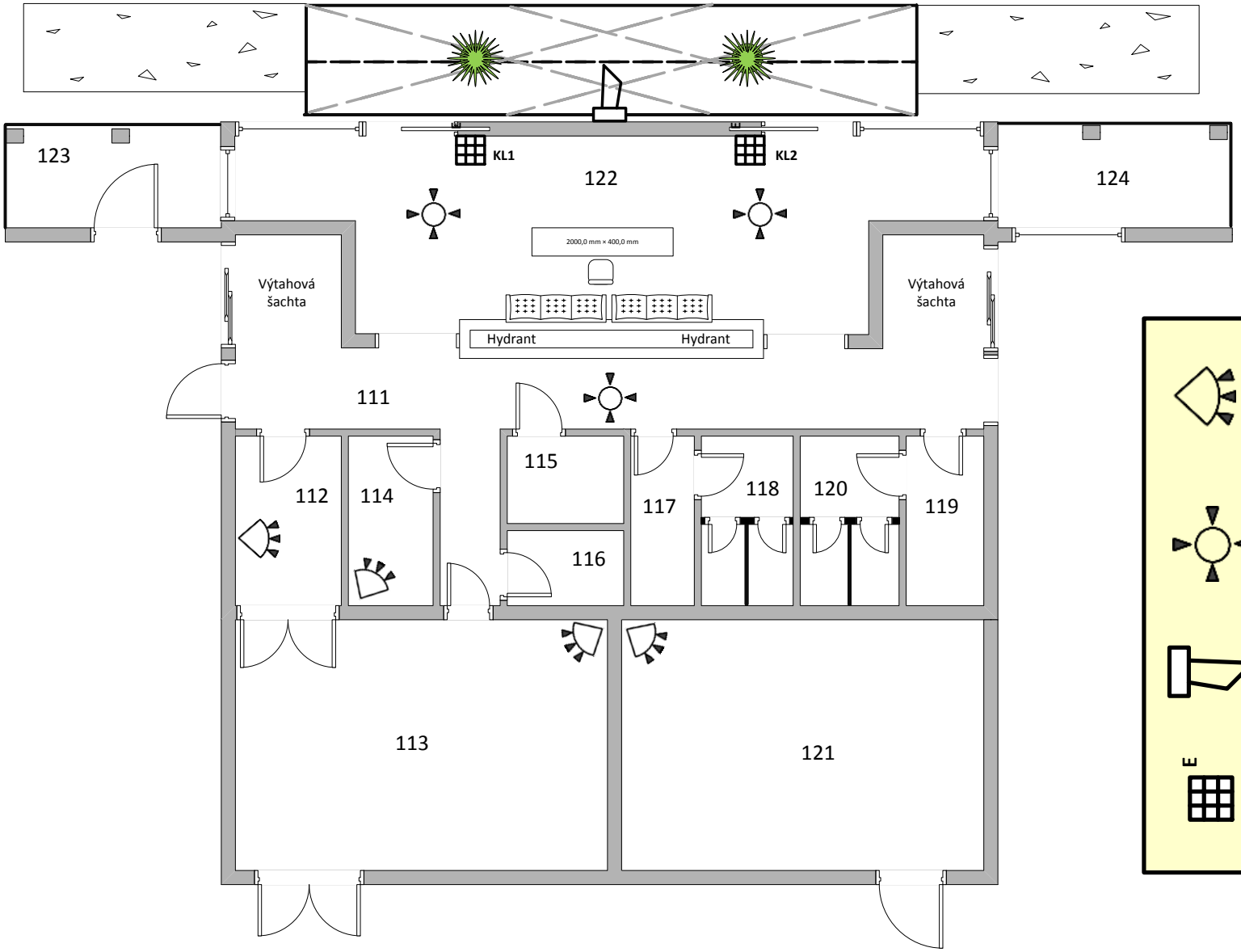
1.patro - pravé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 30



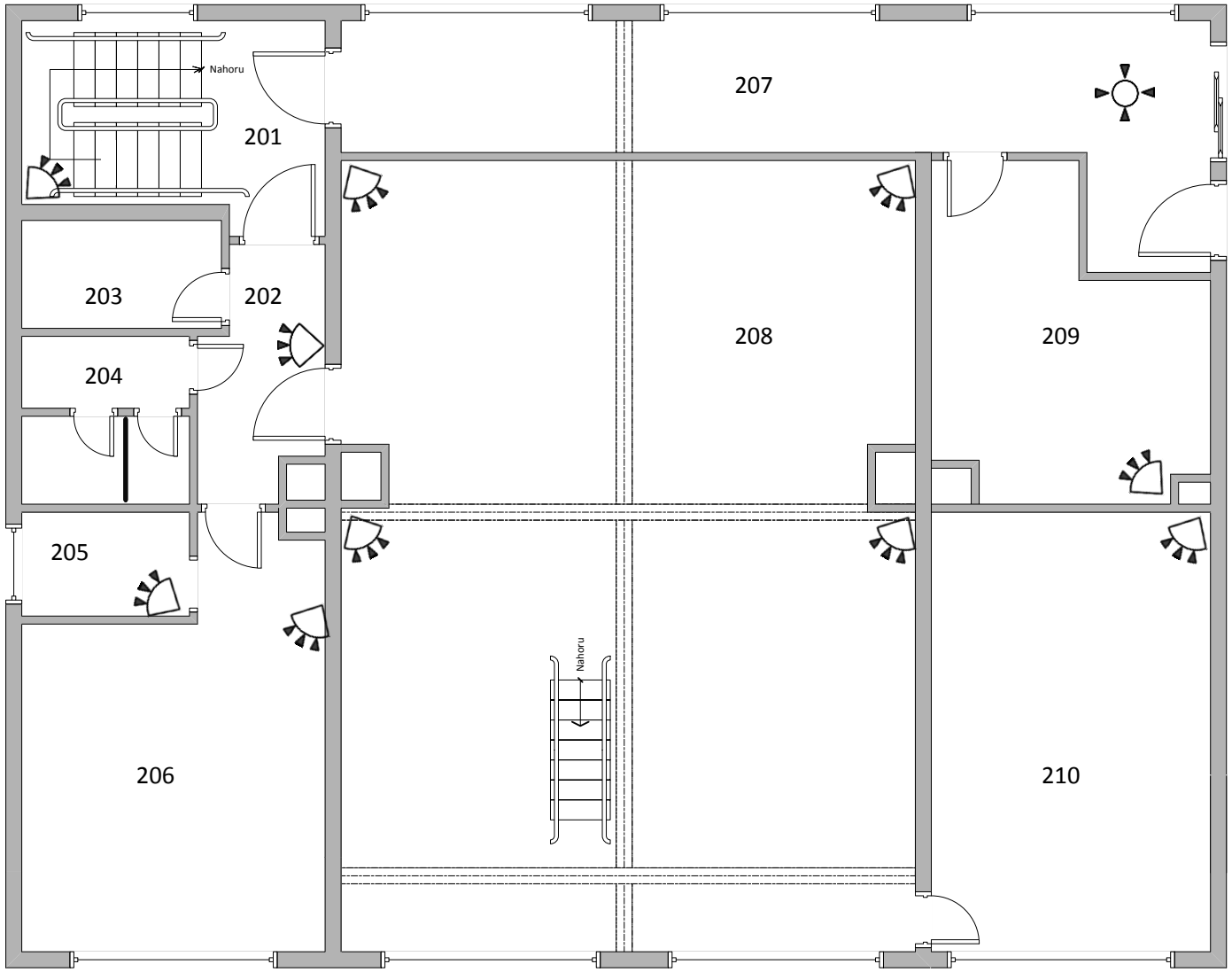
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - střed

EZS

- PIR čidlo
- PIR stropní čidlo (360°)
- siréna
- klávesnice EZS

Příloha 31



Výukové středisko zabývající se výzkumem v chemickém průmyslu

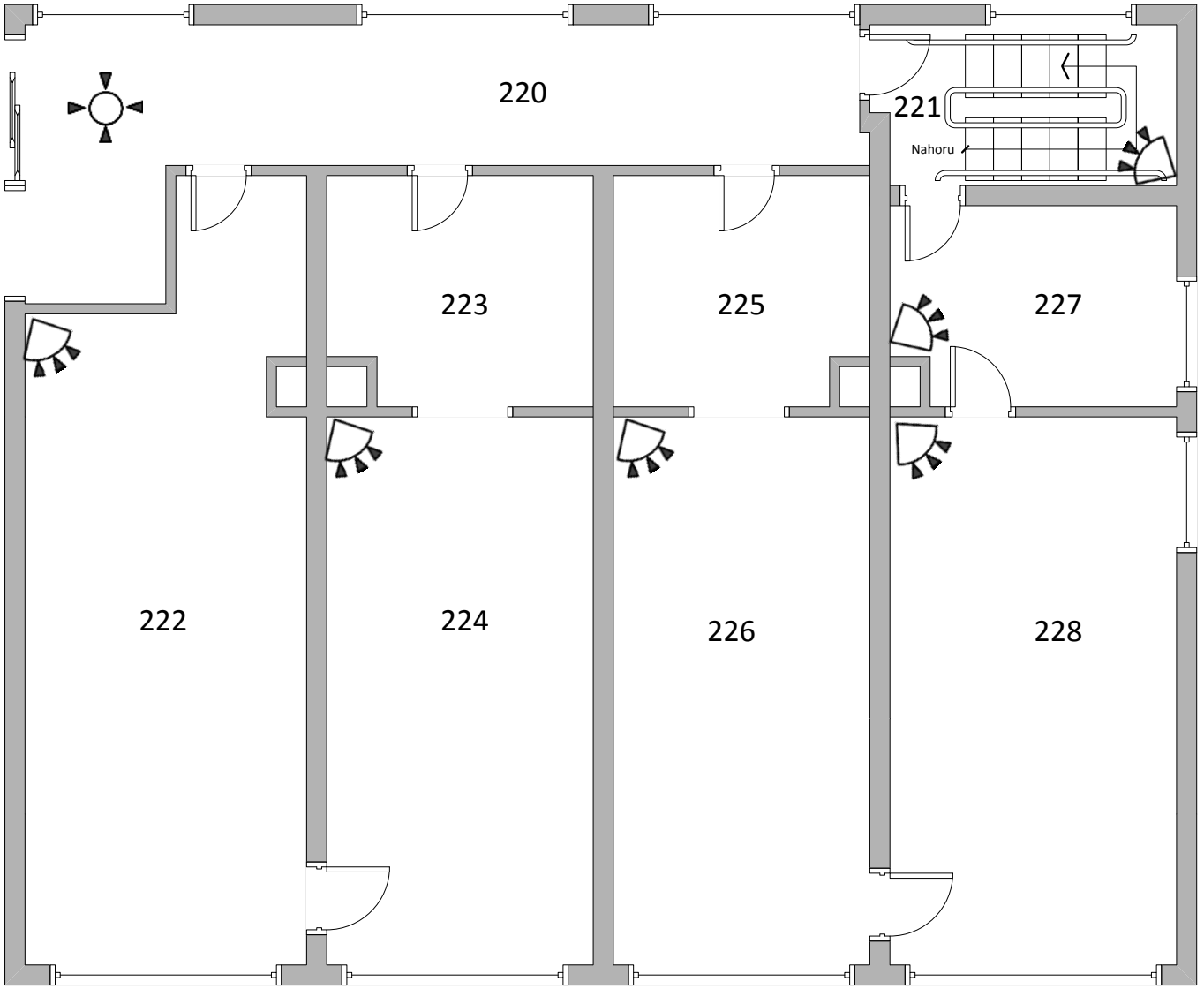
2.patro - levé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 32



Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - pravé křídlo

EZS

- PIR čidlo

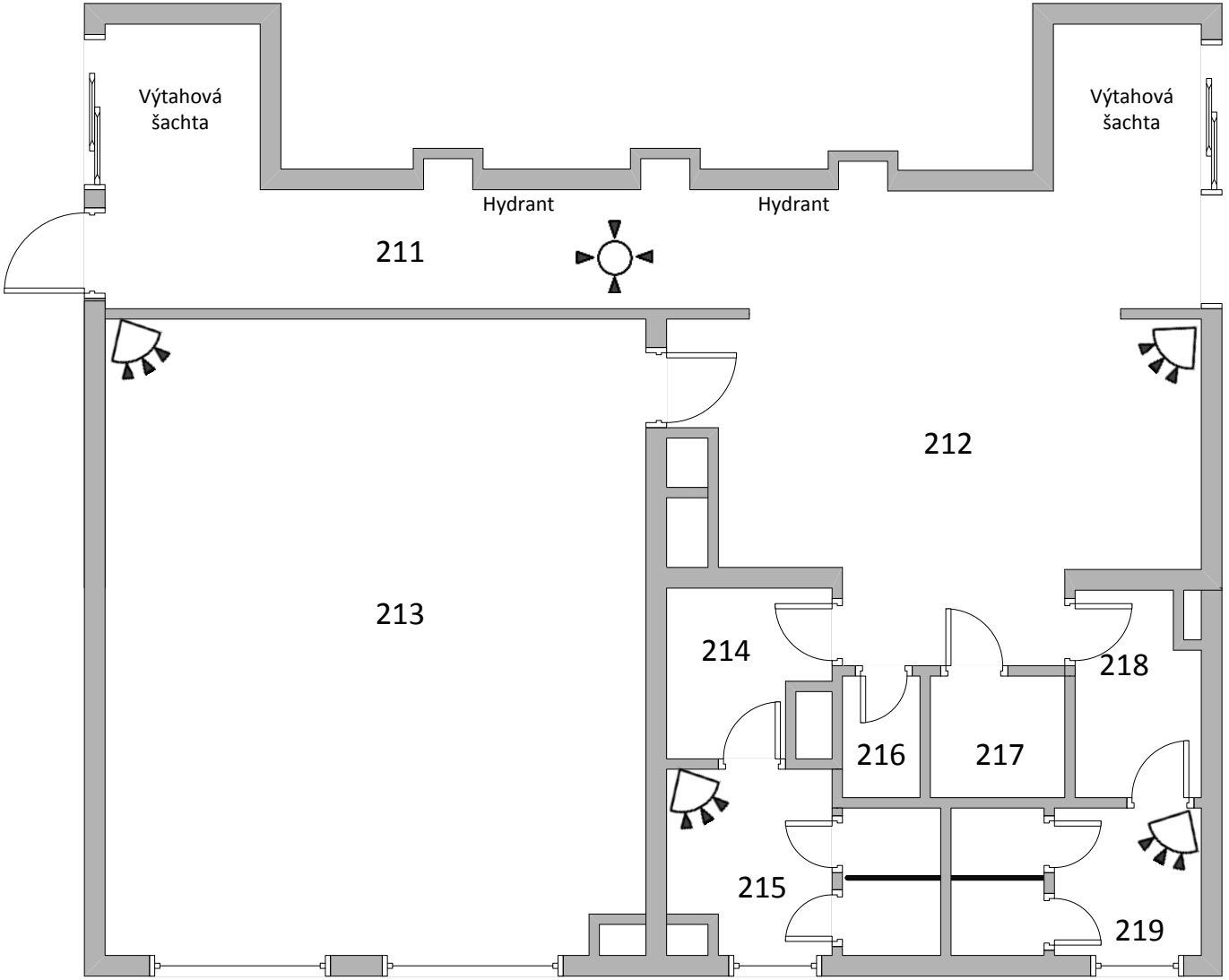
- PIR stropní čidlo (360°)

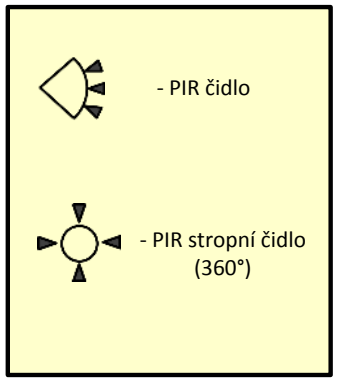
Příloha 33

Výukové středisko zabývající se výzkumem v chemickém průmyslu

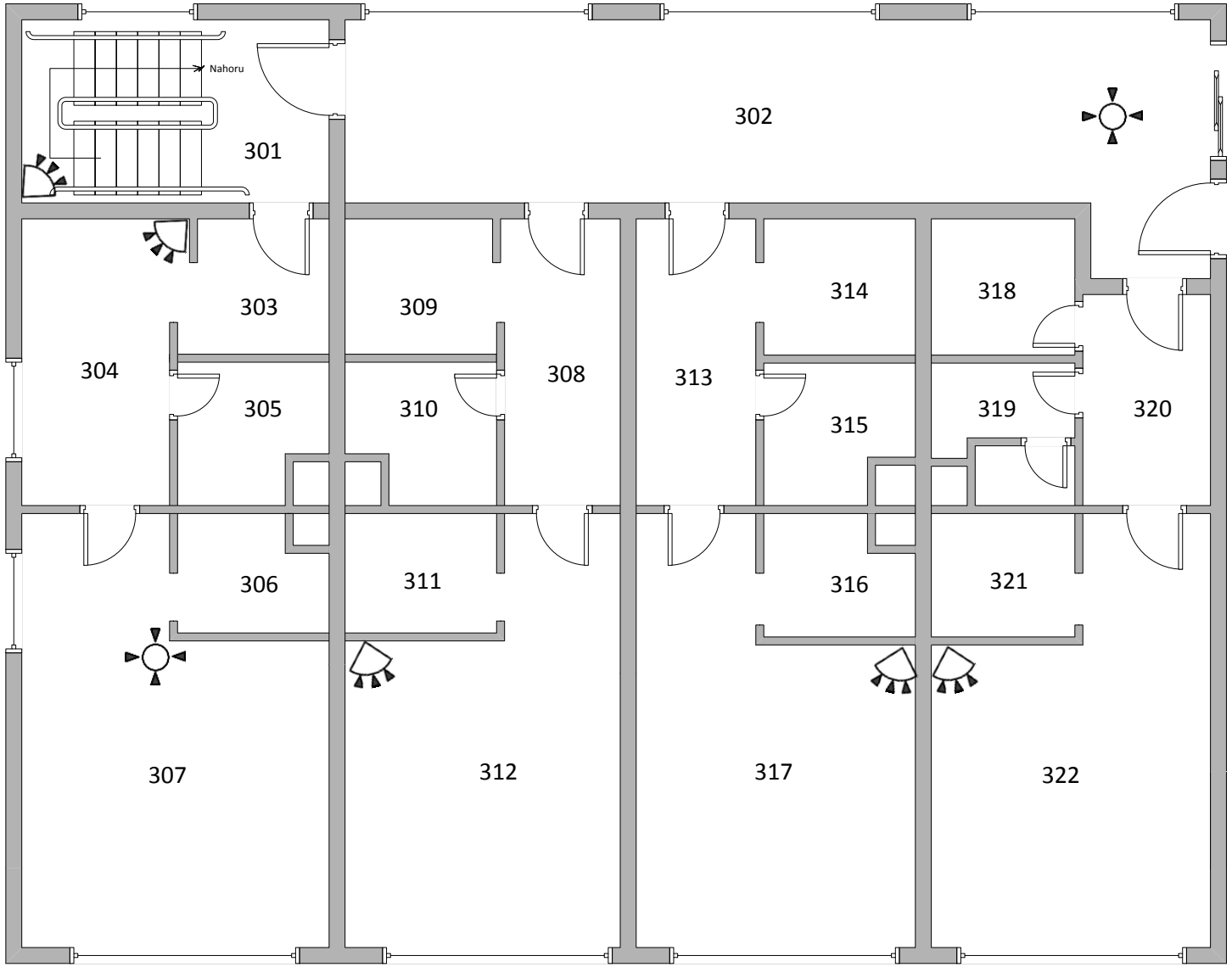
2.patro - střed

EZS





Příloha 34



Výukové středisko zabývající se výzkumem v chemickém průmyslu

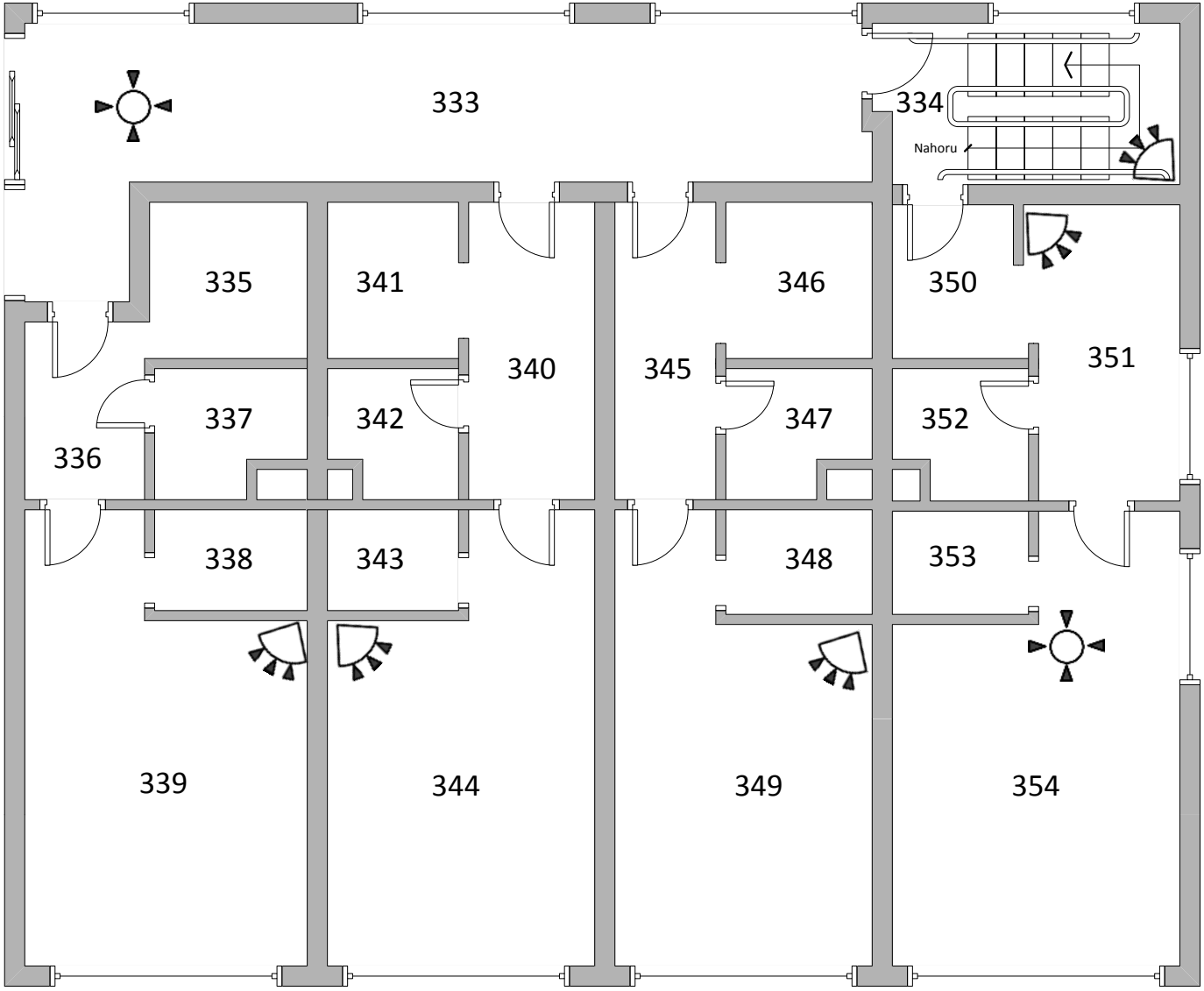
3.patro - levé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 35



Výukové středisko zabývající se výzkumem v chemickém průmyslu

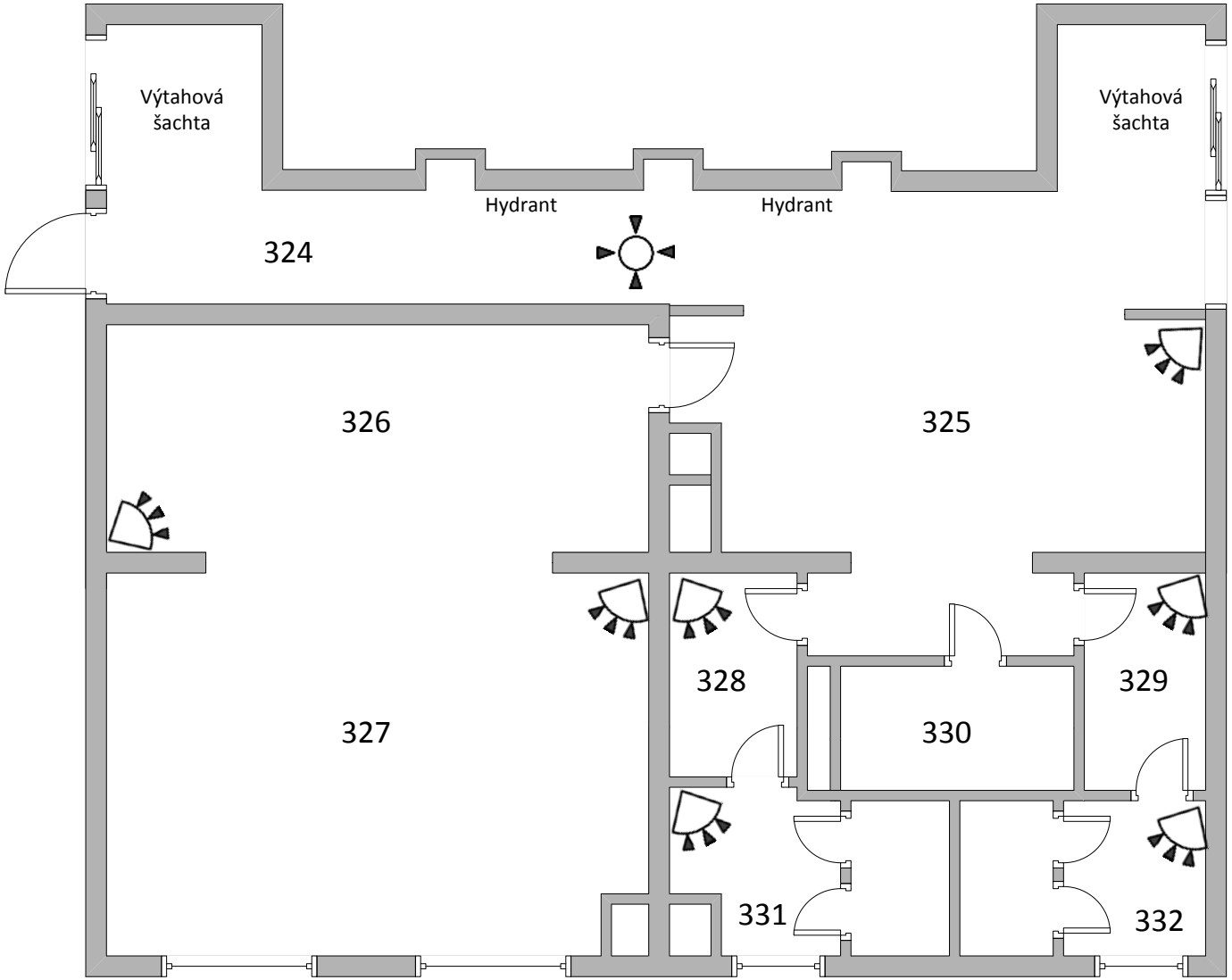
3.patro - pravé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 36



Výukové středisko zabývající se výzkumem v chemickém průmyslu

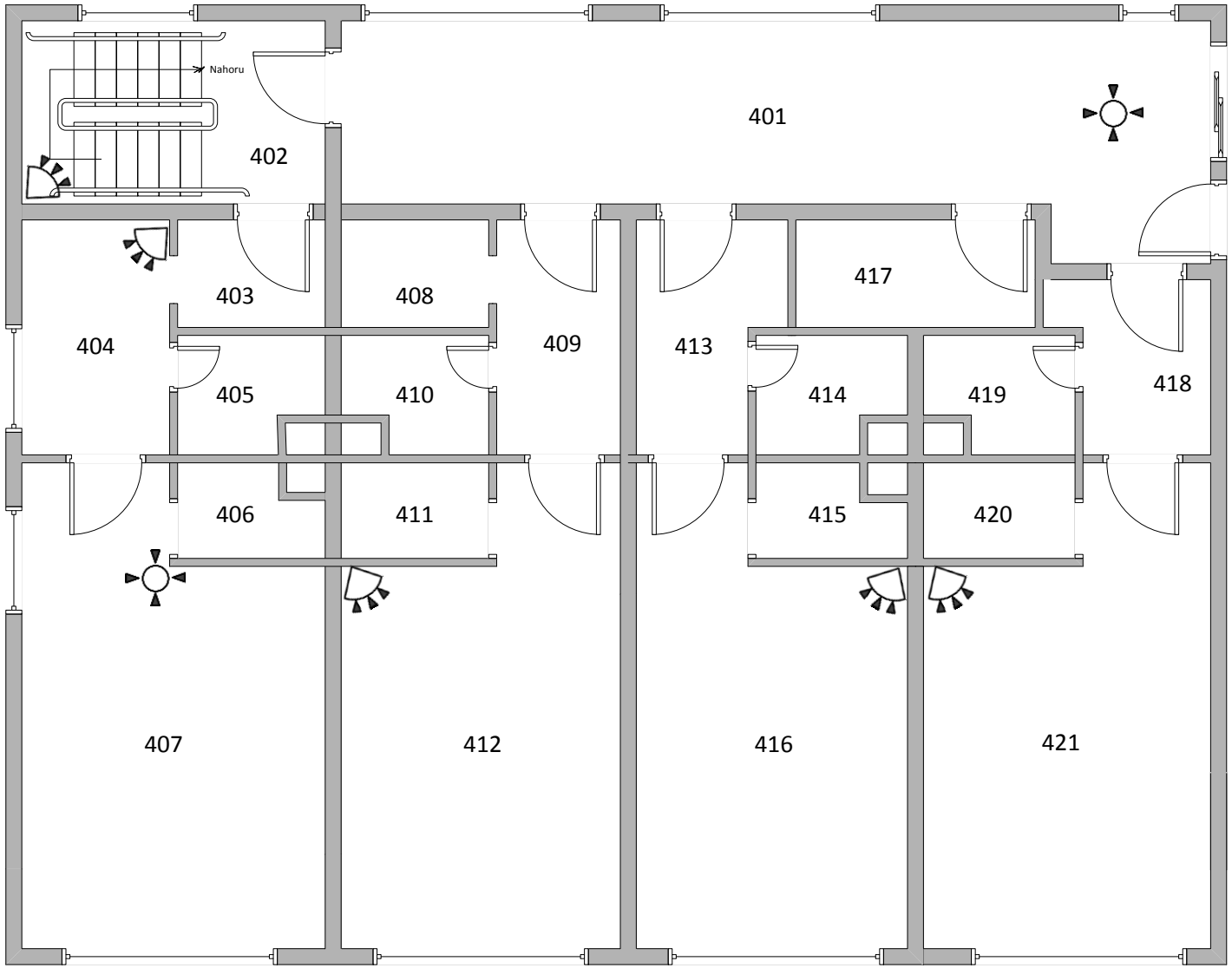
3.patro - střed

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 37



Výukové středisko zabývající se výzkumem v chemickém průmyslu

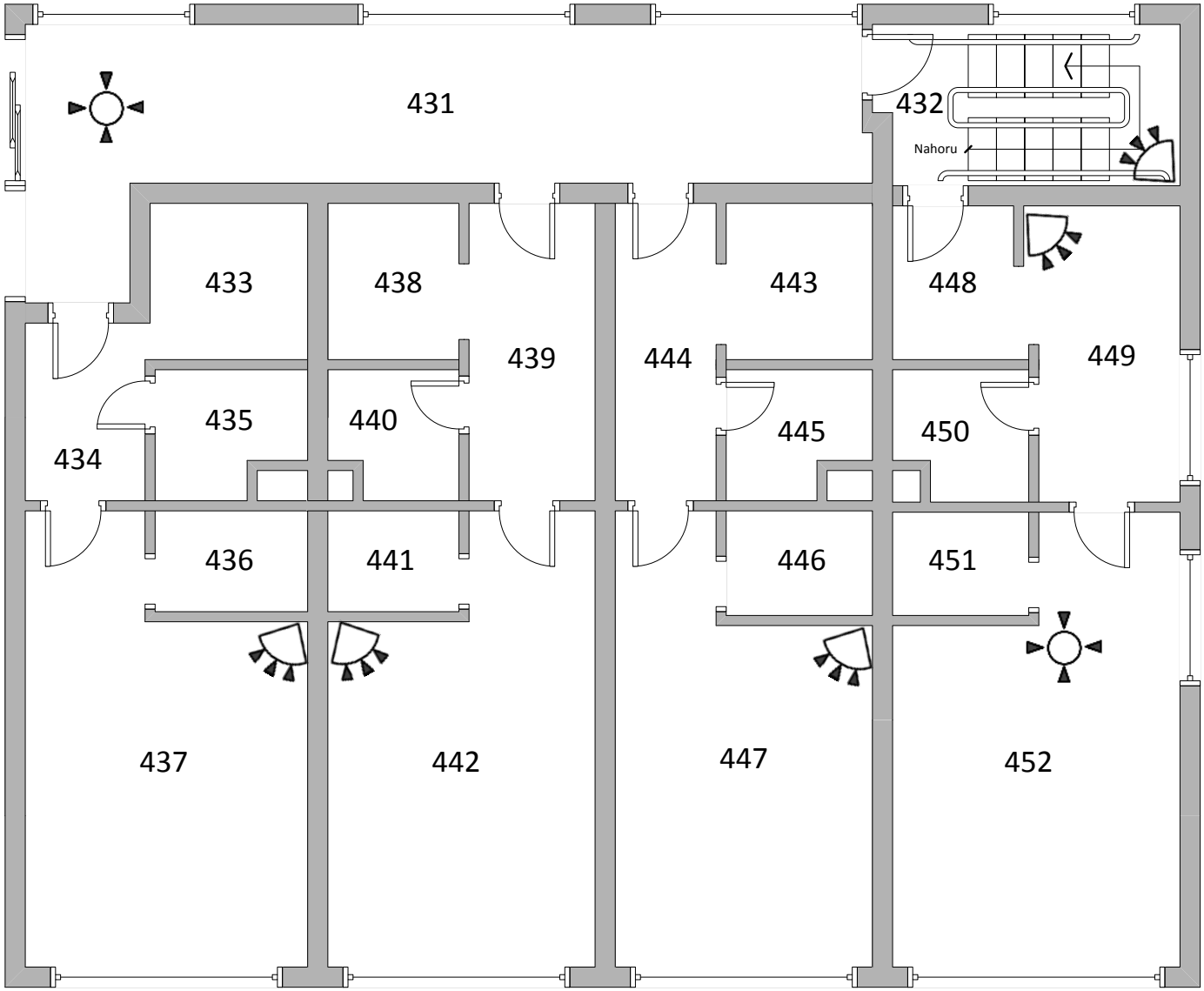
4.patro - levé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 38



Výukové středisko zabývající se výzkumem v chemickém průmyslu

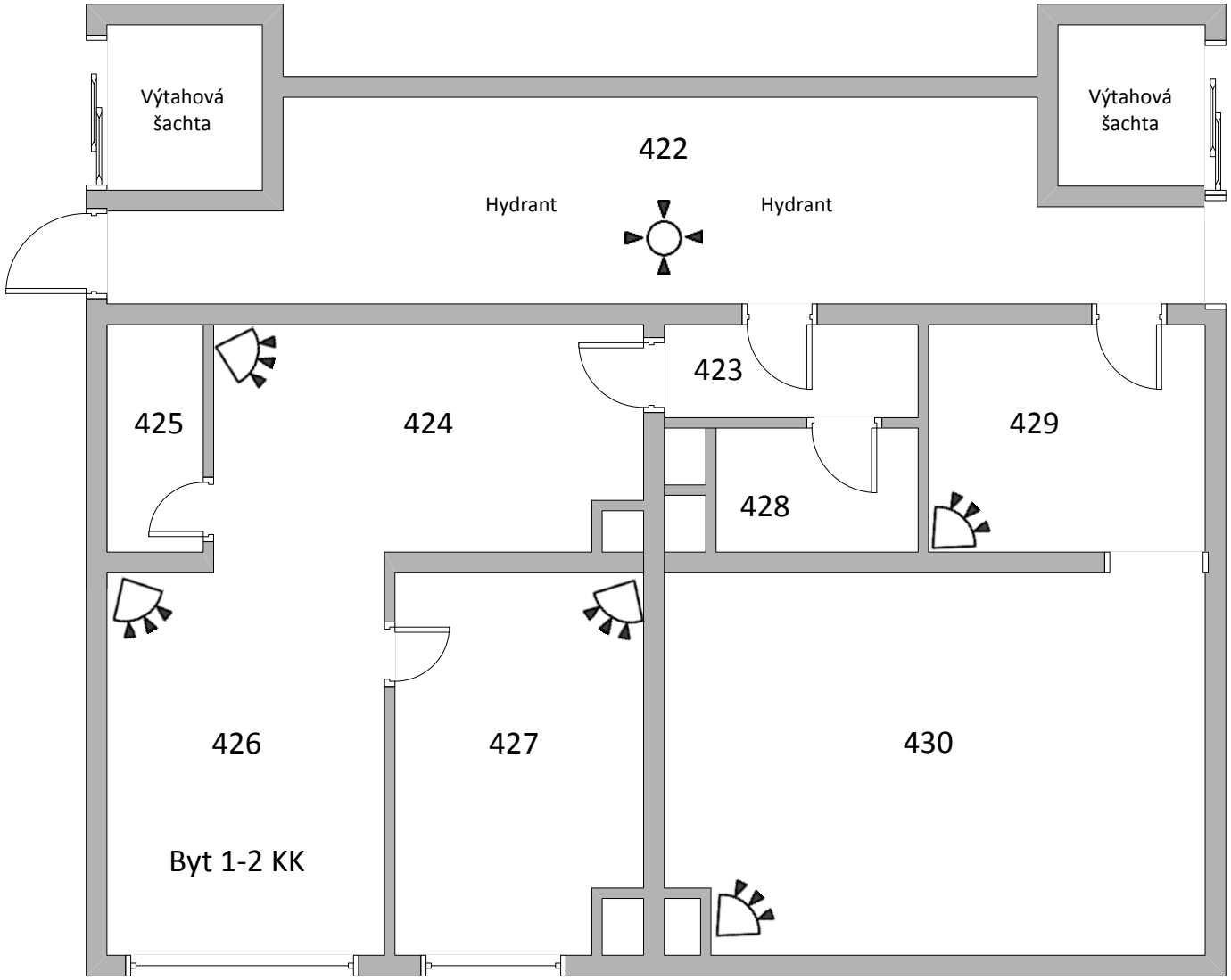
4.patro - pravé křídlo

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

Příloha 39



Výukové středisko zabývající se výzkumem v chemickém průmyslu

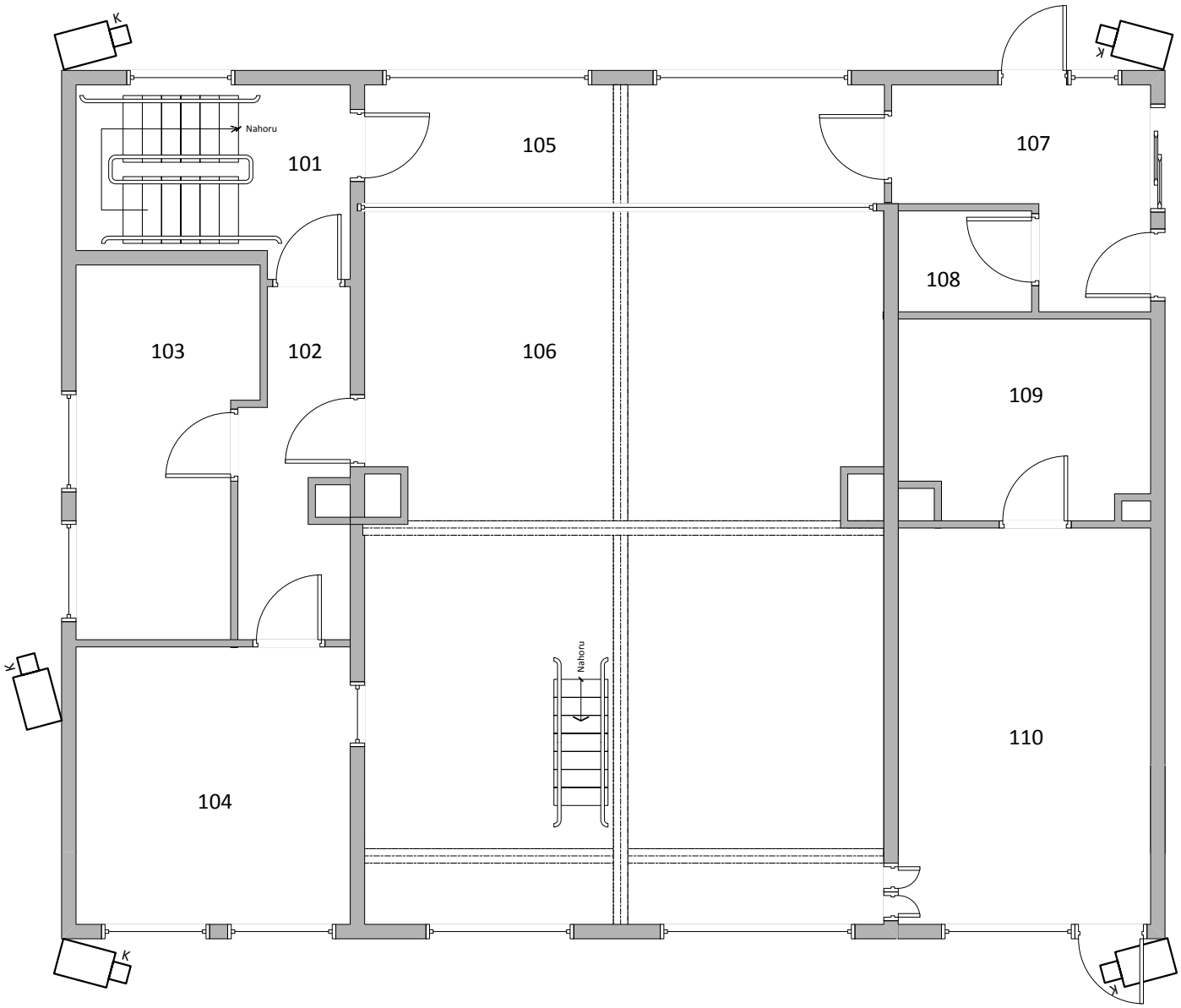
4.patro - střed

EZS

- PIR čidlo

- PIR stropní čidlo (360°)

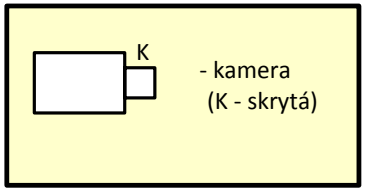
Příloha 40



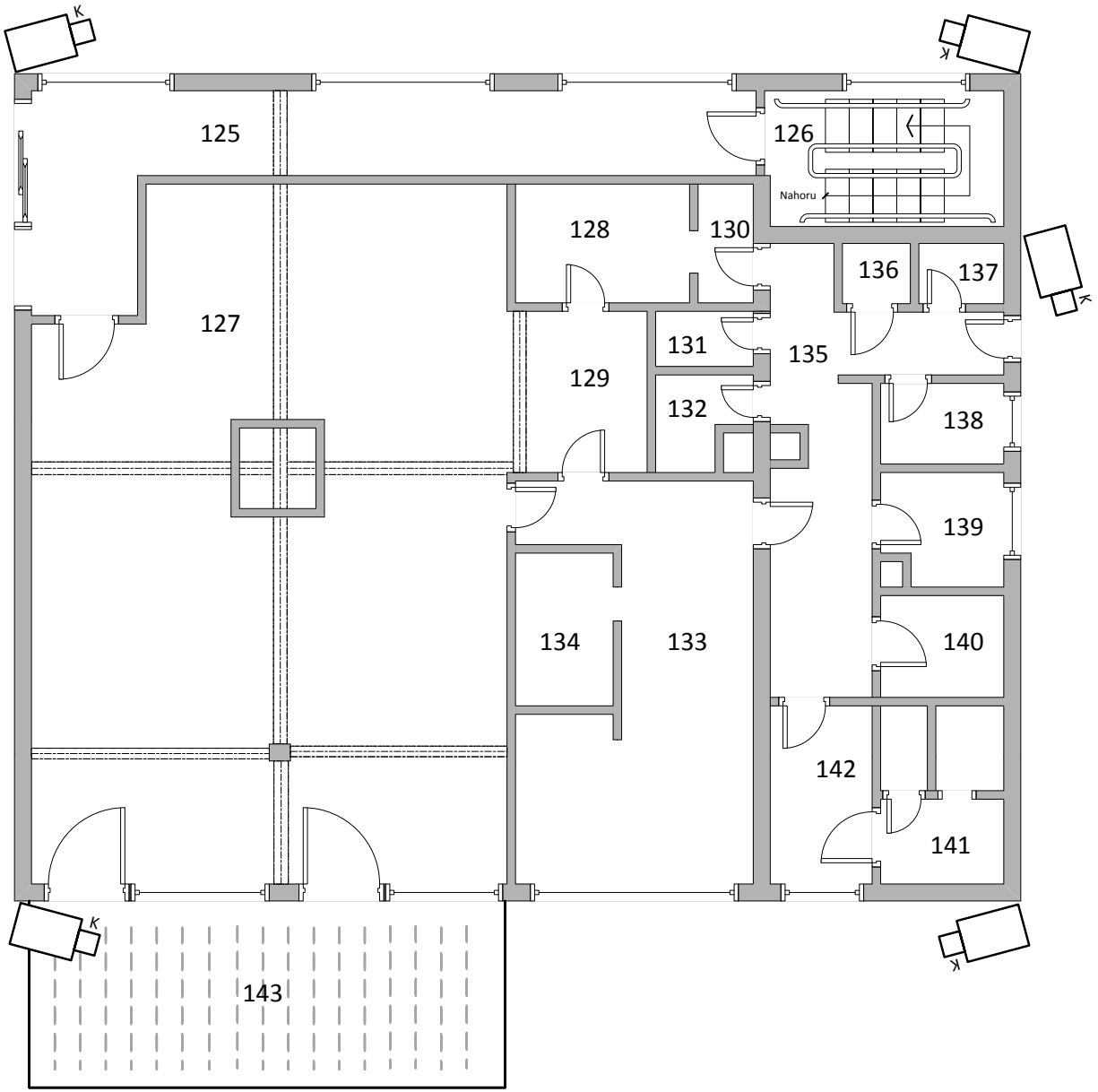
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - levé křídlo

Kamerový systém



Příloha 41



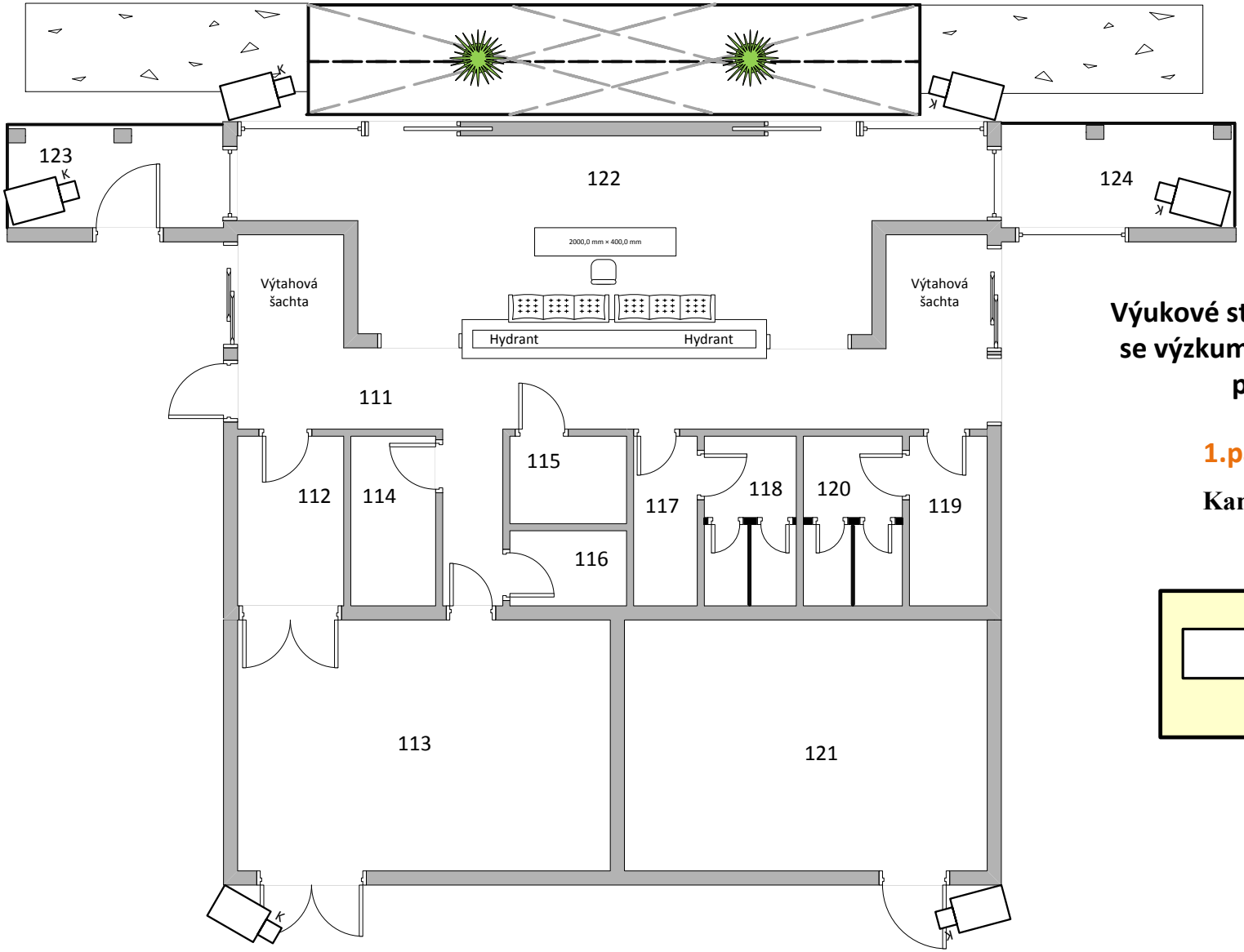
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - pravé křídlo

Kamerový systém

K - kamera
(K - skrytá)

Příloha 42



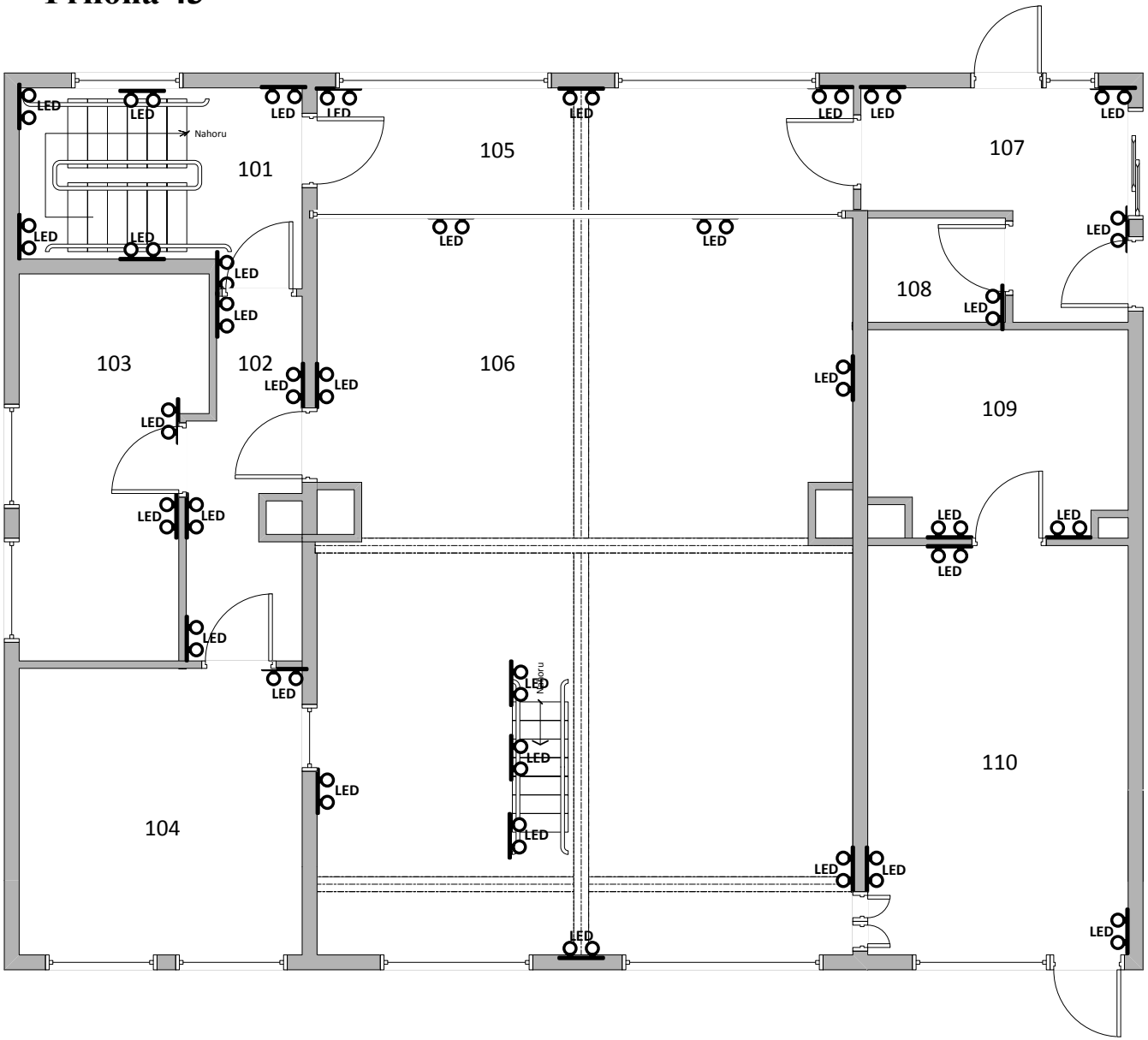
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - střed

Kamerový systém

K - kamera
(K - skrytá)

Příloha 43



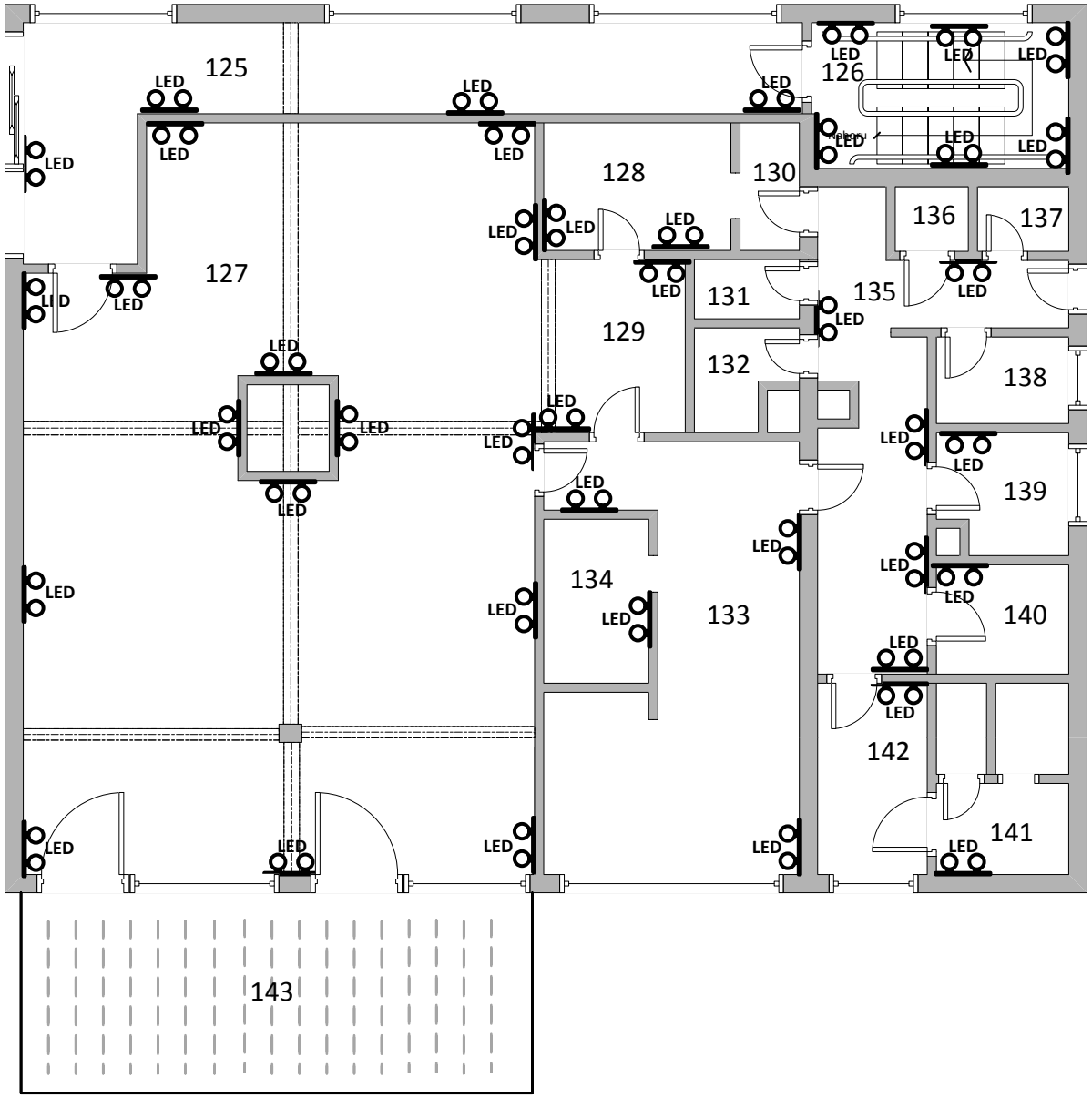
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - levé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 44



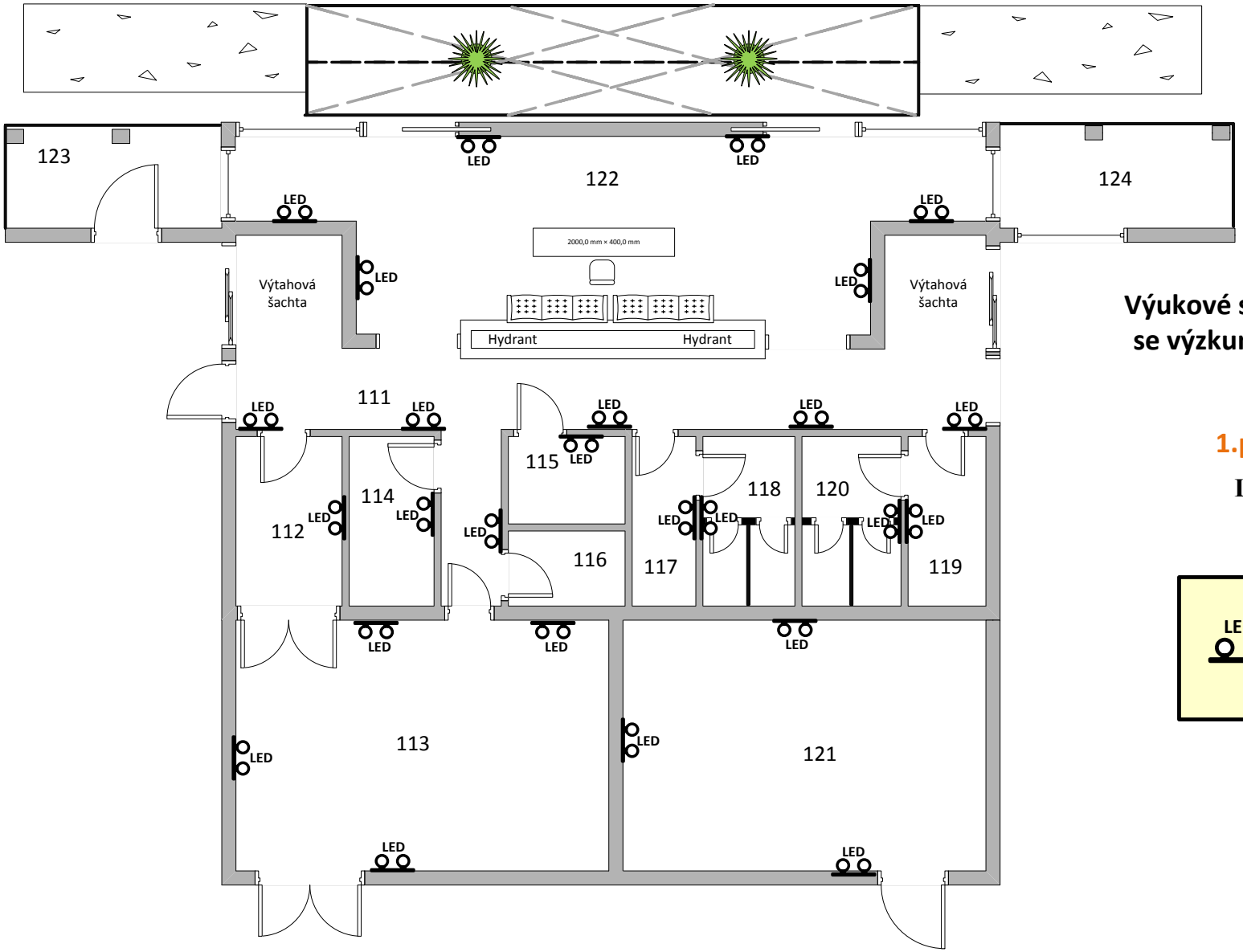
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - pravé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 45



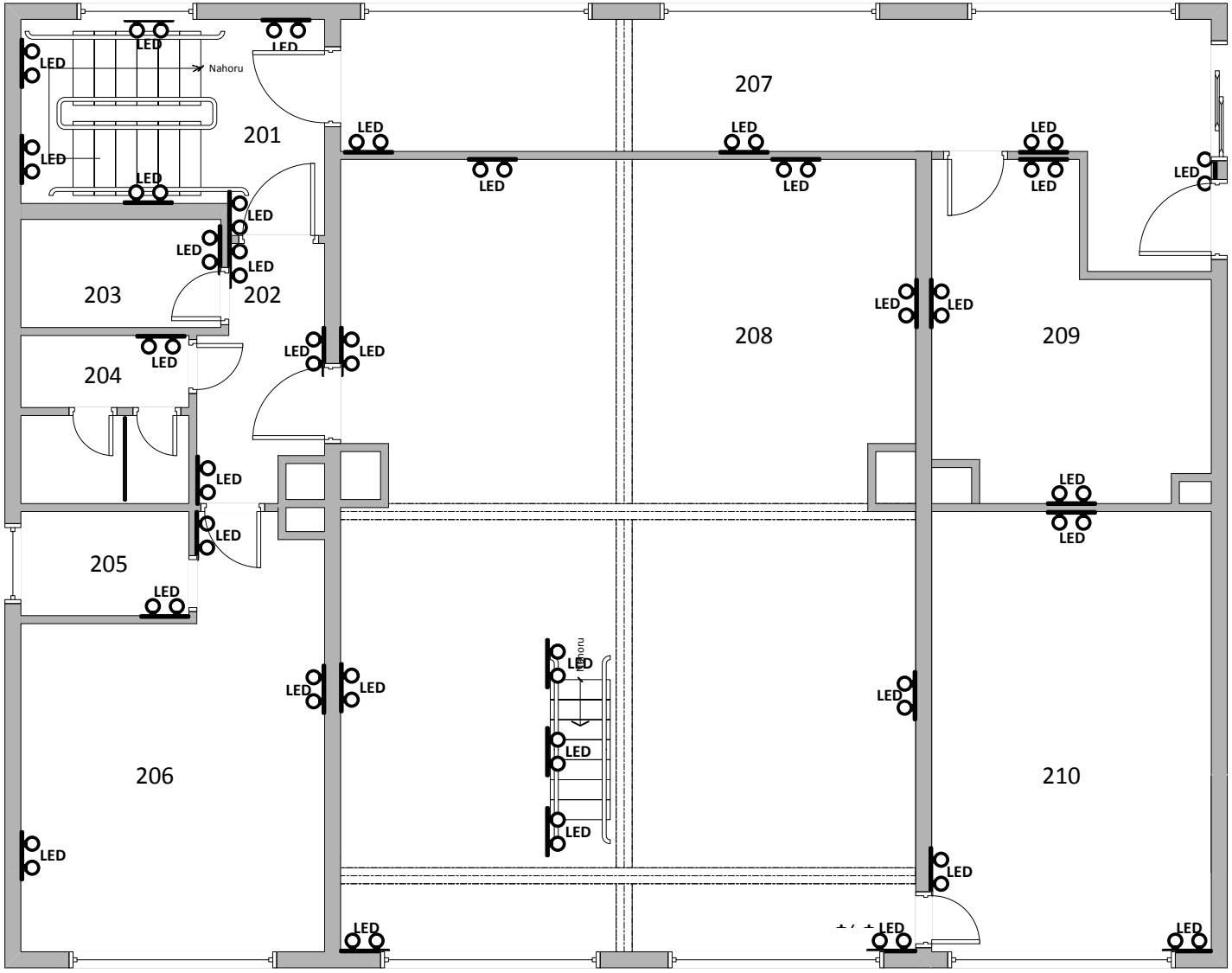
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - střed

LED osvětlení

LED - LED osvětlení

Příloha 46



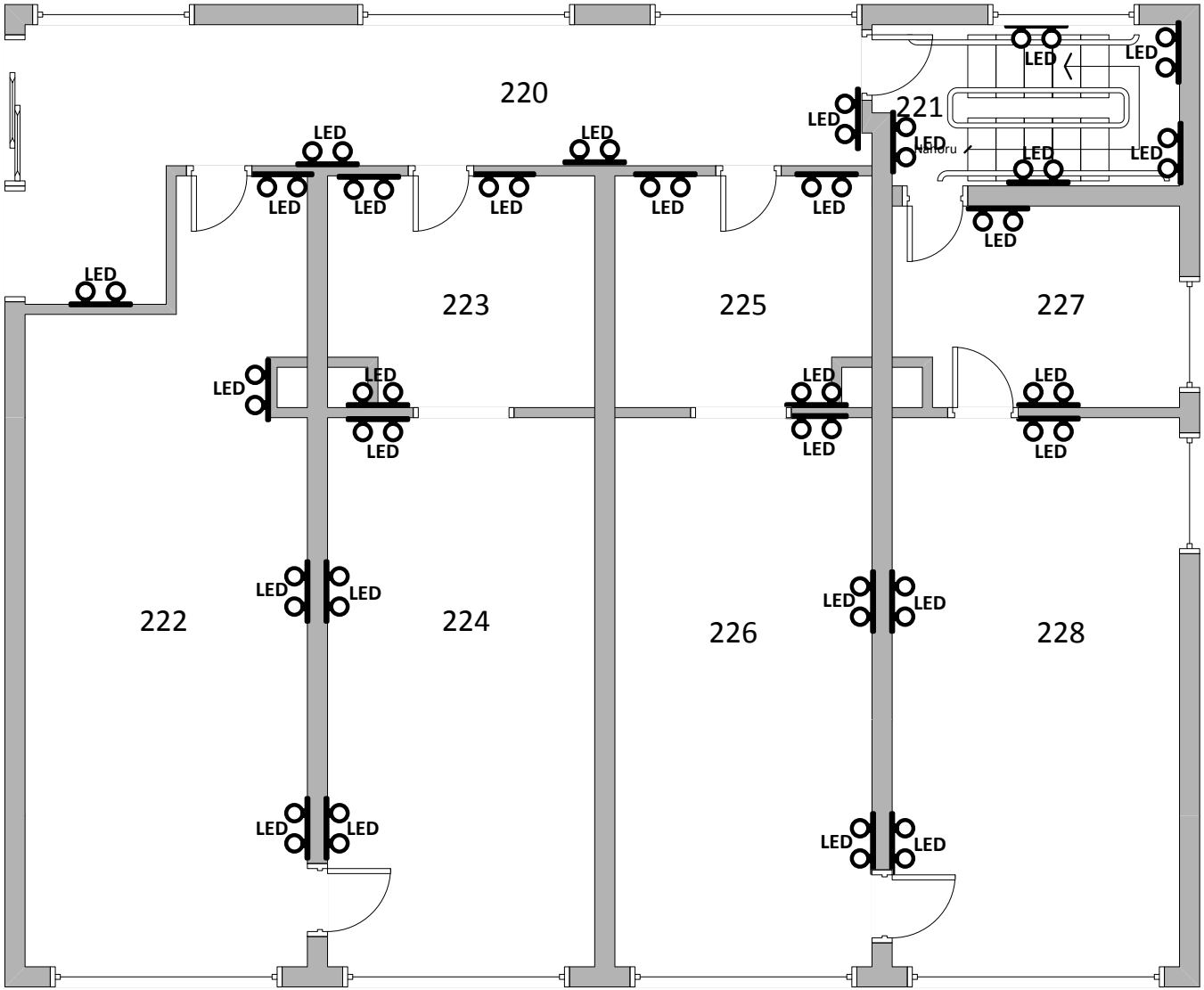
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - levé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 47



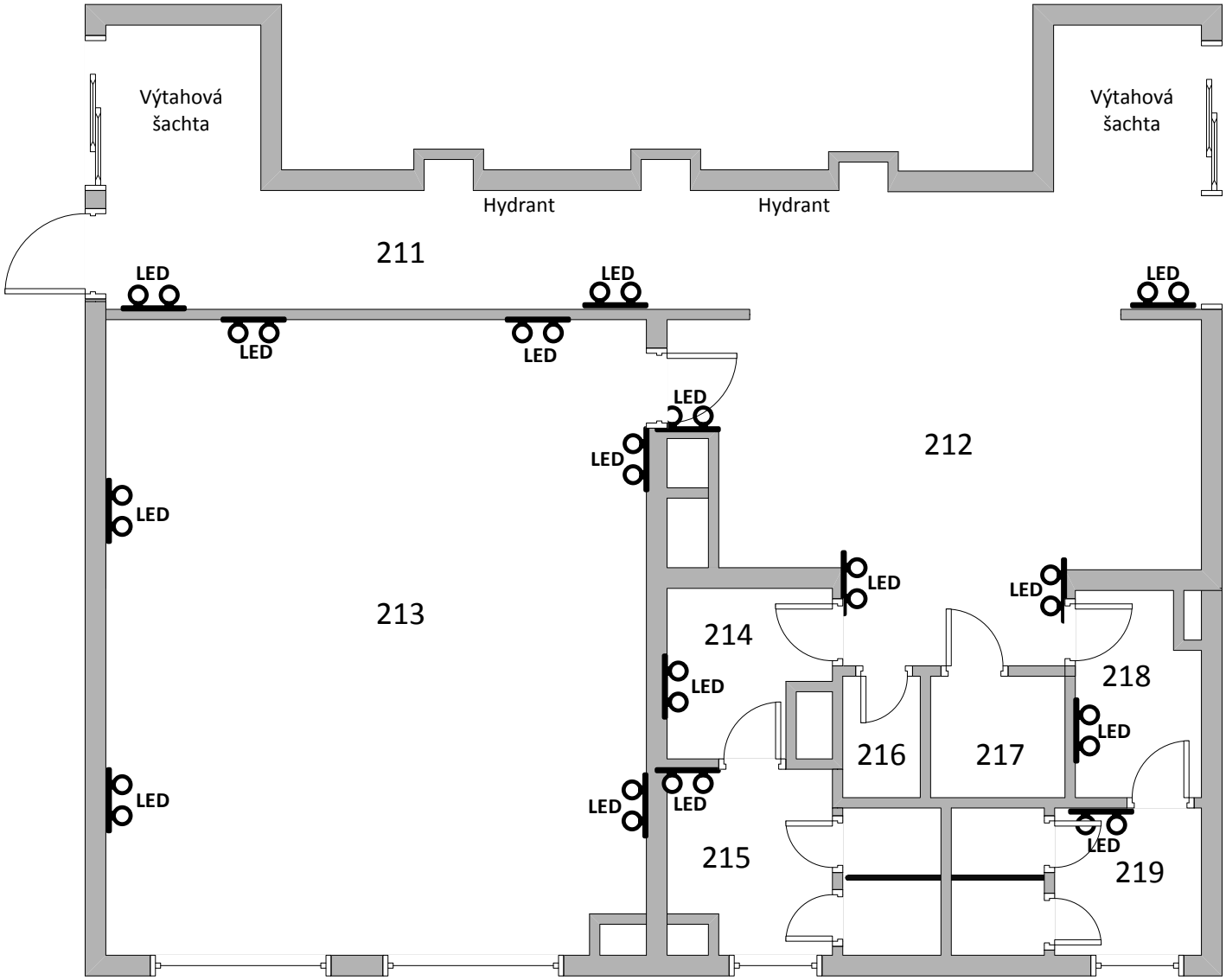
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - pravé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 48



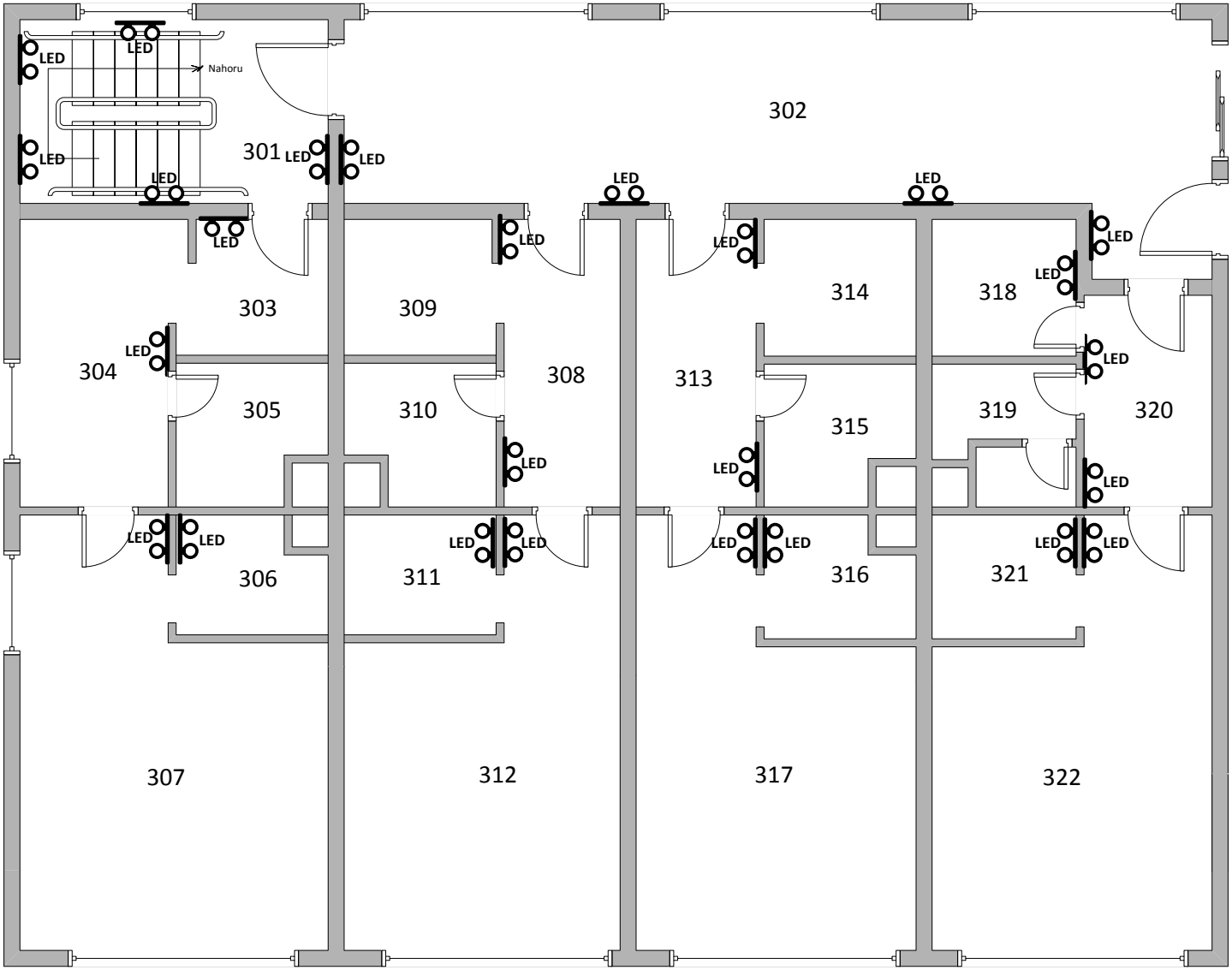
Výukové středisko zabývající se výzkumem v chemickém průmyslu

2.patro - střed

LED osvětlení

LED - LED osvětlení

Příloha 49



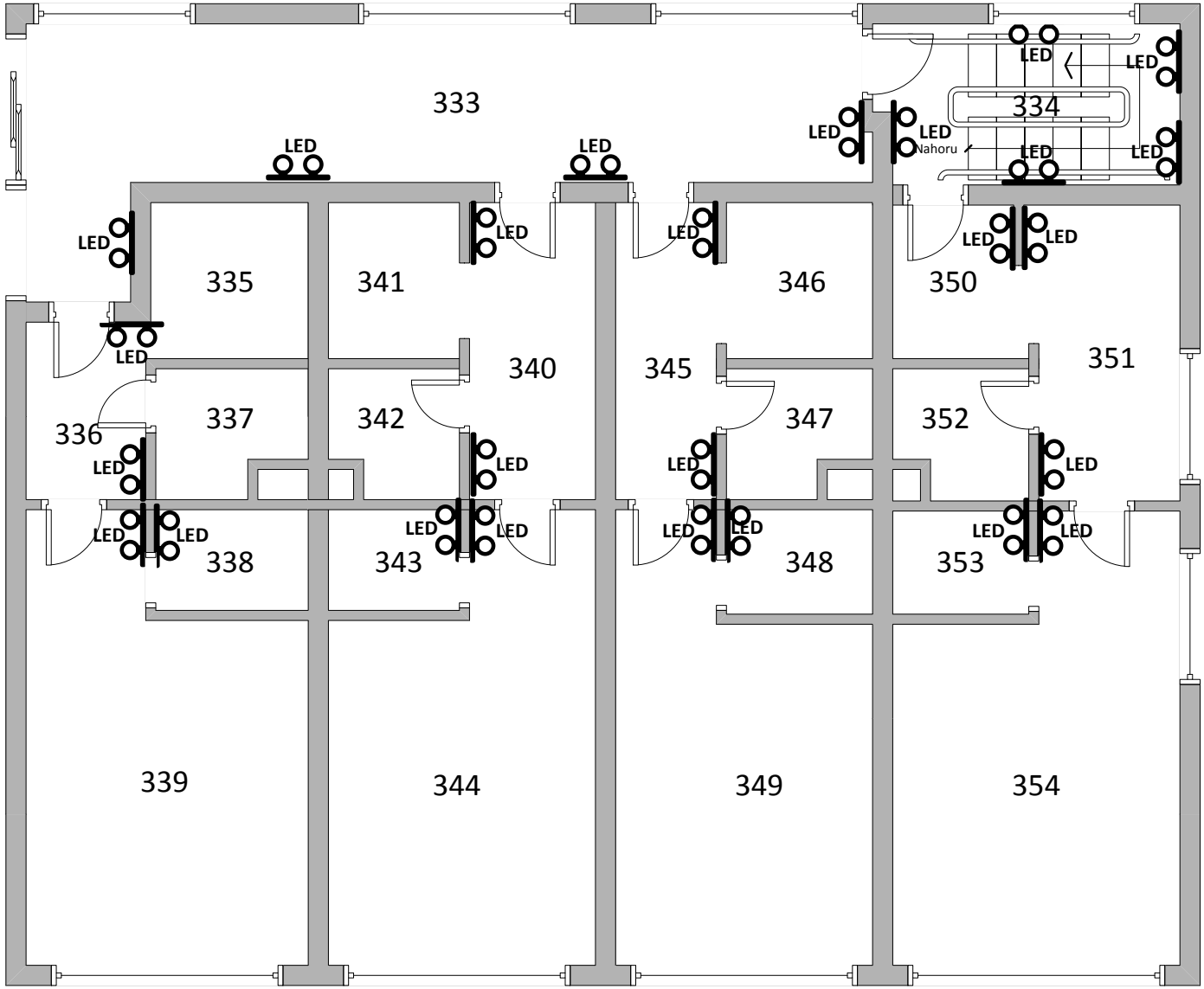
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - levé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 50



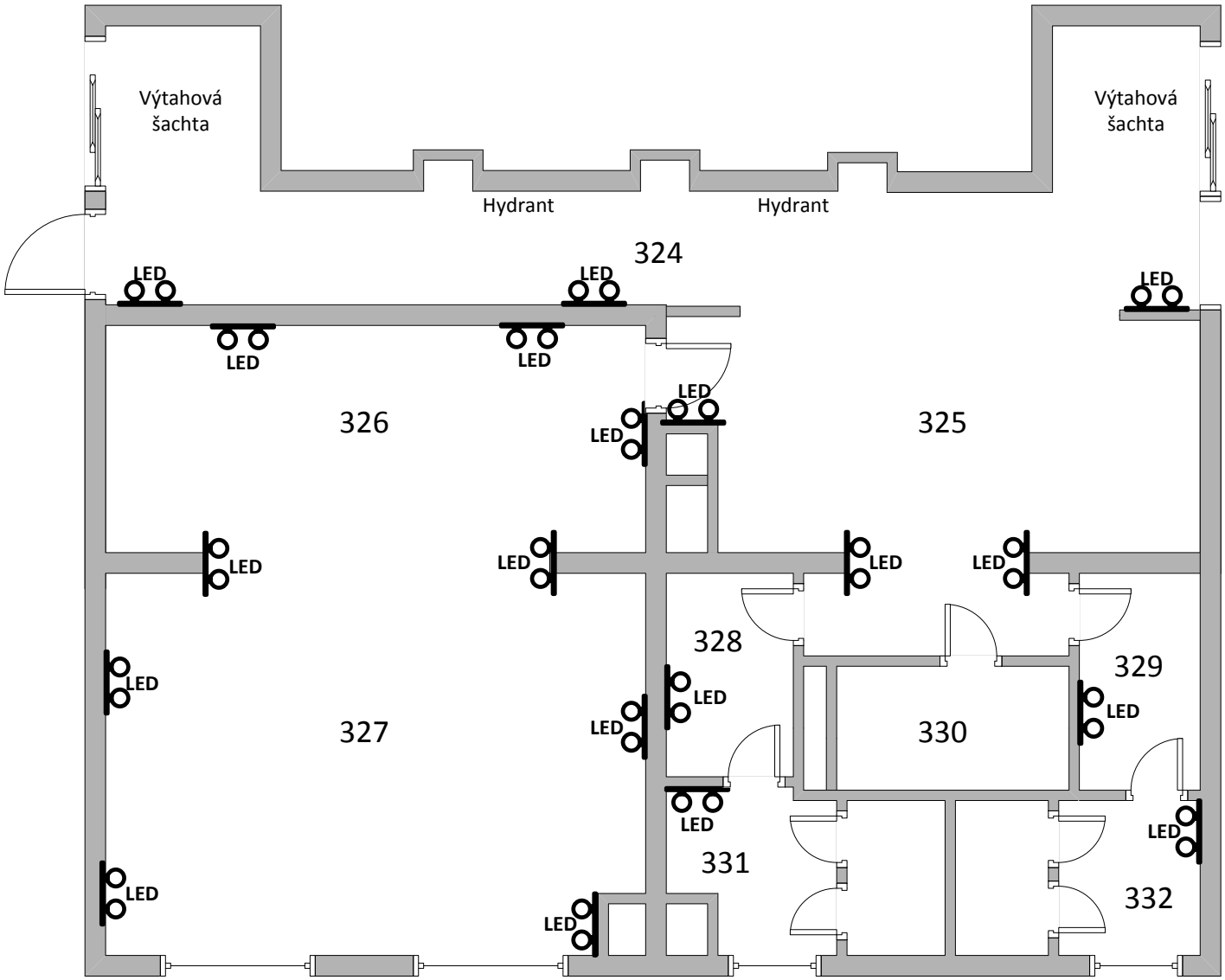
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - pravé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 51



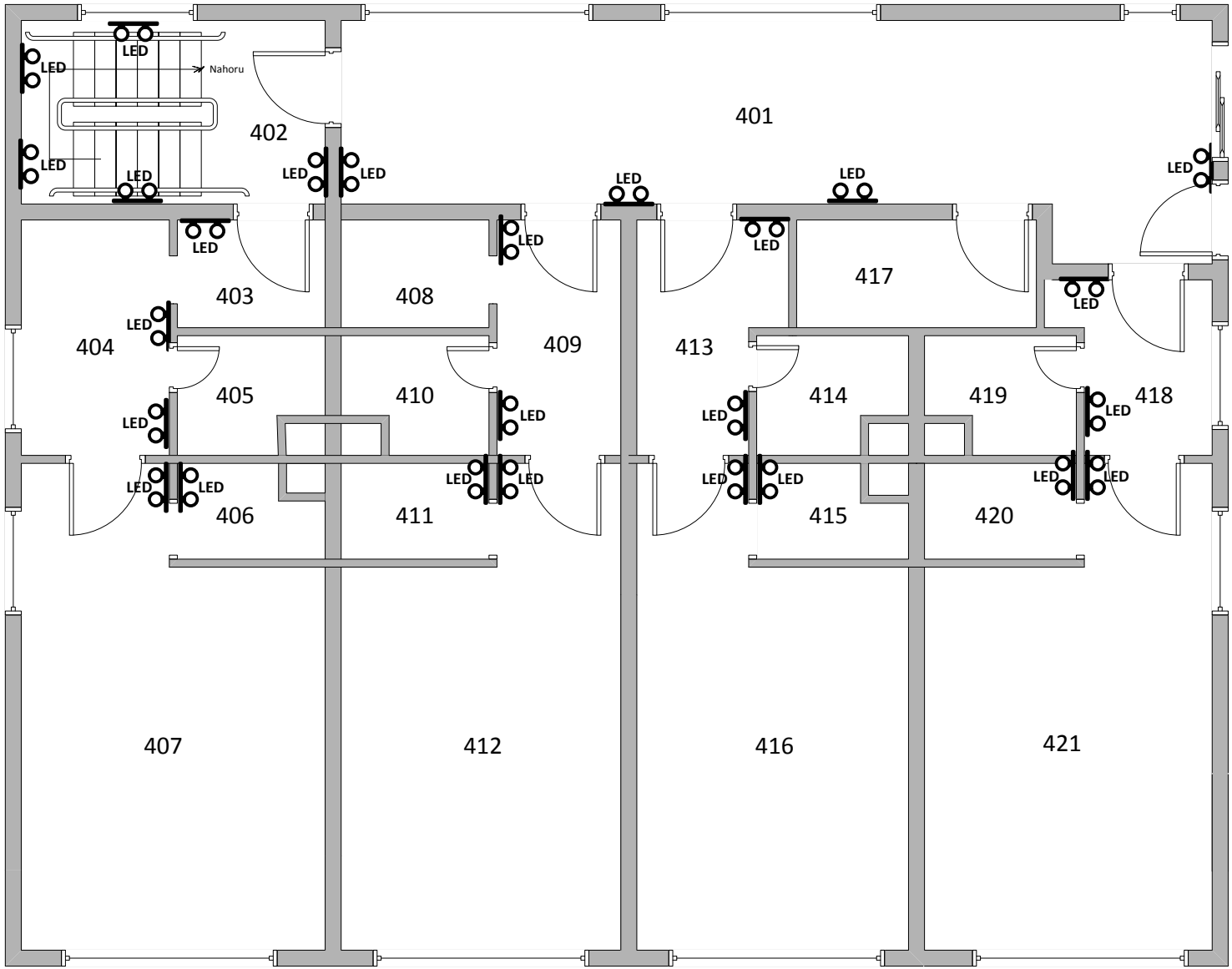
Výukové středisko zabývající se výzkumem v chemickém průmyslu

3.patro - střed

LED osvětlení

LED - LED osvětlení

Příloha 52



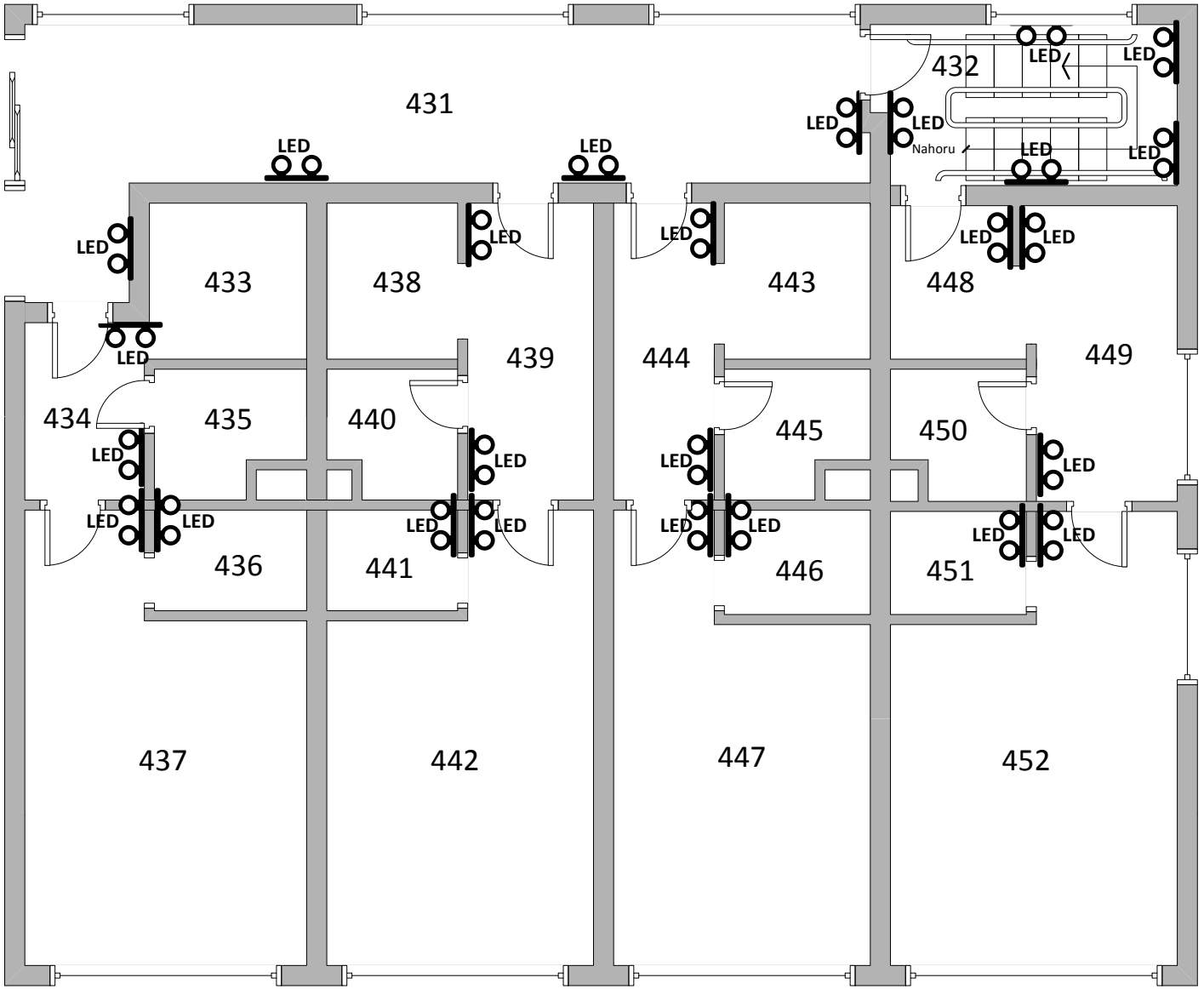
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - levé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 53



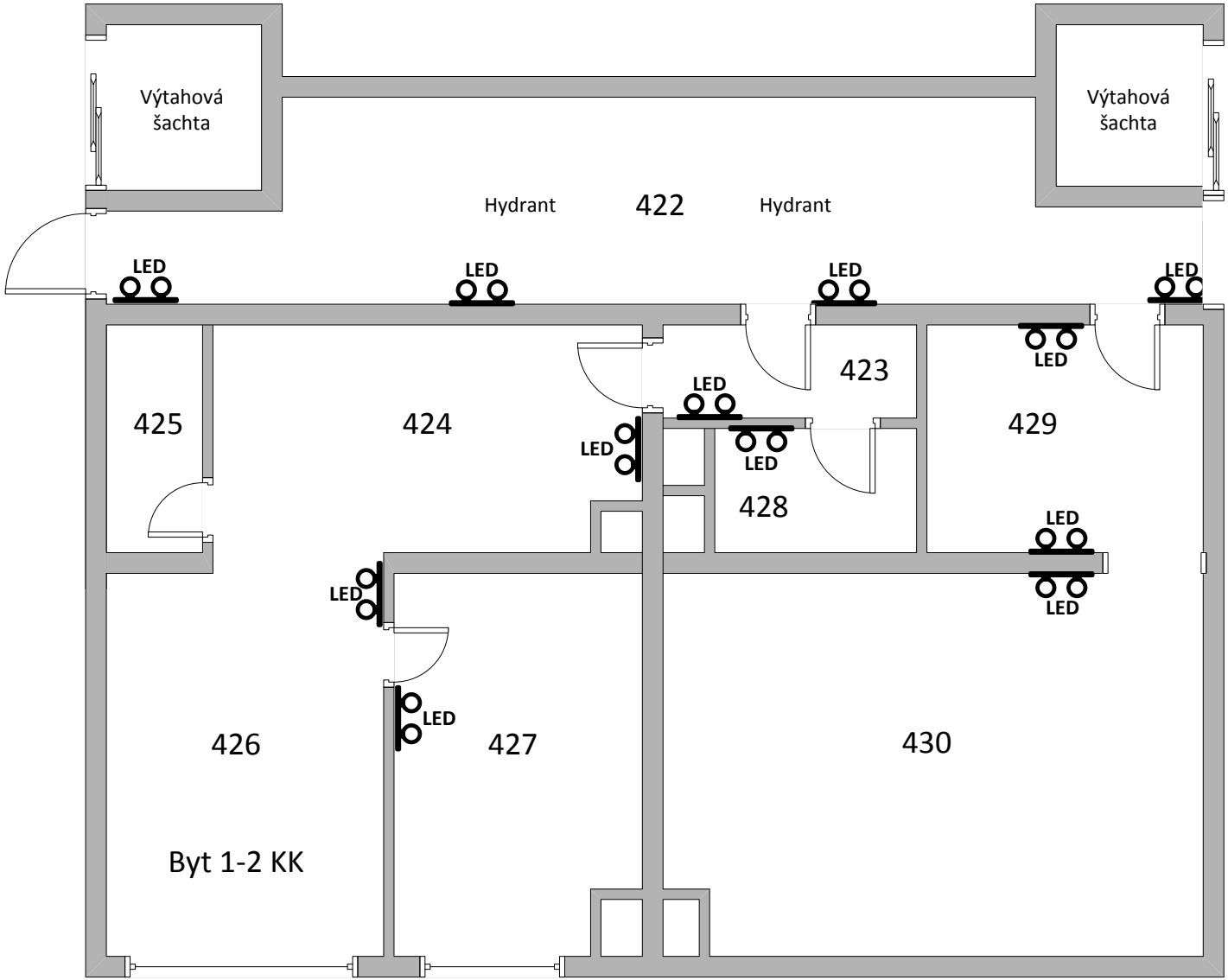
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - pravé křídlo

LED osvětlení

LED - LED osvětlení

Příloha 54



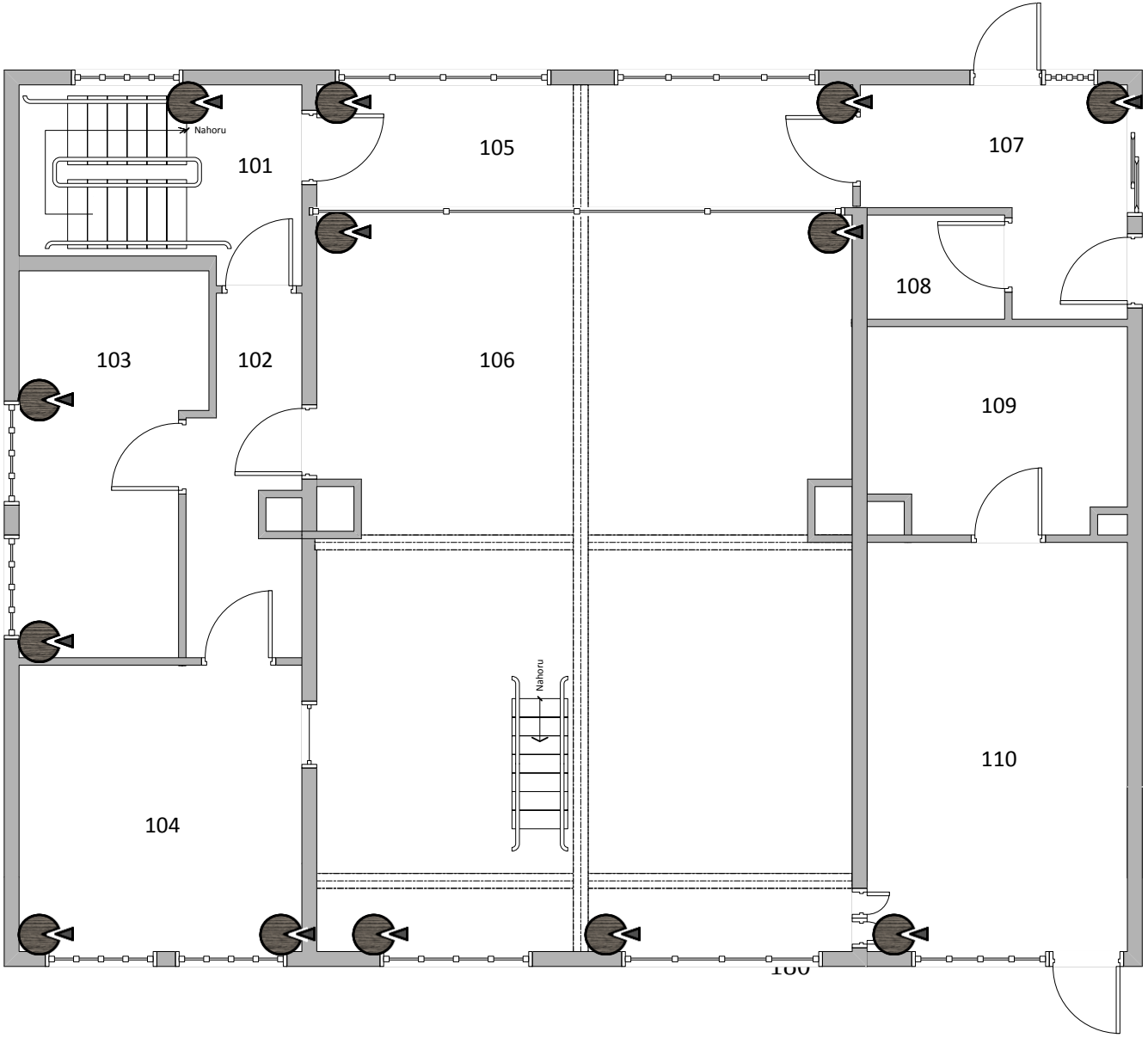
Výukové středisko zabývající se výzkumem v chemickém průmyslu

4.patro - střed

LED osvětlení

LED - LED osvětlení

Příloha 55



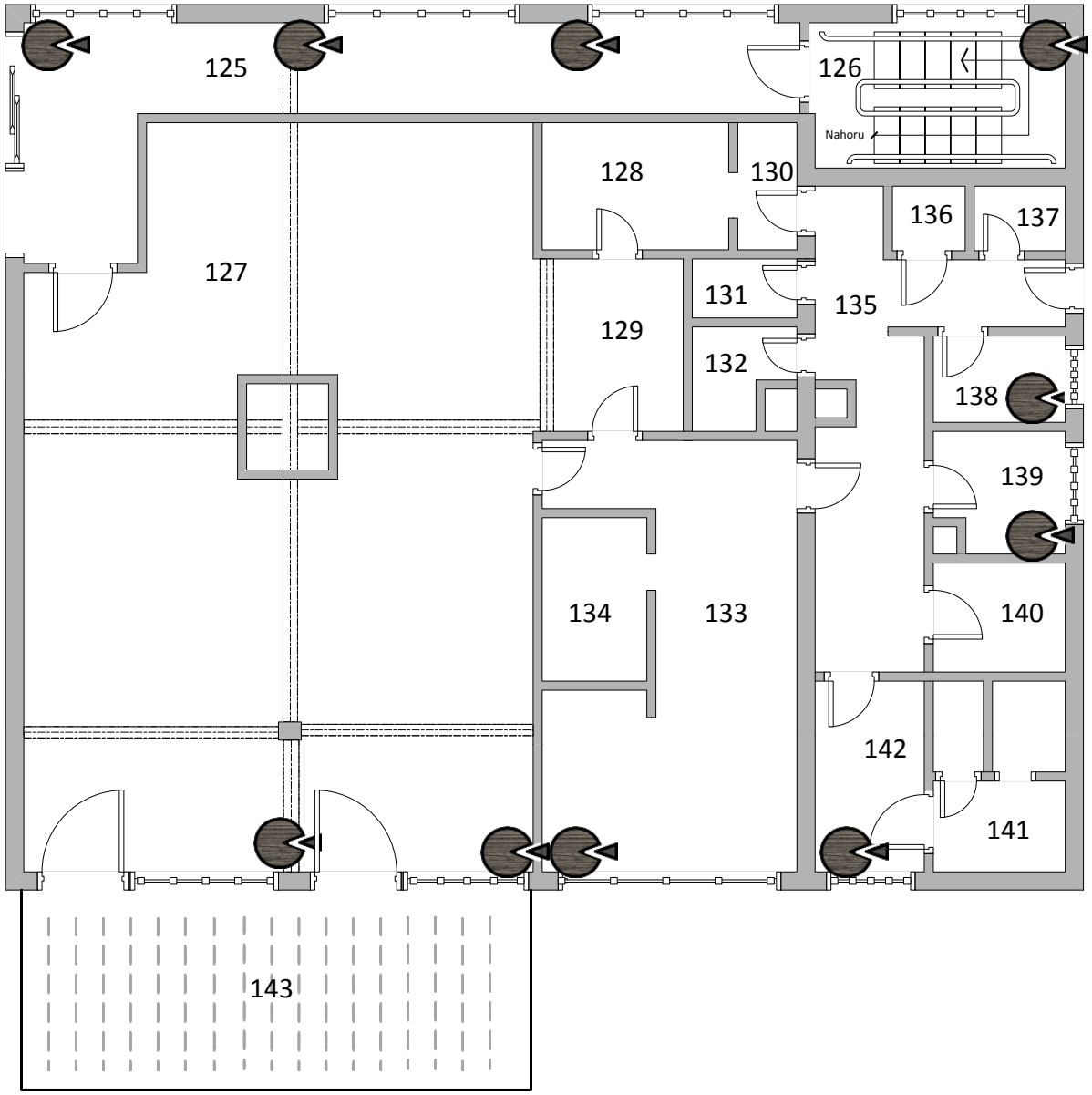
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - levé křídlo

Čidla rozbití skel

- čidlo rozbití skla

Příloha 56



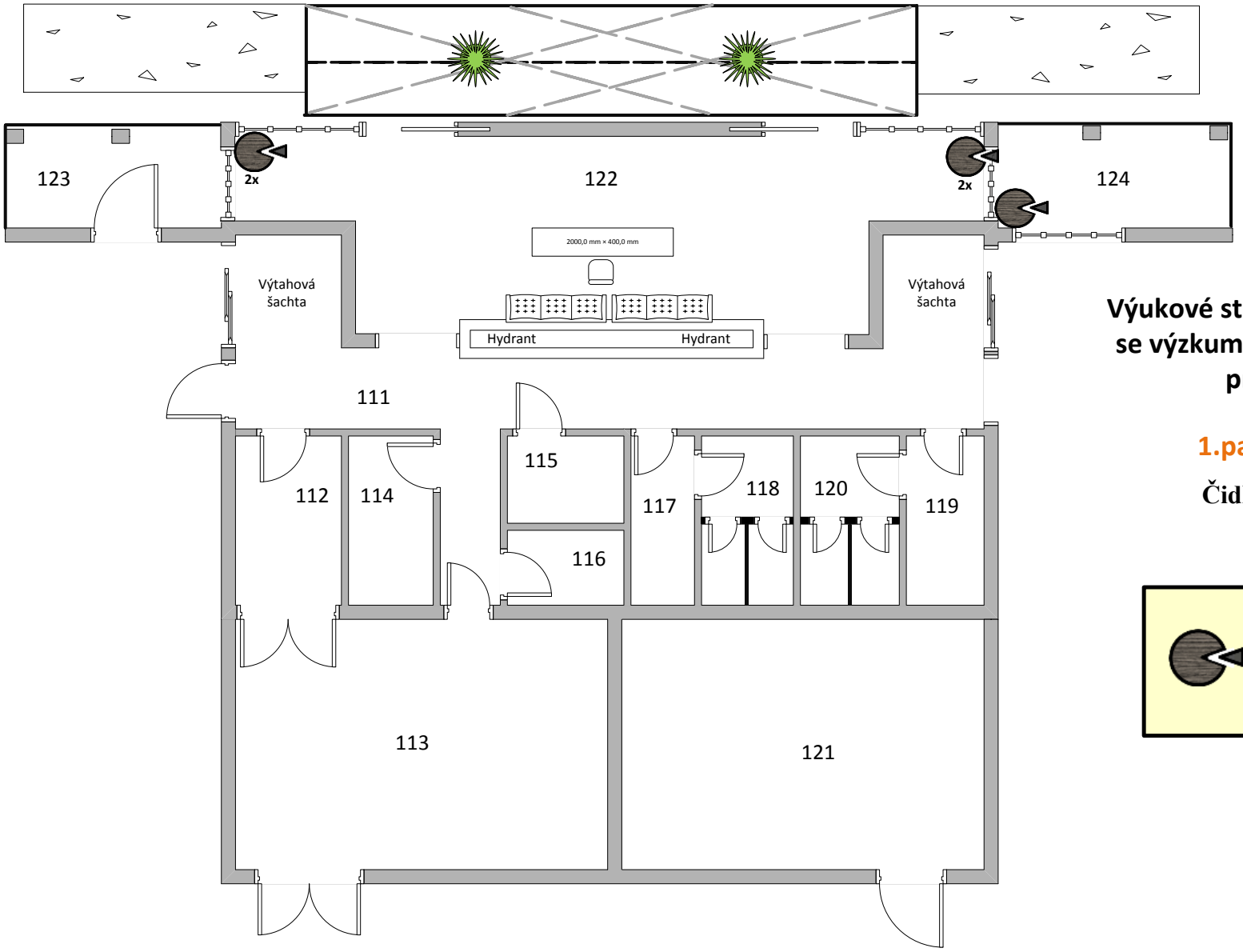
Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - pravé křídlo

Čidla rozbití skel

- čidlo rozbití skla

Příloha 57



Výukové středisko zabývající se výzkumem v chemickém průmyslu

1.patro - střed

Čidla rozbití skel

- čidlo rozbití skla

Příloha 58

Abychom mohli sestavit i jen předběžnou kalkulaci, je nezbytné, abychom znali počet komponent v rámci celého objektu. Počet navržených komponent je znázorněn v tabulce č. 6.

V rámci předběžné kalkulace činí **celková suma 2 668 858,- Kč s DPH**, kde jsou jednotlivé komponenty zapracovány do tabulek 7-16. Ceny materiálu a instalace jsou odhadovány na základě zkušeností a nabídek různých dodavatelů.

Instalace bude započtena jako 1/3 z ceny materiálu, kromě bezpečnostních oken, u nichž bude započítána cena za nasazení jednoho bezpečnostního okna.

V rámci předběžné kalkulace je stanovena rezerva 10% z ceny materiálu a instalace.

Tabulka 6: Počet navržených komponent
Zdroj: Vlastní zpracování

Komponenty	1.NP	2.NP	3.NP	4.NP	Celkem
PIR čidla (180°)	26	20	17	15	78
PIR čidla (360°)	7	3	5	5	20
Čidla rozbití skla	26	-	-	-	26
Detektor kouře	34	16	14	16	80
Detektor plynu	21	16	14	14	65
LED osvětlení	101	82	71	64	318
Čtečky karet	24	13	10	11	58
RFID na dokumenty	50	-	-	-	50
Kamery	16	-	-	-	16
Bezpečnostní okna 3. třídy	15	-	-	-	15
Bezpečnostní okna 4. třídy	12	-	-	-	12

Tabulka 7: Předpokládané náklady EZS
Zdroj: Vlastní zpracování

Předpokládané náklady EZS	
Komponenty	50 000,- Kč
Kabeláž	120 000,-Kč
Instalace	56 667,- Kč
Rezerva	22 667,- Kč
Celková cena	249 334,- Kč
DPH 21%	52 360,- Kč
Fakturovaná částka s 21% DPH	**301 694,- Kč**

Tabulka 8: Předpokládané náklady detektorů kouře
Zdroj: Vlastní zpracování

Předpokládané náklady detektorů kouře	
Komponenty	30 000,- Kč
Kabeláž	150 000,-Kč
Instalace	60 000,- Kč
Rezerva	24 000,- Kč
Celková cena	264 000,- Kč
DPH 21%	55 440,- Kč
Fakturovaná částka s 21% DPH	**319 440,- Kč**

Tabulka 9: Předpokládané náklady detektorů plynu
Zdroj: Vlastní zpracování

Předpokládané náklady detektorů plynu	
Komponenty	35 000,- Kč
Kabeláž	130 000,-Kč
Instalace	55 000,- Kč
Rezerva	22 000,- Kč
Celková cena	242 000,- Kč
DPH 21%	50 820,- Kč
Fakturovaná částka s 21% DPH	**292 820,- Kč**

Tabulka 10: Předpokládané náklady LED osvětlení
Zdroj: Vlastní zpracování

Předpokládané náklady LED nouzového osvětlení	
Komponenty	115 000,- Kč
Kabeláž	250 000,- Kč
Instalace	121 667,- Kč
Rezerva	48 667,- Kč
Celková cena	535 334,- Kč
DPH 21%	112 420,- Kč
Fakturovaná částka s 21% DPH	**647 754,- Kč**

Tabulka 11: Předpokládané náklady kamerového systému
Zdroj: Vlastní zpracování

Předpokládané náklady kamerového systému	
Komponenty	100 000,- Kč
Kabeláž	100 000,- Kč
Instalace	66 667,- Kč
Rezerva	26 667,- Kč
Celková cena	293 334,- Kč
DPH 21%	61 600,- Kč
Fakturovaná částka s 21% DPH	**354 934,- Kč**

Tabulka 12: Předpokládané náklady bezpečnostních oken 3. třídy
Zdroj: Vlastní zpracování

Předpokládané náklady bezpečnostních oken 3. třídy	
Komponenty	55 500,- Kč
Montáž	9 750,- Kč
Rezerva	6 525,- Kč
Celková cena	71 775,- Kč
DPH 21%	15 073,- Kč
Fakturovaná částka s 21% DPH	**86 848,- Kč**

Tabulka 13: Předpokládané náklady bezpečnostních oken 4. třídy
Zdroj: Vlastní zpracování

Předpokládané náklady bezpečnostních oken 4. třídy	
Komponenty	76 800,- Kč
Montáž	7 800,- Kč
Rezerva	8 460,- Kč
Celková cena	93 060,- Kč
DPH 21%	19 543,- Kč
Fakturovaná částka s 21% DPH	**112 603,- Kč**

Tabulka 14: Předpokládané náklady RFID
Zdroj: Vlastní zpracování

Předpokládané náklady RFID na citlivé dokumenty	
Komponenty	4 500,- Kč
Rezerva	450,- Kč
Celková cena	4 950,- Kč
DPH 21%	1 039,- Kč
Fakturovaná částka s 21% DPH	**5 989,- Kč**

Tabulka 15: Předpokládané náklady čidel rozbití skel
Zdroj: Vlastní zpracování

Předpokládané náklady čidel rozbití okenních skel	
Komponenty	18 500,- Kč
Kabeláž	60 000,- Kč
Instalace	26 167,- Kč
Rezerva	10 467,- Kč
Celková cena	115 134,- Kč
DPH 21%	24 178,- Kč
Fakturovaná částka s 21% DPH	**139 312,- Kč**

Tabulka 16: Předpokládané náklady čteček karet
Zdroj: Vlastní zpracování

Předpokládané náklady čteček karet	
Komponenty	69 600,- Kč
Kabeláž	160 000,- Kč
Instalace	76 534,- Kč
Rezerva	30 613,- Kč
Celková cena	336 747,- Kč
DPH 21%	70 717,- Kč
Fakturovaná částka s 21% DPH	**407 464,- Kč**

I když je návrh zabezpečení za poměrně vyšší cenu, tato investice se časem zákazníkovi vrátí. Jestliže by výzkum přišel o citlivé, důležité informace, škoda by mohla přesáhnout nejen investici do výzkumu, ale i budoucí výnos. Tímto by se také měla navrátit investice do zabezpečení objektu. Přičemž nejde jen o ztrátu dat a finanční částky, ale také o lidi, kteří tomu věnovali svůj čas a vložili do toho svoje city.

Příloha 59

Soulad s požadavky

Návrh zabezpečení výukového střediska zaměřeného na výzkum v chemickém průmyslu odpovídá v souladu jak s právními normami, tak s bezpečnostními politikami, normami, technické shodě a z hlediska auditu IS. (22)

Cílem je vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků. Zajistit shodu systémů s bezpečnostními politikami organizace a normami. (22)

- Pro každý IS budou jednoznačně definovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, regulatorní a smluvní požadavky a způsob, jakým je bude organizace dodržovat
- Budou zavedeny vhodné postupy pro zajištění souladu se zákonnými, regulatorními a smluvními požadavky na použití materiálů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví
- Důležité záznamy organizace budou chráněny proti ztrátě, zničení a padělání v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace
- Ochrana dat a soukromí bude zajištěna v souladu s odpovídající legislativou, předpisy, a pokud je to relevantní, tak se smlouvami
- Bude zakázáno používání prostředků pro zpracování informací jiným než autorizovaným způsobem
- V případě kryptografických opatření, budou tato opatření používána v souladu s příslušnými úmluvami, zákony a předpisy
- Vedoucí zaměstnanci budou zajišťovat, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami
- IS budou pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy (24)

Další cíl se zaměřuje na maximalizaci účinnosti auditu a minimalizaci zásahů do/z IS. (22)

- Požadavky auditu a činnosti zahrnující kontrolu provozních systémů budou pečlivě plánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace
- Přístup k nástrojům určeným pro audit IS bude chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení (22)

Příloha 60

Certifikace ISMS

Výukové středisko zaměřené na výzkum v chemickém průmyslu bude požadovat vydání certifikátu, kterým bude moci prokázat svoji schopnost trvale uplatňovat bezpečnostní opatření s cílem poskytnout svým partnerům jistotu o úrovni zabezpečení. (23)

Postup certifikace

Na základě žádosti a informací žadatele k provedení certifikace, certifikační orgán vyhodnotí stupeň připravenosti žadatele. Audit provede posouzení dokumentovaných postupů a pravidel a na místě posoudí rozsah a fungování ISMS. Na závěr sdělí výsledek o posouzení, zda tým auditorů doporučuje vydání příslušného certifikátu či nikoliv. Zpracuje zprávu a předloží posuzované organizaci. V případě schválení závěrů výsledků, vydá certifikační orgán příslušný certifikát. Budou-li odhaleny nedostatky, organizace dostane zprávu, co neodpovídá a na co je potřeba se zaměřit a napravit. (23)